

Quantum cryptography beyond qubits

by

Frédéric Bouchard

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
In partial fulfillment of the requirements
For the degree of
Doctor of Philosophy in Physics

Department of Physics
University of Ottawa

© Frédéric Bouchard, Ottawa, Canada, 2019

Abstract

Over the last few decades, quantum cryptography has been one of the most important quantum technologies developed. It holds the promise of communicating secure information over untrusted channels. In particular, quantum cryptography is immune to the eventual threats posed by large-scale quantum computers, which is not the case for our current classical cryptography infrastructures. In a world where information, communication and privacy are of paramount importance, the development of secure quantum communication infrastructures becomes imperative. So far, most of the quantum cryptographic systems developed to date are based on two-dimensional encoding schemes, analogous to classical bits, known as *qubits*. Nevertheless, other than for the polarization of light, photonic degrees of freedom, i.e. position, momentum, time and frequency, naturally occur as high-dimensional quantum systems. Moreover, by considering high-dimensional encoding schemes beyond qubits, advantages in terms of information capacity and noise tolerance are predicted in theory. In this thesis, the basic components of a high-dimensional quantum cryptographic system are investigated. We begin by reviewing important developments in quantum cryptography and high-dimensional quantum information. As a starting point, two different quantum information tasks, i.e. optimal quantum cloning and quantum metrology, are experimentally investigated for high-dimensional quantum systems in order to demonstrate the numerous advantages of performing quantum tasks beyond qubits. The photonic degree of freedom used in these experiments, known as transverse spatial modes, is obtained by combining the position and momentum photonics degrees of freedom. Thus, we develop a novel method to measure high-dimensional quantum states encoded in arbitrary spatial modes. Using a similar characterization technique, several high-dimensional quantum communication channels are characterized to perform high-dimensional quantum cryptography. The tools developed in the laboratory are then brought to realistic conditions in order to test the feasibility of high-dimensional quantum cryptography. Two different types of quantum channels

are experimentally investigated, namely an intra-city 300 m long free-space link and a short 3 m outdoor underwater link. Finally, we investigate and compare novel high-dimensional protocols to overcome current limitations.

Résumé

Au cours des dernières décennies, la cryptographie quantique a été l'une des technologies quantiques les plus importantes développées. Elle assure l'éventualité de communiquer de l'information confidentielle sur des canaux non-sécurisés. En effet, la cryptographie quantique est à l'abri de la menace éventuelle posée par les ordinateurs quantiques, ce qui n'est pas le cas pour nos infrastructures de cryptographie classiques actuelles. Dans un monde où l'information, la communication et la confidentialité sont d'une grande importance, le développement d'infrastructures quantiques devient impératif. À ce jour, la plupart des systèmes quantiques développés reposent sur des systèmes de codages bidimensionnels, similaires aux bits classiques, connus sous le nom de *qubits*. Outre la polarisation de la lumière, les degrés de liberté photoniques, c'est-à-dire la position, l'impulsion, le temps et la fréquence, apparaissent naturellement sous la forme de systèmes quantiques de grande dimension. De plus, en considérant un système de codage à grande dimension au-delà des qubits, des avantages en termes de capacité d'informations et de tolérance au bruit sont prédits par la théorie. Dans cette thèse, les composantes de base d'un système cryptographique quantique à haute dimension sont étudiées. Nous commençons par examiner les développements importants en matière de cryptographie quantique et d'informations quantiques à haute dimension. Deux tâches d'informations quantiques différentes, c'est-à-dire le clonage quantique optimal et la métrologie quantique, sont étudiées expérimentalement avec des systèmes quantiques de grande dimension afin de démontrer les nombreux avantages de l'exécution de tâches quantiques au-delà des qubits. Le degré de liberté photonique utilisé dans ces expériences, appelé modes spatiaux transversaux, est obtenu en combinant les degrés de liberté de position et d'impulsion des photons. Ainsi, nous développons une nouvelle méthode pour mesurer des états quantiques de haute dimension codés dans des modes spatiaux arbitraires. En utilisant une technique de caractérisation similaire, plusieurs canaux de communication sont caractérisés pour effectuer de la cryptographie quantique en haute di-

mension. Les outils développés en laboratoire sont ensuite testés dans des conditions réalistes afin de valider la plausibilité de la cryptographie quantique à haute dimension. Deux types différents de canaux quantiques sont investigués expérimentalement, c'est-à-dire une liaison urbaine en espace libre d'une longueur de 300 m et une liaison sous-marine extérieure d'une longueur de 3 m. Enfin, nous étudions et comparons de nouveaux protocoles à haute dimension pour surmonter certaines limitations actuelles.

Acknowledgements

First and foremost, I wish to thank my supervisor Prof. Ebrahim Karimi for his continuous support, valuable advice and for giving me numerous opportunities throughout the course of my PhD to grow as a scientist. It was a privilege for me to work in such a unique and dynamic scientific environment. I am also extremely grateful to Prof. Robert Boyd for his valuable advice and support throughout my studies.

I acknowledge the financial support of the Vanier Canada Graduate Scholarship and the Natural Sciences and Engineering Research Council of Canada (NSERC).

I would like to thank Robert Fickler for providing his invaluable advice. Discussing new concepts in order to come up with new ideas with you has been one of the most enjoyable parts of my PhD. Thank you for your enthusiasm both inside and outside the lab. I also wish to thank Alicia Sit for being an amazing fellow student. We always formed a great team when working on experiments in difficult conditions. My PhD would have been quite different without you around. Moreover, I would like to thank Felix Hufnagel for his tenacity while performing several experiments, for many interesting discussions and for having made my PhD such a fun time. All three of them were indispensable in the experiments presented in this thesis. Finally, I would like to thank Hugo Larocque for being an example of determination and excellence. My PhD would not have been so fun without you around.

I wish to thank Khabat Heshami and Duncan England for such nice and fruitful collaboration. I particularly appreciate your ability to keep in mind the bigger picture while I was concerned with the experimental details. Most of the work presented in this thesis would not have been possible without the help and support from Khabat and Duncan. I would also like to thank all the members of the SQO group for all their help and moral support throughout my PhD. Thank you Alicia, Hugo, Felix, Robert, Yingwen, Dominik, Aazad, Jérémie, Dominic, Fatimah, Dilip, Florence, Farshad, and Eli.

I would also like to thank my collaborators and friends in Vienna for being so welcoming during my time spent there. In particular, I wish to thank Marcus Huber, for his support and giving me the opportunity to work on several exciting projects. I have learned a lot from you in such a short time. I would also like to thank Mehul Malik, Robert Fickler, and Florian Brandt. Being the only experimentalists in a group of theorists was an amazing and unique experience that would not have been the same without you. Finally, I would like to thank all the members of the group in Vienna from which I learned as much about physics as I did about coffee.

Moreover, I would like to acknowledge all of my other co-authors Pablo de la Hoz, Gunnar Björk, Markus Grassl, Zdeněk Hradil, Andrei Klimov, Gerd Leuchs, Jaroslav Řeháček, Luis Lorenzo Sanchez-Soto, Natalia Herrera Valencia, Dominique Elser, Christian Peuntinger, Kevin Günthner, Bettina Heim, Christoph Marquardt, and Berthold-Georg Englert. I would also like to thank all of my other international collaborators. It is always great to see you again in conferences.

Finally, I would like to thank my parents, Norman Bouchard and Marie-France Langlois, for their unconditional support and encouragements. In many senses, you have played an essential role through every step of the way. To my brother and sister, Pierre-Olivier Bouchard and Stéphanie Bouchard, you guys rock. Thank you for everything.

Most importantly, I would like to thank my amazing wife, Véronique Bélanger, for being incredibly supportive, in particular during those busy weeks. Thank you for still pretending to be interested in my experiments after all these years and for being such a wonderful distraction from my work. I could not have done it without you.

To the love of my life, Véro.

Table of Contents

Abstract	ii
Résumé	iv
Acknowledgements	vi
List of publications	xii
Statement of originality and collaborative contributions	xvii
List of Figures	xix
1 Introduction	1
2 High-dimensional quantum information	6
2.1 Spatial modes of light	7
2.1.1 Optical orbital angular momentum	8
2.1.2 Generation of spatial modes	8
2.2 Quantum cloning	9
2.3 Quantum metrology	10
2.4 Publication: High-dimensional quantum cloning and applications to quantum hacking	12
2.5 Publication: Quantum metrology at the limit with extremal Majorana constellations	18

3	Characterization of high-dimensional quantum states and processes	22
3.1	Detection of spatial modes	23
3.2	Quantum state tomography	24
3.2.1	Density matrix	24
3.2.2	Quantum state tomography of a qubit	25
3.2.3	High-dimensional quantum state tomography	26
3.3	Quantum process tomography	27
3.4	Publication: Measuring azimuthal and radial modes of photons . . .	29
3.5	Publication: Quantum process tomography of a high-dimensional quantum communication channel	46
4	High-dimensional quantum cryptography through free-space and underwater quantum channels	59
4.1	Quantum cryptography in realistic conditions	60
4.2	High-dimensional quantum cryptography	60
4.3	Free-space quantum communications	61
4.4	Underwater quantum communications	62
4.5	Publication: High-Dimensional intra-city quantum cryptography with structured photons	64
4.6	Publication: Quantum cryptography with twisted photons through an outdoor underwater channel	69
5	Quantum key distribution protocols in high dimensions	80
5.1	Quantum key distribution protocols	81
5.2	Tomographic protocols	81
5.3	Practical quantum key distribution	82
5.4	Distributed-phase-reference protocols	82
5.4.1	Round-robin differential phase shift protocol	83
5.4.2	Chau15 protocol	84

5.5	Publication: Round-Robin Differential Phase-Shift Quantum Key Distribution with Twisted Photons	85
5.6	Publication: Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons	90
6	Conclusions	102
	APPENDICES	104
A	Supplementary materials: High-dimensional quantum cloning and applications to quantum hacking	105
B	Supplementary materials: Quantum metrology at the limit with extremal Majorana constellations	110
C	Supplementary materials: High-dimensional intracity quantum cryptography with structured photons	115
	Bibliography	120

List of publications

Ph.D.

1. F. Brandt, M. Hiekkamäki, **F. Bouchard**, M. Huber, & R. Fickler, “High-dimensional quantum gates using full-field spatial modes of photons”, arXiv:1907.13002 (2019).
2. **F. Bouchard**, D. Koutny, F. Hufnagel, Z. Hradil, J. Rehacek, Y. S. Teo, D. Ahn, H. Jeong, L. L. Sánchez-Soto, G. Leuchs, & E. Karimi, “Compressed sensing of twisted photons”, *Optics Express* **27**, 13 (2019).
3. F. Hufnagel, A. Sit, F. Grenapin, **F. Bouchard**, K. Heshami, D. England, Y. Zhang, B. J. Sussman, R. W. Boyd, G. Leuchs, & E. Karimi, “Characterization of an underwater channel for quantum communications in the Ottawa River”, *Optics Express* **27**, 19 (2019).
4. R. Fickler, **F. Bouchard**, E. Giese, V. Grillo, G. Leuchs, & E. Karimi, “Full-field mode sorter using two optimized phase transformations for high-dimensional quantum cryptography”, arXiv:1905.01175 (2019).
5. S. Ecker, **F. Bouchard**, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, & M. Huber, “Entanglement distribution beyond qubits or: How I stopped worrying and learned to love the noise”, arXiv:1904.01552 (2019).
6. E. Cohen, H. Larocque, **F. Bouchard**, F. Nejdassattari, Y. Gefen, & E. Karimi, “Geometric phase from Aharonov-Bohm to Pancharatnam-Berry and Beyond”, *Nature Physics Review* **1**, 437 (2019).
7. T. Bauer, P. banzer, **F. Bouchard**, S. Orlov, L. Marrucci, E. Santamato, R. Boyd, E. Karimi, & G. Leuchs, “Multi-twist polarization ribbon topologies in

-
- highly-confined optical fields”, *New Journal of Physics* **21**, 053020 (2019).
8. **F. Bouchard**, F. Hufnagel, D. Koutný, A. Abbas, A. Sit, K. Heshami, R. Fickler, & E. Karimi, “Quantum process tomography of a high-dimensional quantum communication channel”, *Quantum* **3**, 138 (2019).
 9. F. Kong, C. Zhang, H. Larocque, Z. Li, **F. Bouchard**, D. H. Ko, G. Brown, A. Korobenko, T. Hammond, R. Boyd, E. Karimi, & P. Corkum, “Vectorizing the spatial structure of high-harmonic radiation from gas”, *Nature Communications* **10** 2020 (2019).
 10. D. Ahn, Y. S. Teo, H. Jeong, **F. Bouchard**, F. Hufnagel, E. Karimi, D. Koutny, J. Rehacek, Z. Hradil, G. Leuchs, & L. L. Sánchez-Soto, “Adaptive compressive tomography with no a priori information”, *Physical Review Letters* **122**, 100404 (2019).
 11. F. Nejdassattari, Y. Zhang, **F. Bouchard**, H. Larocque, A. Sit, E. Cohen, R. Fickler, & E. Karimi, “Experimental Realization of Wave-packet Dynamics in Cyclic Quantum Walks”, *Optica* **6**, 2 (2019).
 12. Y. Zhang, A. Sit, **F. Bouchard**, H. Larocque, E. Cohen, A. C. Elitzur, J. L. Harden, R. W. Boyd, & E. Karimi, “Interaction-Free Ghost-Imaging of Structured Objects”, *Optics Express* **27**, 3 (2019).
 13. **F. Bouchard**, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, & E. Karimi, “Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons”, *Quantum* **2**, 111 (2018).
 14. **F. Bouchard**, N. H. Valencia, F. Brandt, R. Fickler, M. Huber, & M. Malik, “Measuring azimuthal and radial modes of photons”, *Optics Express* **26**, 31925 (2018).
 15. F. Kong, C. Zhang, H. Larocque, **F. Bouchard**, Z. Li, M. Taucer, G. Brown, T. J. Hammond, E. Karimi, & P. B. Corkum, “Spin constrained orbital angular momentum control in high-harmonic generation”, arXiv:1810.05894 (2018).
 16. **F. Bouchard**, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. W. Boyd, & E. Karimi, “Quantum cryptography with twisted photons through an outdoor underwater channel”, *Optics Express* **26**, 22563 (2018).

-
17. A. Sit, R. Fickler, F. Alsaïari, **F. Bouchard**, H. Larocque, P. Gregg, L. Yan, R. W. Boyd, S. Ramachandran, & E. Karimi, “Quantum cryptography with structured photons through a vortex fiber”, *Optics Letters* **43**, 4108 (2018).
 18. **F. Bouchard**, A. Sit, K. Heshami, R. Fickler, & E. Karimi, “Round-Robin Differential Phase-Shift Quantum Key Distribution with Twisted Photons”, *Physical Review A* **96**, 010301(R) (2018).
 19. **F. Bouchard**, P. de la Hoz, G. Björk, R. W. Boyd, M. Grassl, Z. Hradil, E. Karimi, A. B. Klimov, G. Leuchs, J. Rehacek, & L. L. Sánchez-Soto, “Quantum metrology at the limit with extremal Majorana constellations”, *Optica* **4**, 1429 (2017).
 20. V. Grillo, T. R. Harvey, F. Venturi, J. S. Pierce, R. Balboni, **F. Bouchard**, G. Gazzadi, S. Frabboni, A. H. Tavabi, Z.-A. Li, R. E. Dunin-Borkowski, R. W. Boyd, B. J. McMorran, & E. Karimi, “Observation of nanoscale magnetic fields using twisted electron beams”, *Nature Communications* **8**, 689 (2017).
 21. A. Sit, **F. Bouchard**, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Gunthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, & E. Karimi, “High-Dimensional intra-city quantum cryptography with structured photons”, *Optica* **4**, 1006 (2017).
 22. M. G. Rahimian, **F. Bouchard**, H. Al-Khazraji, E. Karimi, P. B. Corkum, & V. R. Bhardwaj, “Polarization dependent nanostructuring of silicon with femtosecond vortex pulse”, *APL Photonics* **2**, 086104 (2017).
 23. H. Larocque, J. Gagnon-Bischoff, D. Mortimer, Y. Zhang, **F. Bouchard**, J. Upham, V. Grillo, R. W. Boyd, & E. Karimi, “Generalized optical angular momentum sorter and its application to high-dimensional quantum cryptography”, *Optics Express* **25**, 19832 (2017).
 24. F. Tamburini, B. Thidé, I. Licata, **F. Bouchard**, E. Karimi, “Majorana states for subluminal structured photons”, arXiv:1707.07160 (2017).
 25. V. Grillo, A. H. Tavabi, F. Venturi, H. Larocque, R. Balboni, G.-C. Gazzadi, S. Frabboni, P.-H. Lu, E. Mafakheri, **F. Bouchard**, R. E. Dunin-Borkowski, R. W. Boyd, M. P. J. Lavery, M. J. Padgett, & E. Karimi, “Measuring the orbital angular momentum spectrum of an electron beam”, *Nature Communications* **8**, 15536 (2017).

26. F. Kong, C. Zhang, **F. Bouchard**, Z. Li, G. G. Brown, D. H. Ko, T. J. Hammond, L. Arissian, R. W. Boyd, E. Karimi, & P. B. Corkum, “Controlling the orbital angular momentum of high harmonic vortices”, *Nature Communications* **8**, 14970 (2017).
27. **F. Bouchard**, R. Fickler, R. W. Boyd, & E. Karimi, “High-dimensional quantum cloning and applications to quantum hacking”, *Science Advances* **3**, e1601915 (2017).
28. **F. Bouchard**, H. Larocque, A. M. Yao, C. Travis, I. De Leon, A. Rubano, E. Karimi, G.-L. Oppo, & R. W. Boyd, “Polarization shaping for control of nonlinear propagation”, *Physical Review Letters* **117**, 233903 (2016).
29. H. Larocque, J. Gagnon-Bischoff, **F. Bouchard**, R. Fickler, J. Upham, R. W. Boyd, & E. Karimi, “Arbitrary optical wavefront shaping via spin-to-orbit coupling”, *Journal of Optics* **18**, 124002 (2016).
30. H. Larocque, **F. Bouchard**, V. Grillo, A. Sit, S. Frabboni, R. E. Dunin-Borkowski, M. J. Padgett, R. W. Boyd, & E. Karimi, “Nondestructive measurement of orbital angular momentum for an electron beam”, *Physical Review Letters* **117**, 154801 (2016).
31. P. Wozniak, P. Banzer, **F. Bouchard**, E. Karimi, G. Leuchs, & R. W. Boyd, “Tighter spots of light with superposed orbital angular momentum beams,” *Physical Review A* **94**, 021803 (2016).

M.Sc.

32. J. Harris, **F. Bouchard**, E. Santamato, W. H. Zurek, R. W. Boyd, & E. Karimi, “Quantum probabilities from quantum entanglement: experimentally unpacking the Born rule,” *New Journal of Physics* **18**, 053013 (2016).
33. **F. Bouchard**, J. Harris, H. Mand, R. W. Boyd, & E. Karimi, “Observation of sub-luminal twisted light in vacuum,” *Optica* **3**, 351 (2016).
34. S. A. Schulz, J. Upham, **F. Bouchard**, I. De Leon, E. Karimi, & R. W. Boyd, “Quantifying the impact of proximity error correction on plasmonic metasurfaces,” *Optical Materials Express* **5**, 2798 (2015).

-
35. **F. Bouchard**, J. Harris, H. Mand, N. Bent, E. Santamato, R. W. Boyd, & E. Karimi, “Observation of quantum recoherence of photons by spatial propagation,” *Scientific Reports* **5**, 15330 (2015).
 36. A. Ahangary, **F. Bouchard**, E. Santamato, E. Karimi, & H. R. Khalesifard, “Dynamics of laser-induced radial birefringence in silver-doped glasses,” *Optics Letters* **40**, 4062 (2015).
 37. **F. Bouchard**, H. Mand, M. Mirhosseini, E. Karimi, & R. W. Boyd, “Achromatic orbital angular momentum generator,” *New Journal of Physics* **16**, 123006 (2014).
 38. **F. Bouchard**, I. De Leon, S. A. Schulz, J. Upham, E. Karimi, & R. W. Boyd, “Optical spin-to-orbital angular momentum conversion in ultra-thin metasurfaces with arbitrary topological charges,” *Applied Physics Letters* **105**, 101905 (2014).

Statement of originality and collaborative contributions

To the best of his knowledge, the author states that the work described in this PhD thesis constitute original research in the field of physics. Below, we provide the collaborative contributions of each participant for every chapter.

F. Bouchard and E. Karimi conceived the idea for the work presented in chapter 2 on high-dimensional quantum cloning and applications to quantum hacking. F. Bouchard, R. Fickler, R. Boyd, and E. Karimi designed the experiment. F. Bouchard performed the experiment and analyzed the data. F. Bouchard and E. Karimi wrote the manuscript with the help from all authors. All authors discussed the results and contributed to the text of the manuscript.

F. Bouchard, L. Sanchez-Sotto, R. Boyd, G. Leuchs, and E. Karimi conceived the idea for the work presented in chapter 2 on quantum metrology at the limit with extremal Majorana constellations. F. Bouchard and E. Karimi designed the experiment. F. Bouchard performed the experiment. F. Bouchard, P. de la Hoz, Z. Hradil, J. Řeháček, and L. Sanchez-Sotto analyzed the data. P. de la Hoz, G. Björk, M. Grassl, A. Klimov, and L. Sanchez-Sotto developed the theory. F. Bouchard, L. Sanchez-Sotto and E. Karimi wrote the manuscript with help from all authors. All authors discussed the results and contributed to the text of the manuscript.

F. Bouchard, N. H. Valencia, M. Huber, and M. Malik initiated the work presented in chapter 3 on measuring azimuthal and radial modes of photons. F. Bouchard conceived the idea. F. Bouchard and F. Brandt performed the experiment. F. Bouchard analyzed the data. F. Bouchard wrote the manuscript with the help from all authors. All authors discussed the results and contributed to the text of the manuscript.

F. Bouchard, K. Heshami, and E. Karimi initiated the work presented in chapter 3 on quantum process tomography of a high-dimensional quantum communication

channel. F. Bouchard, F. Hufnagel, and A. Abbas performed the experiment. F. Bouchard and D. Koutný analyzed the data. F. Bouchard wrote the manuscript with the help from all authors. All authors discussed the results and contributed to the text of the manuscript.

E. Karimi, R. Boyd, G. Leuchs, and C. Marquardt initiated the work presented in chapter 4 on high-dimensional intracity quantum cryptography with structured photons. A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, and E. Karimi designed and built the Ottawa intra-city link. A. Sit, F. Bouchard, and R. Fickler performed the experiment. H. Larocque and J. Gagnon-Bischoff fabricated the q -plates. A. Sit, F. Bouchard and R. Fickler analyzed the data. A. Sit, F. Bouchard, D. Elser, C. Peuntinger, K. Günthner, C. Marquardt, G. Leuchs, R. Boyd, and E. Karimi designed the first iteration in Erlangen, Germany. K. Heshami developed the theory. A. Sit, F. Bouchard, R. Fickler, and E. Karimi wrote the manuscript with the help from all authors. All authors discussed the results and contributed to the text of the manuscript.

F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, and E. Karimi initiated the work presented in chapter 4 on quantum cryptography with twisted photons through an outdoor underwater channel. F. Bouchard, A. Sit, F. Hufnagel, A. Abbas performed the experiment. F. Bouchard, A. Sit, F. Hufnagel, and K. Heshami analyzed the data. F. Bouchard, A. Sit, F. Hufnagel, and E. Karimi wrote the manuscript with the help from all authors. All authors discussed the results and contributed to the text of the manuscript.

F. Bouchard, K. Heshami, R. Fickler, and E. Karimi initiated the work presented in chapter 5 on round-robin differential-phase shift quantum key distribution with twisted photons. F. Bouchard performed the experiment. F. Bouchard and K. Heshami analyzed the data. F. Bouchard, A. Sit, K. Heshami, R. Fickler, and E. Karimi wrote the manuscript. All authors discussed the results and contributed to the text of the manuscript.

F. Bouchard, K. Heshami, and E. Karimi initiated the work presented in chapter 5 on the experimental investigation of high-dimensional quantum key distribution protocols with twisted photons. F. Bouchard performed the experiment. F. Bouchard and K. Heshami analyzed the data. F. Bouchard, K. Heshami, R. Fickler, and E. Karimi wrote the manuscript. All authors discussed the results and contributed to the text of the manuscript.

List of Figures

2.1 **Laguerre-Gauss modes.** The phase profile and intensity profile of several LG modes are shown for azimuthal index values of $\ell \in \{-3, -2, -1, 0, 1, 2, 3\}$ and radial index values of $p \in \{0, 1, 2\}$. The phase is shown by the value of the hue colour and the intensity profile by its opacity.

Chapter 1

Introduction

At the turn of the twentieth century, a handful of brilliant physicists developed a physical theory describing some of the most puzzling phenomena found at the time. This theory is now known as *Quantum mechanics* and has always captured our imagination by incorporating mind-boggling effects such as the wave-particle duality, the principle of superposition, and quantum tunnelling, to name a few. Since then, quantum mechanics has been experimentally verified over and over with tremendous success, eventually leading to the development of countless ubiquitous technologies. The transistor and the laser are examples that would be hard to imagine living without in today's world overwhelmed by computers and smartphones. Nevertheless, in the year 1935, a group of three physicists, Einstein, Podolsky and Rosen, published a paper questioning the completeness of quantum mechanics pointing out an even more puzzling phenomenon predicted by the theory [1]. This phenomenon, referred to as *Verschränkung* by Schrödinger in German, is now known as quantum entanglement. Since then, quantum entanglement went through the incredible journey of evolving from a topic of philosophy [2], theoretical physics [3], experimental physics [4, 5, 6], and now applied physics [7]. Today, the term quantum technologies refers to the emerging applications of the second quantum revolution based on quantum entanglement and superposition [8]. Such applications are usually divided in three categories: (1) Quantum computing [9], (2) Quantum cryptography [10, 11], and (3) Quantum sensing [12]. Quantum cryptography will be the subject of this thesis.

In 1984, Bennett and Brassard introduced the concept of quantum cryptography in what is now known as the BB84 protocol [10]. They made the extraordinary realization that the quantum nature of light could somehow be linked to the completely unrelated problem of sharing information in a secure manner. Once pointed out, quan-

tum cryptography can be understood from various elementary quantum mechanical principles. For example, Heisenberg’s uncertainty principle [13] implies that the measurement of a variable inevitably disturbs its conjugate variable. Hence, by taking advantage of an encoding scheme over a set of conjugate variables, an eavesdropper would be detected by measuring disturbances in the shared quantum information. Another fundamental principle in quantum mechanics is the no-cloning theorem [14] stating that it is impossible to copy a quantum state without introducing errors in the copied clones. In the context of cryptography, the no-cloning theorem clearly prevents an adversary, even when equipped with a quantum cloning machine, from eavesdropping on the photon’s quantum states without introducing disturbances in the channel. The uncertainty principle and the no-cloning theorem offer an intuitive understanding of the security of quantum cryptography. Nevertheless, a formal security analysis is required to calculate the amount of information leaked to an eavesdropper and the remaining amount of secure information left to the authorized partner.

In fact, quantum cryptography corresponds to a larger body of cryptographic techniques based on quantum resources. Although quantum money [15] and quantum secret sharing [16] are both examples of quantum cryptographic schemes, quantum key distribution (QKD) [10] is by far the most well-known and matured one. In particular, QKD takes place between two authorized partners, i.e. a sender and a receiver, conventionally referred to as *Alice* and *Bob*, respectively. Interestingly, Alice and Bob do not encode their message directly onto the sent photons. Rather, they encode a string of random bits, which is known as the shared secret key. Subsequently, the message is broadcasted over an authenticated public channel using the random shared secret key as a one time pad. An eavesdropper, conventionally referred to as *Eve*, without the key in her possession will only see random noise instead of the message. Assuming that Alice and Bob alone share the secret key, this symmetric-key encryption scheme is known to be absolutely secure. In contrast, a public-key encryption scheme, such as those currently in use today for online applications, lies on mathematically “hard” problems that are computationally expensive to break. Hence, the main goal of QKD is to distribute a random key that is known solely by Alice and Bob.

In its original form, the BB84 protocol was proposed using polarization qubits. In particular, a “0” is associated to the horizontally polarized state of a single photon, i.e. $|H\rangle$, and a “1” is associated to the vertically polarized state of a single photon, i.e. $|V\rangle$, in the $\{|H\rangle, |V\rangle\}$ basis. In order to be secure, Alice and Bob must also

encode information on the photons using another basis that is mutually unbiased to the first basis, analogous to the example of conjugate variables with the uncertainty principle. Bases with this property are known as mutually unbiased bases (MUB). A second MUB can be realized by also associating a “0” and a “1” to the diagonally, i.e. $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ and anti-diagonally, i.e. $|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$ polarized state of single photons, respectively. Alice and Bob then randomly choose a MUB to prepare and measure the single photon’s states, respectively. Later on, they will share the information of which MUB was used, over a public channel, and the bits encoded in mismatching MUB will be discarded. This process is known as *sifting*. For the cases where Alice and Bob did prepare and measure the photons in the same MUB, perfect correlation among the bits is expected. In that case, Alice and Bob now share a secret key, achieving the goal of QKD. However, in actual implementations, errors in Alice and Bob’s shared key are to be expected due to imperfect devices and noises in the channel, and may not be from an adversary eavesdropper. Nevertheless, all errors in the shared key must be associated to an eavesdropper in order to avoid making any wrong assumptions. Therefore, a crucial matter in QKD is the assessment of security given a certain level of errors in the shared key [17]. For the case of the BB84 protocol, the error threshold is 11.0 % after which the quantum channel is deemed insecure. To understand the meaning of an error threshold for security in a QKD system, we have to think about the strategies available to the eavesdropper. In particular, the eavesdropper’s wish is twofold: (1) extract as much information from the channel as possible, and (2) introduce the least amount of disturbances in the channel. However, quantum mechanics prohibits the eavesdropper to do both at the same time. Thus, Eve must find the optimal trade-off to gain as much information about Alice and Bob’s photons, but to keep the introduced errors as low as possible. This point is specifically the error threshold mentioned above.

In the original proposal by Bennett and Brassard, the polarization of light was used as the degree of freedom to encode the information. Since then, the first experimental demonstrations of QKD were done using polarization due to the simplicity in generation and detection [18, 19, 20]. However, photons also possess other interesting degrees of freedom, such as time-bins, frequency-bins, position, and momentum. Moreover, it is possible to combine position and momentum to form a set of discrete modes, referred to as transverse spatial modes. In the presence of cylindrical symmetry, the set of spatial modes that is most advantageous are the Laguerre-Gauss (LG) modes which are invariant upon free-space propagation. Moreover, LG modes are complete, orthogonal and can be labelled by two mode indices, i.e. an azimuthal

mode index, ℓ , and a radial mode index, p . Information can then be encoded in the mode indices similar to the case of polarization. However, we notice here that we have at our disposal a larger encoding alphabet compared to polarization, i.e. “0”, “1”, but also “2”, “3”, and so forth [21]. In practice, the extent of the alphabet is dictated by the experimental implementations, e.g. the size of the aperture at Alice’s and Bob’s stages, the distance of the free-space link, the resolution of the generation and detection devices, etc. Clearly, by employing a larger alphabet (high-dimensional encoding), a larger amount of information can be encoded on a single photon which increases the information capacity of the channel. However, from a security standpoint, it is not clear whether putting more of the information on a single photon places the eavesdropper at an advantage or a disadvantage. As we will see in the following chapters, high-dimensional encoding is particularly robust against eavesdropping and leads to a larger tolerance to noise [22]. Finally, larger alphabets lead to more freedom in the elaboration of quantum protocols with novel functionalities [23].

In chapter 2, we experimentally investigated two important quantum information protocols in order to understand some of the benefits of high-dimensional encoding schemes. In particular, high-dimensional quantum cloning and quantum metrology are performed using the azimuthal set of spatial modes. In chapter 3, we start by introducing a new technique to measure arbitrary spatial modes with extremely high mode fidelity. A similar technique is then used to fully characterize different types of channels, i.e. a channel with no eavesdropper and a channel with the eavesdropper performing an optimal quantum cloning attack and an intercept-resend attack. The full characterizations of the quantum channels are carried out for dimensions ranging from 2 to 5. Finally, a formal security analysis is performed in order to evaluate the different scenarios where high-dimensional QKD is most advantageous. In chapter 4, a high-dimensional QKD system based on spatial modes of photons is developed and used in two different realistic quantum channels. In the first case, we consider a 300 m turbulent intra-city link over the campus of the University of Ottawa. Afterwards, we consider an outdoor 3 m underwater link with strong absorption and turbulence. In both cases, the protocol employed is given by a high-dimensional version of the original BB84 QKD scheme. Finally, in chapter 5, we investigate novel high-dimensional quantum cryptographic protocols and compare them to their well-established counterparts. In particular, we develop an experimental platform accommodating a large number of high-dimensional protocols and enabling one to change to the protocol yielding the best performances considering the conditions of the channel.

As a final note, although the subject of this thesis is on quantum cryptography, I have also been involved in several other projects throughout my PhD dealing with spatial modes in quantum optics [24, 25, 26, 27, 28, 29, 30], classical optics [31, 32, 33, 34, 35], nonlinear optics [36], attosecond physics [37, 38, 39], and matter waves [40, 41, 42].

Chapter 2

High-dimensional quantum information

This chapter is based on the following papers:

1. **F. Bouchard**, R. Fickler, R. W. Boyd, & E. Karimi, “High-dimensional quantum cloning and applications to quantum hacking”, *Science Advances* **3**, e1601915 (2017).

DOI: <https://doi.org/10.1126/sciadv.1601915>

© 2017 American Association for the Advancement of Science

2. **F. Bouchard**, P. de la Hoz, G. Björk, R. W. Boyd, M. Grassl, Z. Hradil, E. Karimi, A. B. Klimov, G. Leuchs, J. Rehacek, & L. L. Sánchez-Soto, “Quantum metrology at the limit with extremal Majorana constellations”, *Optica* **4**, 1429 (2017).

DOI: <https://doi.org/10.1364/OPTICA.4.001429>

© 2017 Optical Society of America

2.1 Spatial modes of light

By definition, an optical mode simply is a solution of Maxwell's equations. In particular, it is convenient to work with a complete and orthonormal set of modes. For the polarization degree of freedom, using the Dirac bra-ket notation, such a set would look like $\{|H\rangle, |V\rangle\}$, or in the circular basis $\{|L\rangle, |R\rangle\}$, where $|H\rangle$, $|V\rangle$, $|L\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$, and $|R\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$ correspond to horizontal, vertical, left-circular, and right-circular polarization states, respectively. For the case of transverse spatial modes, let us start with Maxwell's equations and get to a form that can be directly apply to laser beams found in the laboratory. For instance, Maxwell's equations in vacuum can be rearranged to obtain the wave equation. Assuming a monochromatic electromagnetic wave at frequency ω , we obtain a time-independent wave equation also known as Helmholtz's equation. Finally, it is typical to deal with physical beams loosely focusing where the transverse size of the beam is larger than its wavelength [43]. Thus the paraxial approximation is carried out resulting in the paraxial wave equation. In cylindrical coordinates, i.e. r , ϕ and z , a complete and orthonormal family of modes known as the Laguerre-Gauss (LG) modes, see Fig. 2.1, is given by

$$\begin{aligned} \text{LG}_{\ell,p}(r, \phi, z) &= \sqrt{\frac{2p!}{\pi (p+|\ell|)!}} \frac{1}{w(z)} \left(\frac{\sqrt{2}r}{w(z)} \right)^{|\ell|} L_p^{|\ell|} \left(\frac{2r^2}{w(z)^2} \right) \\ &\times \exp \left(-r^2 \left[\frac{1}{w(z)^2} - i \frac{k}{2R(z)} \right] + i\ell\phi + i\zeta_{\ell,p}(z) \right), \end{aligned} \quad (2.1)$$

where $L_p^{|\ell|}(\cdot)$ is the generalized Laguerre polynomial, $\ell \in \{0, \pm 1, \pm 2, \dots\}$ is the azimuthal mode index, $p \in \{0, 1, 2, \dots\}$ is the radial mode index, $w(z) = w_0 \sqrt{1 + (z/z_R)^2}$ is the spot size, w_0 is the beam waist, $z_R = kw_0^2/2$ is the Rayleigh range, k is the wave number, $R(z) = z[1 + (z_R/z)^2]$ is the wavefront's radius of curvature, and $\zeta_{\ell,p}(z) = (2p + |\ell| + 1) \arctan(z/z_R)$ is the propagation dependent Gouy phase. Therefore, a quantum state given by mode indices ℓ and p , i.e. $|\ell, p\rangle$, is expressed in the position basis by the LG modes, i.e. $\langle r, \phi, z | \ell, p \rangle = \text{LG}_{\ell,p}(r, \phi, z)$. Finally, a subset of the LG modes of the form $\exp(i\ell\phi)$, also represents a complete and orthonormal set for azimuthal modes. Its ease of generation and detection, as well as its robustness, makes this family of azimuthal modes an essential tool and a great testbed for experiments in classical and quantum optics.

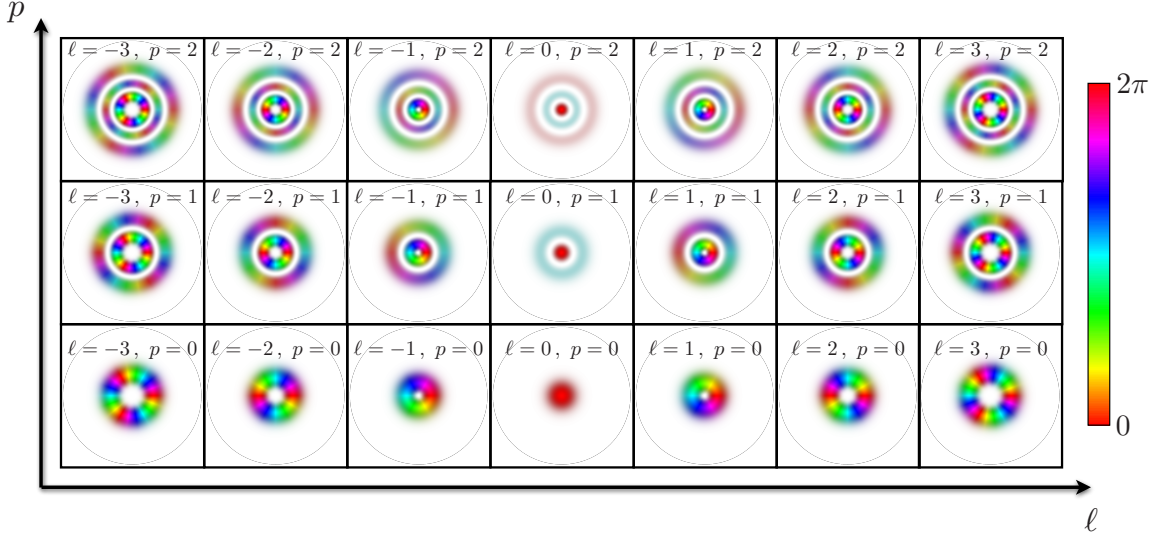


Figure 2.1: **Laguerre-Gauss modes.** The phase profile modulated by the intensity profile of several LG modes are shown for azimuthal index values of $\ell \in \{-3, -2, -1, 0, 1, 2, 3\}$ and radial index values of $p \in \{0, 1, 2\}$. The phase is shown by the value of the hue colour and the intensity profile by its opacity.

2.1.1 Optical orbital angular momentum

Optical beams with a helical wavefront of the form $\exp(i\ell\phi)$ have attracted a lot of attention in classical and quantum optics. Most importantly, it has been recognized that a beam characterized by such a phase profile carries a quantized orbital angular momentum (OAM) value of $\ell\hbar$ per photon along the photon's propagation direction, where $\hbar$ is the reduced Planck constant [44]. Due to the importance of this property, such modes are also referred to as OAM modes or OAM states. Interestingly, OAM carrying optical beams finds numerous applications in several areas of classical optics such as imaging, lithography, optical tweezers [45, 46, 47, 48]. Nevertheless, in this thesis, OAM states of photons are mainly used for applications in quantum information, more particularly as a realization of high-dimensional quantum states.

2.1.2 Generation of spatial modes

In general, arbitrary spatial modes can be challenging to generate since both the intensity and the phase of an incoming beam must be manipulated. Nevertheless, the generation of OAM modes can be achieved straightforwardly by manipulating the phase of an incoming beam, which can be done using a variety of devices. Liquid-crystal

based devices such as spatial light modulators (SLM) and q -plates are among the most practical due to their high-resolution, repeatability and their dynamic nature. In particular, SLMs can be used with well-known holographic techniques to generate phase profiles with extremely high mode fidelity and can be dynamically modified using computer-generated holograms [49, 50]. On the other hand, q -plates are fixed devices able to generate a single profile [51, 52, 32]. However, their phase-imprinting method does not rely on holography, but rather on geometric phases, leading to a higher generation efficiency and direct generation of spin-orbit non-separable beams [53], also known as structured light [54]. Since then, a wide range of devices based on geometric phases have been proposed to generate OAM modes [55, 56, 57, 58]. All the aforementioned devices can also be used for the detection of OAM modes by further coupling the outgoing beam to a single mode fibre (SMF). The detection of OAM and general spatial modes will be covered in more details in the next chapter.

2.2 Quantum cloning

In many senses, quantum cloning can be seen as the precursor to quantum information science [59]. Indeed, this was foreseen by Park [60] in 1970 and by the reviewers of a key paper submitted to *Foundations of Physics* in 1981 [61]. In the latter, the author proposed a scheme, named FLASH, where superluminal communications would be possible. Of course, the reviewers realized that such a scheme would have alarming implications in terms of causality and that the paper was indeed wrong. Nevertheless, one of the reviewers still recommended publishing the paper since he anticipated that its publications would stimulate further investigations in the way we treat information quantum mechanically. Not long after, the no-cloning theorem, which had been derived in the referee report of the FLASH paper [62], was published by Wootters and Zurek [14]. In essence, the no-cloning theorem states that it is impossible to create perfect copies of an arbitrary unknown quantum state and can be proven in a few lines using only the linearity of quantum mechanics. Although simple, the no-cloning theorem has had a remarkable impact on the field of quantum information.

A few years later, an interesting question was raised: Given that the no-cloning theorem prohibits a perfect quantum cloning machine, is it possible to realize a quantum cloning machine that produces imperfect clones? More interestingly, how good is a quantum cloning machine allowed to be according to the laws of quantum mechan-

ics? Quantitatively, the answer to this question can be framed in terms of a cloning fidelity $\mathcal{F}$, which is defined as

$$\mathcal{F} = \langle \psi | \hat{\rho}_1 | \psi \rangle = \langle \psi | \hat{\rho}_2 | \psi \rangle, \quad (2.2)$$

where $|\psi\rangle$ is the unknown quantum state to be cloned, and $\hat{\rho}_1$ and $\hat{\rho}_2$ are the density matrices corresponding to the cloned copies. Here, we have assumed a specific type of quantum cloning machine known as a $1 \rightarrow 2$ symmetric quantum cloning machine, which transforms a single quantum state into two cloned copies with equal fidelity. Furthermore, a quantum cloning machine is said to be optimal if it achieves the highest cloning fidelity allowed by quantum mechanics [63]. Optimal quantum cloning machines are investigated by considering a general ansatz for a parametrized unitary transformation which acts on the initial state and additional ancilla. The cloning fidelity is then directly calculated and maximized using the Lagrange multiplier method, which takes into considerations constraints on the cloning transformation due to unitarity, normalization, and isotropy conditions [64]. The study of optimal quantum cloning machines resulted in the first security analysis of quantum cryptography. Indeed, upper bounds on cloning fidelity could be translated in terms of error thresholds in QKD. As the development of QKD continued, more elaborate attacks were considered in security proofs, i.e. state-dependent cloning, asymmetric cloning, collective, and coherent attacks. Finally, it is interesting to investigate optimal cloning machines beyond qubits, i.e. high-dimensional quantum cloning. From a fundamental standpoint, high-dimensional quantum cloning allows one to investigate the implications of encoding larger amounts of information on a single physical system at the quantum level. Astonishingly, when the dimensionality of the quantum system is enlarged, the cloning fidelity decreases according to the following expression [65],

$$\mathcal{F} = \frac{1}{2} + \frac{1}{1+d}, \quad (2.3)$$

where d is the state dimension. In this chapter, we experimentally investigate high-dimensional optimal quantum cloning and its implications in terms of high-dimensional quantum cryptography [66].

2.3 Quantum metrology

In order to demonstrate the full potential and versatility of high-dimensional states of light, we finish this chapter by exploring a different application of quantum entanglement, namely *quantum metrology*. In particular, quantum metrology exploits

quantum resources in order to perform parameter estimations with a precision going beyond classical statistical limits. For instance, the central limit theorem tells us that statistical errors can be suppressed using a larger number of measurements, where the errors scale inversely with the square root of the number of repeated measurements. However, in quantum mechanics, the limit on the precision of a measurement is dictated by the Heisenberg uncertainty principle, which may result in measurements with larger precision than what is classically allowed. An example of a quantum state that achieves the Heisenberg scaling, i.e. that saturates the Heisenberg uncertainty principle, is known as the N00N state and is given by $(|N, 0\rangle - |0, N\rangle) / \sqrt{2}$, where N photons are distributed between two bosonic modes [67]. Another family of quantum states with metrological potential are known as extremal Majorana constellations, also known as the kings of quantumness. In this chapter, we experimentally investigate the performances of N00N states and extremal Majorana constellations in quantum metrology by taking advantage of a high-dimensionally encoded single photon state, reaching dimensions as high as 21 [68]. In comparison to multi-photon states, high-dimensional quantum states can be generated, manipulated and detected with high fidelities and efficiencies, whereas multi-photon states are still limited to relatively small photon numbers in practice.

QUANTUM MECHANICS

High-dimensional quantum cloning and applications to quantum hacking

Frédéric Bouchard,¹ Robert Fickler,¹ Robert W. Boyd,^{1,2} Ebrahim Karimi^{1,3*}

Attempts at cloning a quantum system result in the introduction of imperfections in the state of the copies. This is a consequence of the no-cloning theorem, which is a fundamental law of quantum physics and the backbone of security for quantum communications. Although perfect copies are prohibited, a quantum state may be copied with maximal accuracy via various optimal cloning schemes. Optimal quantum cloning, which lies at the border of the physical limit imposed by the no-signaling theorem and the Heisenberg uncertainty principle, has been experimentally realized for low-dimensional photonic states. However, an increase in the dimensionality of quantum systems is greatly beneficial to quantum computation and communication protocols. Nonetheless, no experimental demonstration of optimal cloning machines has hitherto been shown for high-dimensional quantum systems. We perform optimal cloning of high-dimensional photonic states by means of the symmetrization method. We show the universality of our technique by conducting cloning of numerous arbitrary input states and fully characterize our cloning machine by performing quantum state tomography on cloned photons. In addition, a cloning attack on a Bennett and Brassard (BB84) quantum key distribution protocol is experimentally demonstrated to reveal the robustness of high-dimensional states in quantum cryptography.

INTRODUCTION

High-dimensional information is a promising field of quantum information science that has matured over the last years. It is known that, by using not only qubits but also qudits, that is, d -dimensional quantum states, it is possible to encode more information on a single carrier, increase noise resistance in quantum cryptography protocols (1), and investigate fundamental properties of nature (2). Photonic systems have been shown to be promising candidates in quantum computation and cryptography for many proof-of-principle demonstrations as well as for “flying” quantum carriers to distribute high-dimensionally encoded states. Orbital angular momentum (OAM) of light, which provides an unbounded state space, has long been recognized as a potential high-dimensional degree of freedom for conducting experiments on the foundations of quantum mechanics (3, 4), quantum computation (5), and cryptography (6). The main characteristic of photons carrying OAM is their twisted wavefront, characterized by an $\exp(i\ell\varphi)$ phase term, where ℓ is an integer and φ is the azimuthal coordinate (7). In the context of quantum information, OAM states of photons have the advantage of representing quantum states belonging to an infinitely large, but discrete, Hilbert space (8). Finite subspaces of dimension d can be considered as laboratory realizations of photonic qudits. Here, we adopt the OAM degree of freedom of single photons to achieve high-dimensional quantum cloning and perform quantum hacking on a high-dimensional quantum communication channel. Although perfect cloning of unknown quantum states is forbidden (9), it is interesting to ask how similar to the initial quantum state the best possible quantum clone can be. The answer is given in terms of the cloning fidelity $\mathcal{F}$, which is defined as the overlap between the initial state to be cloned and that of the cloned copies. This figure of merit is a measure of the accuracy of a cloned copy obtained from a specific cloner. Schemes that achieve the best possible

fidelity are called optimal quantum cloning and play an important role in quantum information (10). For instance, an optimal state estimation yields a bounded fidelity of $\mathcal{F}_{\text{est}} = 2/(1+d)$, where d is the dimension of the quantum state (11). Optimal quantum cloning turns out to be a more efficient way of broadcasting the quantum state of a single system because it yields a fidelity that is always higher than that of optimal state estimation, which has been experimentally realized for low-dimensional photonic states (12–15). Moreover, this enhancement in fidelity grows larger with higher-dimensional quantum states, further motivating experimental investigations of high-dimensional quantum cloning. Hence, high-dimensional optimal quantum cloning machines are of great importance whenever quantum information is to be transmitted among multiple individuals without knowledge of the input quantum state. Here, we concentrate on the $1 \rightarrow 2$ universal optimal quantum cloning machine, for which the optimal fidelity of the two cloned copies is given by $\mathcal{F}_{\text{clo}} = 1/2 + 1/(1+d)$, where d is the dimension of the Hilbert space of the states that are to be cloned (16).

RESULTS

Optimal quantum cloning with OAM states of single photons

We use the symmetrization method to realize a universal optimal quantum cloning machine for high-dimensional OAM states (17, 18). In this method, the quantum state that is to be cloned, namely, $|\psi\rangle$, is sent to one of the input ports of a nonpolarizing beam splitter. In the other input port, a completely mixed state of the appropriate dimension, given by $\hat{\rho}_{\text{mix}} = I_d/d$, is sent, where I_d is the d -dimensional identity matrix. The symmetrization method relies on the well-known two-photon interference effect at a 50:50 beam splitter first proposed by Hong *et al.* (19). When two indistinguishable single photons enter a beam splitter, one into each input port, the photons will “bunch” because of their bosonic nature and exit the beam splitter together through the same output port. This principle is the essence of the symmetrization method for optimal quantum cloning. When both input photons are interfering at the beam splitter, two “cloned” photons will

2017 © The Authors,
some rights reserved;
exclusive licensee
American Association
for the Advancement
of Science. Distributed
under a Creative
Commons Attribution
NonCommercial
License 4.0 (CC BY-NC).

¹Department of Physics, University of Ottawa, 25 Templeton Street, Ottawa, Ontario K1N 6N5, Canada. ²Institute of Optics, University of Rochester, Rochester, NY 14627, USA. ³Department of Physics, Institute for Advanced Studies in Basic Sciences, 45137-66731 Zanjan, Iran.

*Corresponding author. Email: ekarimi@uottawa.ca

jointly exit one of the output ports. We note that this cloning scheme does not require knowledge of the input state and applies to any arbitrary state. This property is a result of the “universality” of the cloning machine and shows the versatility of our scheme. Each state of the output cloned photon is represented by a reduced density matrix obtained by tracing over the other photon. Because both cloned photons are characterized by an identical cloned state, the cloner is thus said to be “symmetric.” Hence, the symmetrization method is considered to be a symmetric optimal universal quantum cloning machine (UQCM). In our experiment, we implement a high-dimensional version of this UQCM with OAM states of single photons (see Fig. 1). We generate and measure the OAM states by manipulating the phase front of the photons using a liquid crystal phase-only spatial light modulator (SLM) (see the Supplementary Materials for a more detailed experimental discussion).

Cloning fidelity

To characterize the quality of our UQCM, we use two different approaches to evaluate the yielding cloning fidelities: measuring the probability of successful cloning and full-state tomography of the cloned photons. In this first series of measurements, we evaluate the cloning fidelity, $\mathcal{F}_\psi$, of a given arbitrary input state, $|\psi\rangle$, from the probability of finding both output cloned photons in

the state $|\psi\rangle$, that is, $\mathcal{P}(|\psi\rangle, |\psi\rangle)$. This probability can be obtained experimentally by means of coincidence measurements: $\mathcal{F}_\psi = \mathcal{P}(|\psi\rangle, |\psi\rangle) = (N(|\psi\rangle, |\psi\rangle) + \sum_{i \neq \psi} N(|\psi\rangle, |i\rangle)) / N_{\text{tot}}$, where $N(|i\rangle, |j\rangle)$ represents the number of coincidence measurements between the states $|i\rangle$ and $|j\rangle$, N_{tot} is the total number of coincidence measurements (that is, $N_{\text{tot}} = N(|\psi\rangle, |\psi\rangle) + 2 \sum_{i \neq \psi} N(|\psi\rangle, |i\rangle)$), and $|i\rangle$ and $|j\rangle$ represent elements of the basis containing $|\psi\rangle$. The factor of 2 that appears in the definition of N_{tot} is a result of the symmetric nature of our cloning machine, where $N(|i\rangle, |j\rangle) = N(|j\rangle, |i\rangle)$. Further, one can obtain from normalization, $\mathcal{P}(|i\rangle, |\psi\rangle) = N(|i\rangle, |\psi\rangle) / N_{\text{tot}}$, for $i \neq \psi$. Here, we note that the optimal cloning fidelity depends on the HOM interference visibility $\mathcal{V}$ through the relation

$$\mathcal{F}(\mathcal{V}) = \frac{1}{2} + \frac{1}{1+d} \left(\frac{2\mathcal{V}}{1+\mathcal{V}} \right)$$

Dimensionality and universality of the cloning machine

Compared to a full tomographic reconstruction, this method requires fewer measurements and thus enables us to characterize the cloning fidelity of our cloner under a wider range of circumstances. For instance, the effect of dimensionality on a UQCM is a crucial point for any optimal cloning schemes. As mentioned previously, increasing the

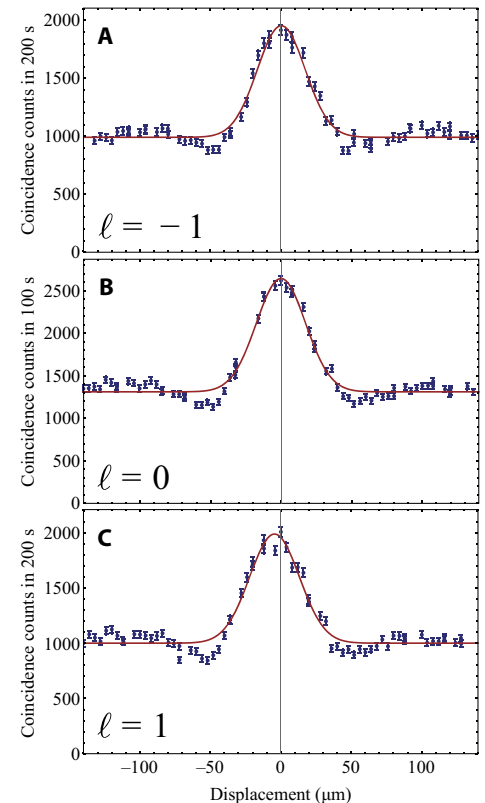
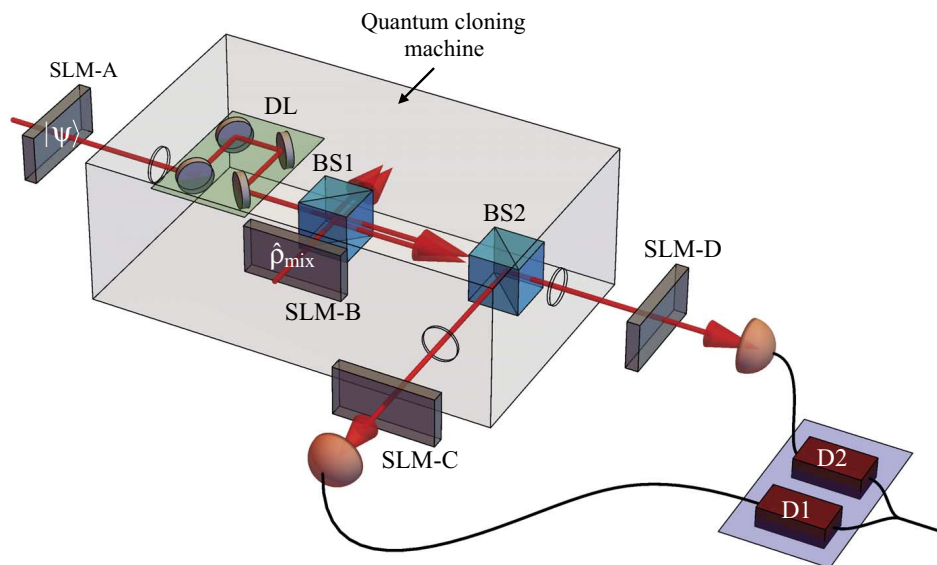


Fig. 1. Simplified sketch of the experimental design. The input quantum state $|\psi\rangle$ is imprinted on a single photon using an SLM-A. The single photon is subsequently sent to the cloning machine for optimal cloning. The cloning machine consists of a delay line (DL), to adjust the arrival time of the input photon, a second photon that is in a completely mixed state when exiting SLM-B, and a first beam splitter (BS1). The two photons are made to arrive at the beam splitter simultaneously using the DL. The two photons exiting one of the output ports of the first beam splitter together are separated at a second beam splitter (BS2) and are sent out of the cloning machine. The cloned photons are then detected and characterized using detectors (D1 and D2) and SLMs (SLM-C and SLM-D), respectively. (A to C) Examples of Hong-Ou-Mandel (HOM) coalescence curves for input photons of $\ell = -1, 0, 1$, respectively (top to bottom). The curve is obtained by recording the coincidences between the output ports of BS2 for various delays of one of the input photons. Examples of enhancement peaks of $R_{\ell=-1} = 1.97 \pm 0.08$, $R_{\ell=0} = 2.02 \pm 0.08$, and $R_{\ell=1} = 1.99 \pm 0.09$ are obtained experimentally, and agree with the theoretical value of $R_{\text{th}} = 2$, corresponding to a visibility of $\mathcal{V} = 1$.

dimensionality of the input quantum states results in a decrease of the cloning fidelity. This decrease in cloning fidelity can serve as an intuitive explanation for the superiority of high-dimensional quantum cryptography. In our experiment, we measure the cloning fidelity of our cloning machine for different input states belonging to the computational OAM basis of various dimensions $d \in \{2, 3, 4, 5, 6, 7\}$. We find near-perfect agreement of the experimentally evaluated cloning fidelities to the theoretical predictions of the high-dimensional $1 \rightarrow 2$ symmetric optimal UQCM (see Fig. 2). In addition, we experimentally verify the universality of our cloning machine by performing quantum cloning of every state of all $d + 1$ OAM mutually unbiased bases (MUBs) (see Fig. 3A) (20, 21). Once more, we find near-optimal cloning fidelities for all MUBs, thus demonstrating the viability and universality of our optimal quantum cloner (see the Supplementary Materials). Note that MUBs and their elements are playing an important role in quantum communication and information, as basis states used in quantum cryptographic protocols (22) and quantum state tomography (23), for example.

Optimal cloning of a Gaussian state

As a second series of measurements for a complete characterization of our UQCM, we fully reconstruct the high-dimensional cloned quantum states by means of quantum state tomography. Moreover,

our UQCM should be able to clone the state regardless of the input state and its complex structure in the high-dimensional state space. An exemplary and visually interesting high-dimensional state is the so-called Gaussian state given by the following superposition

$$|\psi_{\text{Gauss}}\rangle = \mathcal{N} \sum_{\ell=-3}^{\ell=3} \exp[-(\ell/2)^2] |\ell\rangle$$

where $\mathcal{N}$ is a normalization constant. We experimentally generate the Gaussian state of dimension $d = 7$ and perform full quantum state tomography on one of the output cloned photons. The theoretically expected and experimentally achieved results are shown in Fig. 3B. The cloned Gaussian state has a fidelity of 0.80 ± 0.03 with respect to the theoretically expected cloned density matrix. Thus, for an arbitrary complex input state $|\psi_{\text{Gauss}}\rangle$, the experimental cloning fidelity, $\mathcal{F} = \langle \psi_{\text{Gauss}} | \hat{\rho}_{\text{cl}} | \psi_{\text{Gauss}} \rangle$, of our UQCM obtained from complete quantum state tomography can be estimated to be around 0.40 ± 0.01 . In comparison to the average fidelity obtained previously for $d = 7$ of 0.59 ± 0.02 , which we evaluated from success probabilities, the lower fidelity value can be explained by measurement errors and cross-talk among spatial modes for several MUBs. For complete state tomography, these errors have a stronger adverse effect, and a much larger number of measurements (56 measurements in dimension 7),

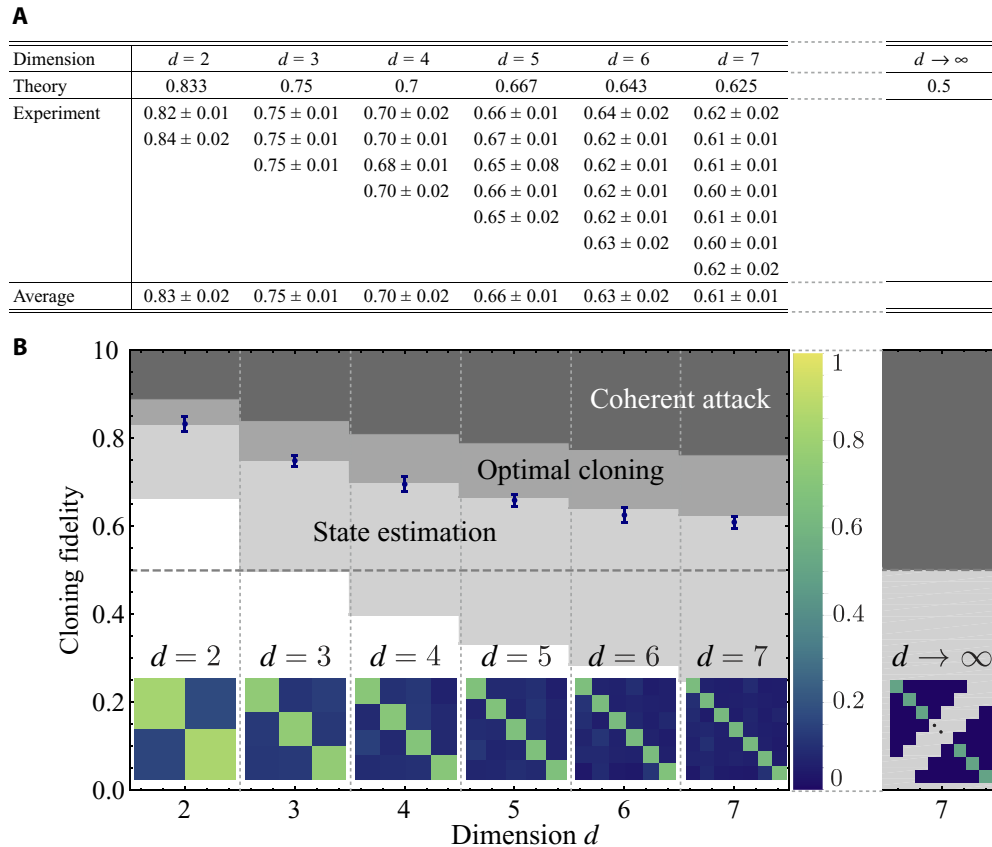


Fig. 2. Optimal cloning fidelity for various dimensions. (A) Experimental values of the cloning fidelities are shown for each d number of elements of the logical basis, along with theoretical values, for various dimensions d . (B) The average cloning fidelities (blue dots) are plotted for various dimensions, along with probability matrices $\mathcal{P}(|j\rangle, |\psi\rangle)$ of detecting a cloned photon in any output state $|j\rangle$ of the OAM logical basis, given an input state $|\psi\rangle$ of the same basis. The diagonal elements of the probability matrices correspond to the cloning fidelity of each element of the basis. The light and dark gray shaded areas correspond to fidelities not accessible by state estimation and $1 \rightarrow 2$ optimal symmetric UQCM, respectively. In quantum cryptography, a more effective class of quantum hacking, namely, coherent attacks (1), yields larger fidelities illustrated by the dim gray shaded area.

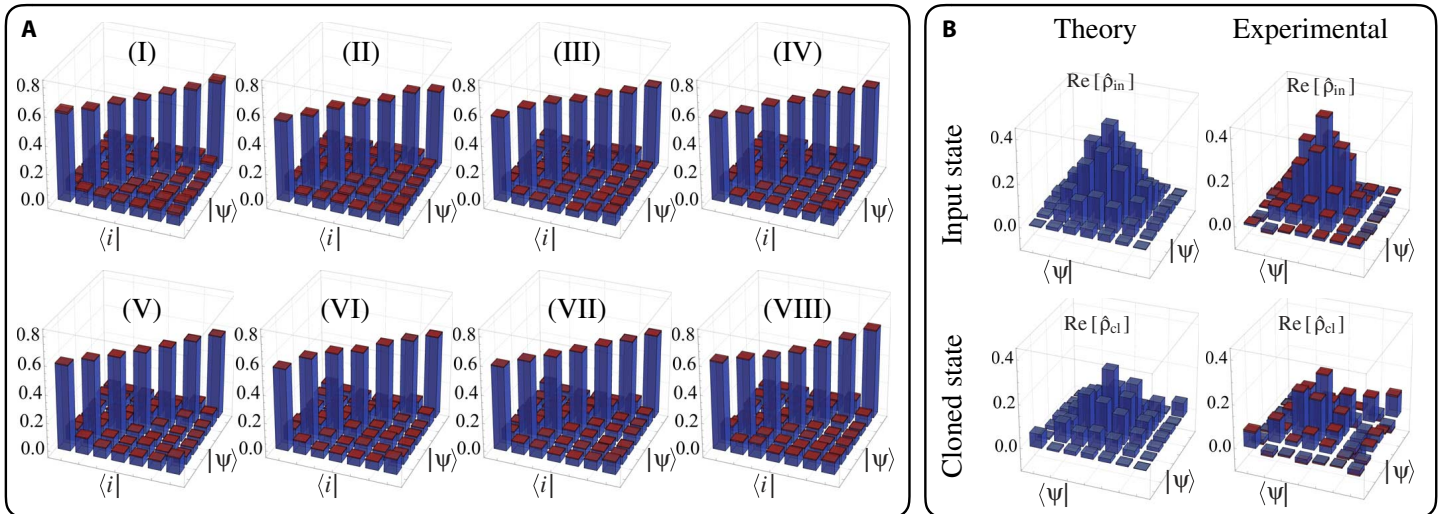


Fig. 3. Cloning fidelities for various MUBs and cloning of Gaussian states in dimension $d = 7$. (A) Probability $\mathcal{P}(|i\rangle, |\psi\rangle)$ of detection of an output cloned state $|i\rangle$ given an input state $|\psi\rangle$, where $|i\rangle$ and $|\psi\rangle$ belong to a specific MUB. This set of measurement is repeated for all $d + 1$ MUBs (I) to (VIII), in dimension 7. The on-diagonal elements represent the cloning fidelities for each element of a given basis. (B) Theoretical and experimental high-dimensional cloning of a Gaussian state. The cloned fidelity is obtained by calculating the overlap of the reduced density matrix of the cloned state with the input state. The experimental reduced density matrix of the cloned state is obtained by full quantum state tomography. The experimentally reconstructed density matrices of the Gaussian state before and after cloning are shown along with their theoretical counterparts.

that is, $d(d + 1)$, are required (see the Supplementary Materials). However, both methods show that our implementation of a symmetric UQCM can be used to clone any arbitrarily complex quantum state up to dimension 7, without a significant deterioration of the optimal state fidelities. Hence, cloning of high-dimensional quantum states encoded in the OAM degree of freedom might become a building block of future high-dimensional quantum information applications.

Cloning attack in quantum cryptography

As a final test of the ability to clone high-dimensional quantum states, we implement a cloning attack into a high-dimensional quantum key distribution (QKD) scheme. In a QKD protocol, a sender (Alice) and receiver (Bob) use quantum states to distribute a random, secret key shared between both parties. The shared key is then used to communicate an encrypted message through a classical channel, using the perfectly secure one-time pad protocol. The security of QKD derives from the fact that the presence of an eavesdropper (Eve) will result in the introduction of errors in the shared key, which can originate, for example, from the nonperfect but optimal cloning done by the eavesdropper (24). Note that the dimensionality of the quantum states used to distribute the key directly affects the cloning fidelity and thus the amount of errors introduced by a possible cloning attack.

We first perform a high-dimensional QKD using the seminal BB84 protocol (22), extended using OAM states of dimension $d = 7$. An eavesdropper with access to a high-dimensional UQCM then performs individual attacks on the QKD channel. In our experiment, the first MUB is given by the logical OAM basis $\{|\ell\rangle; \ell = -3, -2, -1, 0, 1, 2, 3\}$, and the second MUB is given by the Fourier angle basis $\{|\phi_i\rangle; i = 1, 2, 3, 4, 5, 6, 7\}$. Projective measurements are shown with and without the cloning attack in Fig. 4 (A and B), respectively. The lower fidelity due to a cloning attack is readily visible. A visually compelling illustration of the effect of an eavesdropper on Alice and Bob's shared key can be given by directly using the established raw sifted key, without performing further

error correction and privacy amplification, as a one-time pad to share an encrypted message, for example, an image of their favorite optical phenomenon. We experimentally simulate such a situation by performing the high-dimensional BB84 protocol with and without Eve's attack using our UQCM. In a real-world QKD, experimental errors will always be introduced in the raw key, leading to a slightly deteriorated image after Bob's decryption (see Fig. 4A). However, if Eve performs her cloning attack while Alice and Bob are trying to establish their key, the errors increase significantly, which is then directly visible in Bob's decrypted image (see Fig. 4B). The quantum bit error rate (QBER) is given by 0.16 and 0.57, without and with the cloning attack, respectively. In the absence of an eavesdropper, the QBER is well below the error bound for security in dimension 7, that is, $D_{\text{coh}} = 23.72\%$ (1). Thus, error correction and privacy amplification may be performed in order for Alice and Bob to obtain a completely secure and errorless shared key. However, in the presence of the eavesdropper, the QBER is well above the bound in dimension 7, immediately revealing the presence of Eve. Furthermore, the mutual information between Alice and Bob may be calculated from

$$I_{AB}^d = \log_2(d) + (1 - e_B^N) \log_2(1 - e_B^N) + e_B^N \log_2(e_B^N / (d - 1))$$

where e_B^N is Bob's error rate (25). Experimental values of 1.73 and 0.36 bits per photon were obtained for Alice and Bob's mutual information without and with the cloning attack, respectively. In addition, we performed quantum hacking to a two-dimensional QKD protocol (BB84). In this case, the QBER is given by 0.19 and 0.007, with and without the cloning attack, which is well above and below the security bound in dimension 2, that is, $D_{\text{coh}}(2) = 11.00\%$, respectively. Hence, it is clear that high-dimensional quantum cryptography leads to higher signal disturbance in the presence of an optimal cloning attack, resulting in a larger tolerance to noise in the quantum channel.

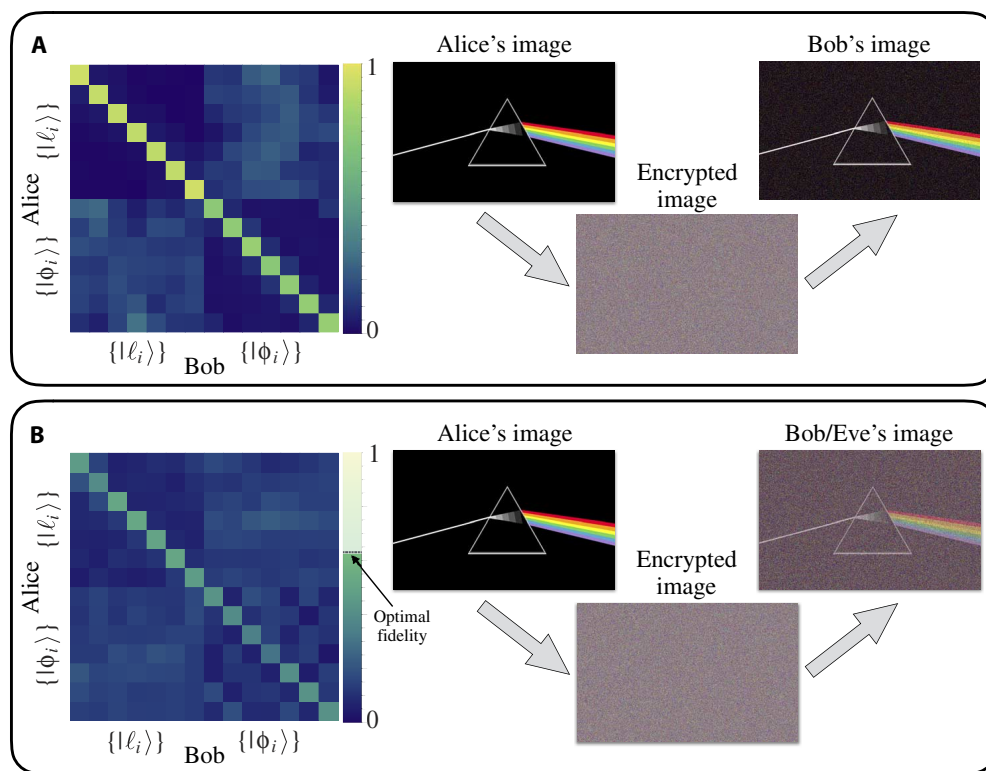


Fig. 4. High-dimensional QKD without and with quantum hacking. (A) Experimental probability matrices obtained from projective measurements are shown on the left side. The bases selected by Alice and Bob are indicated on the vertical and horizontal axes, respectively. On the right, we show Alice's initial message and Bob's decrypted message. (B) Experimental probability matrices with the presence of an eavesdropper having access to a symmetric optimal UQCM. Similarly, Alice's initial message is shown along with the decrypted message obtained by both Bob and Eve. One may note that for the BB84 protocol, the symmetric UQCM does not lead to the optimal individual attack. Rather, our UQCM results in the optimal individual attack for the QKD protocol exploiting all $d + 1$ available MUBs. In the simpler case of the BB84 protocol, the optimal attack consists of the asymmetric Fourier-covariant cloner (1, 26), which cannot be straightforwardly implemented in our experimental setup.

DISCUSSION

In conclusion, we showed the feasibility of high-dimensional optimal quantum cloning of OAM states of single photons. This scheme was further used to perform a cloning attack to a secure quantum channel, revealing the robustness of high-dimensional quantum cryptography upon quantum hacking. Moreover, studying the effect of dimensionality and universality on optimal quantum cloning reveals its advantage over optimal state estimation in quantum information schemes, where unknown quantum states must be distributed.

MATERIALS AND METHODS

The experimental setup can be divided into three parts: a single-photon source, a HOM interferometer, and a cloning characterization apparatus (see fig. S1). Single-photon pairs were generated by the process of spontaneous parametric down-conversion at a nonlinear type I β -barium borate crystal illuminated by a quasi-continuous wave ultraviolet laser operating at a wavelength of 355 nm. The single photons were spatially filtered to the fundamental Gaussian mode by coupling the generated pairs to single-mode optical fibers, with a measured coincidence rate of 30 kHz, within a coincidence time window of 5 ns. The partner photons were each made to illuminate an SLM, to generate the desired photonic states, and subsequently sent at a 50:50 nonpolarizing beam splitter, one at each input port. The path taken by the photons, generated at the nonlinear crystal to get to the beam splitter, must be equidistant for both photons of a given pair to observe the two-photon interference effect. This can be achieved with a precision of tens of micrometers using a

programmable translational stage. Polarizers and interference filters were inserted in the path of each photon. The photons were then made indistinguishable in arrival time, polarization, and frequency. On the other hand, the spatial modes of the photons were kept as a degree of freedom representing photonic quantum states for the UQCM. Following the HOM interference beam splitter, the bunched photons were sent to a second beam splitter, separating them for further coincidence detection. Last, the separated output cloned photons were detected and characterized with SLMs followed by single-mode optical fibers.

SUPPLEMENTARY MATERIALS

Supplementary material for this article is available at <http://advances.sciencemag.org/cgi/content/full/3/2/e1601915/DC1>

Supplementary Text

fig. S1. Detailed experimental setup.

fig. S2. Experimental cloning fidelities for every element of each MUB in dimension 7.

fig. S3. Projective measurements of the input and cloned Gaussian state.

REFERENCES AND NOTES

1. N. J. Cerf, M. Bourennane, A. Karlsson, N. Gisin, Security of quantum key distribution using d -level systems. *Phys. Rev. Lett.* **88**, 127902 (2002).
2. M. Krenn, M. Huber, R. Fickler, R. Lapkiewicz, S. Ramelow, A. Zeilinger, Generation and confirmation of a (100×100) -dimensional entangled quantum system. *Proc. Natl. Acad. Sci. U.S.A.* **111**, 6243–6247 (2014).
3. A. C. Dada, J. Leach, G. S. Buller, M. J. Padgett, E. Andersson, Experimental high-dimensional two-photon entanglement and violations of generalized Bell inequalities. *Nat. Phys.* **7**, 677–680 (2011).

4. J. Harris, F. Bouchard, E. Santamato, W. H. Zurek, R. W. Boyd, E. Karimi, Quantum probabilities from quantum entanglement: Experimentally unpacking the Born rule. *New J. Phys.* **18**, 053013 (2016).
5. F. Cardano, F. Massa, H. Qassim, E. Karimi, S. Slussarenko, D. Paparo, C. de Lisio, F. Sciarrino, E. Santamato, R. W. Boyd, L. Marrucci, Quantum walks and wavepacket dynamics on a lattice with twisted photons. *Sci. Adv.* **1**, e1500087 (2015).
6. M. Mirhosseini, O. S. Magaña-Loaizal, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, R. W. Boyd, High-dimensional quantum cryptography with twisted light. *New J. Phys.* **17**, 033033 (2015).
7. L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, J. Woerdman, Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes. *Phys. Rev. A* **45**, 8185–8189 (1992).
8. G. Molina-Terriza, J. P. Torres, L. Torner, Twisted photons. *Nat. Phys.* **3**, 305–310 (2007).
9. W. K. Wootters, W. H. Zurek, A single quantum cannot be cloned. *Nature* **299**, 802–803 (1982).
10. N. Gisin, S. Massar, Optimal quantum cloning machines. *Phys. Rev. Lett.* **79**, 2153 (1997).
11. D. Bruß, C. Macchiavello, Optimal state estimation for d -dimensional quantum systems. *Phys. Lett. A* **253**, 249–251 (1999).
12. A. Lamas-Linares, C. Simon, J. C. Howell, D. Bouwmeester, Experimental quantum cloning of single photons. *Science* **296**, 712–714 (2002).
13. W. T. M. Irvine, A. L. Linares, M. J. A. de Dood, D. Bouwmeester, Optimal quantum cloning on a beam splitter. *Phys. Rev. Lett.* **92**, 047902 (2004).
14. E. Nagali, L. Sansoni, F. Sciarrino, F. De Martini, L. Marrucci, B. Piccirillo, E. Karimi, E. Santamato, Optimal quantum cloning of orbital angular momentum photon qubits through Hong–Ou–Mandel coalescence. *Nat. Photonics* **3**, 720–723 (2009).
15. E. Nagali, D. Giovannini, L. Marrucci, S. Slussarenko, E. Santamato, F. Sciarrino, Experimental optimal cloning of four-dimensional quantum states of photons. *Phys. Rev. Lett.* **105**, 073602 (2010).
16. P. Navez, N. J. Cerf, Cloning a real d -dimensional quantum state on the edge of the no-signaling condition. *Phys. Rev. A* **68**, 032313 (2003).
17. M. Ricci, F. Sciarrino, C. Sias, F. De Martini, Teleportation scheme implementing the universal optimal quantum cloning machine and the universal NOT gate. *Phys. Rev. Lett.* **92**, 047901 (2004).
18. F. Sciarrino, C. Sias, M. Ricci, F. De Martini, Quantum cloning and universal NOT gate by teleportation. *Phys. Lett. A* **323**, 34–39 (2004).
19. C. K. Hong, Z. Y. Ou, L. Mandel, Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 2044 (1987).
20. T. Durt, B.-G. Englert, I. Bengtsson, K. Życzkowski, On mutually unbiased bases. *Int. J. Quantum Inf.* **8**, 535 (2010).
21. A. Klappenecker, M. Rötteler, Constructions of mutually unbiased bases, in *Finite Fields and Applications* (Springer, 2004), pp. 137–144.
22. C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, paper presented at the International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984.
23. R. B. A. Adamson, A. M. Steinberg, Improving quantum state estimation with mutually unbiased bases. *Phys. Rev. Lett.* **105**, 030406 (2010).
24. K. Bartkiewicz, K. Lemr, A. Černoč, J. Soubusta, A. Miranowicz, Experimental eavesdropping based on optimal quantum cloning. *Phys. Rev. Lett.* **110**, 173601 (2013).
25. W.-H. Zhang, L. Ye, Optimal asymmetric phase-covariant and real state cloning in d dimensions. *New J. Phys.* **9**, 318 (2007).
26. H. Fan, H. Imai, K. Matsumoto, X.-B. Wang, Phase-covariant quantum cloning of qudits. *Phys. Rev. A* **67**, 022317 (2003).

Acknowledgments

Funding: This work was supported by the Canada Research Chairs Program and Canada Foundation for Innovation. F.B. acknowledges the support of the Vanier Canada Graduate Scholarships Program of the Natural Sciences and Engineering Research Council of Canada (NSERC). R.F. acknowledges the support of the Banting postdoctoral fellowship of the NSERC. All authors acknowledge the support of the Max Planck–University of Ottawa Center for Extreme and Quantum Photonics. **Author contributions:** F.B. and E.K. conceived the idea. F.B., R.F., R.W.B., and E.K. designed the experiment. F.B. performed the experiment and analyzed the data. F.B. and E.K. wrote the manuscript with the help from other authors. All authors discussed the results and contributed to the text of the manuscript. **Competing interests:** The authors declare that they have no competing interests. **Data and materials availability:** All data needed to evaluate the conclusions in the paper are present in the paper and/or the Supplementary Materials. Additional data related to this paper may be requested from the authors.

Submitted 13 August 2016

Accepted 14 December 2016

Published 3 February 2017

10.1126/sciadv.1601915

Citation: F. Bouchard, R. Fickler, R. W. Boyd, E. Karimi, High-dimensional quantum cloning and applications to quantum hacking. *Sci. Adv.* **3**, e1601915 (2017).

Quantum metrology at the limit with extremal Majorana constellations

F. BOUCHARD,¹ P. DE LA HOZ,² G. BJÖRK,³  R. W. BOYD,^{1,4} M. GRASSL,⁵ Z. HRADIL,⁶ E. KARIMI,^{1,7,*} 
A. B. KLIMOV,⁸ G. LEUCHS,^{5,1} J. ŘEHÁČEK,⁶ AND L. L. SÁNCHEZ-SOTO^{2,5} 

¹Department of Physics, University of Ottawa, 150 Louis Pasteur, Ottawa, Ontario K1N 6N5, Canada

²Department of Optics, Faculty of Physics, Universidad Complutense, 28040 Madrid, Spain

³Department of Applied Physics, Royal Institute of Technology (KTH), AlbaNova, SE-106 91 Stockholm, Sweden

⁴Institute of Optics, University of Rochester, Rochester, New York 14627, USA

⁵Max Planck Institute for the Science of Light, Staudtstraße 2, 91058 Erlangen, Germany

⁶Department of Optics, Palacký University, 17. listopadu 12, 771 46 Olomouc, Czech Republic

⁷Department of Physics, Institute for Advanced Studies in Basic Sciences, 45137-66731 Zanjan, Iran

⁸Department of Physics, Universidad de Guadalajara, 44420 Guadalajara, Jalisco, Mexico

*Corresponding author: ekarimi@uottawa.ca

Received 30 June 2017; revised 2 October 2017; accepted 21 October 2017 (Doc. ID 301465); published 17 November 2017

Quantum metrology allows for a tremendous boost in the accuracy of measurement of diverse physical parameters. The estimation of a rotation constitutes a remarkable example of this quantum-enhanced precision. The recently introduced Kings of Quantumness are especially germane for this task when the rotation axis is unknown, as they have a sensitivity independent of that axis and they achieve a Heisenberg-limit scaling. Here, we report the experimental realization of these states by generating up to 21-dimensional orbital angular momentum states of single photons, and confirm their high metrological abilities. © 2017 Optical Society of America

OCIS codes: (270.0270) Quantum optics; (270.5585) Quantum information and processing; (120.3940) Metrology.

<https://doi.org/10.1364/OPTICA.4.001429>

The conventional description of the quantum world involves a key mathematical object—the quantum state—that conveys complete information about the system under study; once it is known, the probabilities of the outcomes of any measurement can be predicted. This statistical description entails counterintuitive effects that have prompted several notions of quantumness, yet no single one captures the whole breadth of the physics.

There are, however, instances of quantum states that behave in an almost classical way. The paradigm of such a behavior is that of coherent states of light [1]; they are as much localized as possible in phase space, a property that is preserved under free evolution.

The concept of coherent states has been extended to other physical systems [2]. The case of spin is of paramount importance. The corresponding spin coherent states have minimal uncertainty and they are conserved under rotations. So, in the usual way of speaking, they mimic a classical angular momentum as much as possible. One could rightly wonder what kind of state might serve

as the opposite of a coherent state. The answer will depend on the ways to formalize the idea of being “the opposite” [3]. Here, we take advantage of the Majorana representation, which maps a pure spin S into $2S$ points on the Bloch sphere [4].

It turns out that the Majorana representation of a coherent state consists of a single point (with multiplicity $2S$). At the opposite extreme, we can imagine states whose Majorana representations are spread uniformly over the sphere. The resulting states are precisely the Kings of Quantumness [5,6]. With such symmetric spreadings, the constellations essentially map onto themselves for relatively small rotations around arbitrary axes. This means that they resolve rotations around any axis approximately equally well. We emphasize that the problem of estimating a rotation is of utmost interest in magnetometry [7–9], polarimetry [10,11], and metrology in general [12]. In this work, we experimentally demonstrate the generation of these states and certify their potential for quantum metrology [13].

Let us first set the stage for our experiment. We consider a system that can be described in terms of two independent bosonic modes with creation operators $\hat{a}_\alpha^\dagger$, with $\alpha \in \{+, -\}$. This encompasses many different instances, such as strongly correlated systems, light polarization, Bose–Einstein condensates, and Gaussian–Schell beams, to mention only a few [14]. The Stokes operators for these two-mode systems can be compactly expressed as [15] $\hat{\mathbf{S}} = \frac{1}{2} \hat{a}_\alpha^\dagger \boldsymbol{\sigma}_{\alpha\beta} \hat{a}_\beta$, where $\boldsymbol{\sigma}$ denotes the Pauli matrices, and summation over repeated indices is assumed. One can verify that $\hat{\mathbf{S}}^2 = \hat{S}_0(\hat{S}_0 + 1)$ with $\hat{S}_0 = \hat{N}/2$, and $\hat{N} = \hat{a}_+^\dagger \hat{a}_+ + \hat{a}_-^\dagger \hat{a}_-$ being the total number of excitations.

From now on, we restrict our attention to the case where N is fixed. This corresponds to working in a $(2S + 1)$ -dimensional Hilbert space $\mathcal{H}_S$ of spin S (with $N = 2S$). This space $\mathcal{H}_S$ is spanned by the Dicke basis $|S, m\rangle$, wherein the action of $\hat{\mathbf{S}}$ operators is the standard for an angular momentum. Sometimes, it is preferable to use the two-mode Fock basis $|N_+, N_- \rangle$, related to the Dicke basis by $N_+ = S + m$ and $N_- = S - m$.

Spin coherent states are constructed much in the same way as in the canonical case [2]: they are displaced versions of the north pole of the Bloch unit sphere S_2 . If $\mathbf{n}$ is a unit vector in the direction of the spherical angles (θ, ϕ) , they can be defined as $|\mathbf{n}\rangle = e^{i\phi\hat{S}_z} e^{i\theta\hat{S}_y} |S, S\rangle$. They are not orthogonal, but one can still decompose an arbitrary state $|\Psi\rangle$ using this overcomplete set. The associated coherent-state wave function is $\Psi(\mathbf{n}) = \langle \mathbf{n} | \Psi \rangle$, and the corresponding probability distribution, $Q(\mathbf{n}) = |\Psi(\mathbf{n})|^2$, is nothing but the Husimi function.

The wave function $\Psi(\mathbf{n})$ can be expanded in terms of the Dicke basis $|S, m\rangle$. If the corresponding coefficients are $\Psi_m = \langle S, m | \Psi \rangle$, we obtain $\Psi(\mathbf{n}) = (1 + |z|^2)^{-S} \sum_{m=-S}^S c_m \Psi_m z^{S+m}$, where $c_m = \sqrt{(2S)! / [(S-m)!(S+m)!]}$, and $z = \tan(\theta/2) e^{-i\phi}$ is the complex number derived by the stereographic projection of (θ, ϕ) . Apart from the unessential positive prefactor, this is a polynomial of order $2S$; thus, $|\Psi\rangle$ is determined by the set $\{z_i\}$ of the $2S$ complex zeros of $\Psi(\mathbf{n})$. These zeros, which are also the zeros of $Q(\mathbf{n})$, specify the so-called constellation by an inverse stereographic map of $\{z_i\} \mapsto (\theta_i, \phi_i)$.

Since the spherical harmonics $Y_{Kq}(\mathbf{n})$ are a complete set of orthonormal functions on S_2 , they may be used to expand the Husimi function $Q(\mathbf{n})$. The resulting coefficients, ϱ_{Kq} , are nothing but the standard state multipoles [16], and there are $2S + 1$ of them (see Supplement 1). The monopole is trivial, as it is just a constant term. The dipole indicates the position of the state in the Bloch sphere. When it vanishes, the state has vanishing (first-order) polarization and points nowhere in the mean. If the quadrupole also vanishes, the variance of the state is uniform; i.e., no directional signature can be observed in its second-order fluctuations, and we say that it is second-order unpolarized. Similar interpretation holds for higher-order multipoles. One can also look at these multipoles as the K th directional moments of the state constellation and, therefore, these terms resolve progressively finer angular features.

The quantity $\sum_q |\varrho_{Kq}|^2$ gauges the overlap of the state with the K th multipole pattern. It seems thus suitable to look at the cumulative distribution [17] $\mathcal{A}_M = \sum_{K=1}^M \sum_{q=-K}^K |\varrho_{Kq}|^2$, which concisely condenses the state angular capacity up to order M ($1 \leq M \leq 2S$). Observe that the monopole is omitted, as it is just a constant term.

The spin coherent states $|\mathbf{n}\rangle$ have remarkably simple constellations, just the point $-\mathbf{n}$, and they maximize $\mathcal{A}_M$ for all orders M , confirming yet from another perspective the outstanding properties of these states [5].

In contradistinction, the Kings are those pure states that make $\mathcal{A}_M \equiv 0$ for the highest possible value of M . This means that they convey the relevant information in higher-order fluctuations. The search for these states has been systematically undertaken recently in Ref. [5], where the interested reader can check the details (see also Supplement 1, where one can find the nonzero components Ψ_m of the Kings). The resulting Majorana constellations for some values of S are depicted in Fig. 1. For $S = 3$, the constellation is a regular octahedron and the state is third-order unpolarized ($M = 3$). For $S = 5$, it consists of two pentagons. For $S = 6$ we have the icosahedron, and the corresponding state is fifth-order unpolarized. For $S = 10$ we have a slightly stretched dodecahedron (i.e., the four pentagonal rings that define its vertices are displaced against the pole), and it is fifth-order unpolarized. As we can appreciate, the Kings have the points very symmetrically placed on the unit sphere, so their constellations

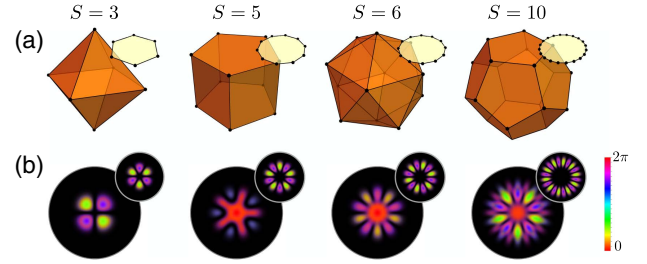


Fig. 1. (a) The Majorana constellations in the Bloch sphere for the Kings (orange) and the NOON states (yellow) corresponding to spin $S = 3, 5, 6$, and 10 . (b) The Laguerre–Gauss representation of the same Kings and NOON states, shown in (a), where the azimuthal index ℓ corresponds to m in the Dicke basis. We consider the fundamental radial mode, i.e., $p = 0$, where p is the radial index of the Laguerre–Gauss modes.

possess many axes along which they return to themselves after a rotation. Consequently, they can resolve relatively small angles around a large number of axes.

Other states with a high degree of angular resolution are the NOON states, given by $|\text{NOON}\rangle = \frac{1}{\sqrt{2}}(|N, 0\rangle - |0, N\rangle)$ in the two-mode Fock basis and $\frac{1}{\sqrt{2}}(|S, S\rangle - |S, -S\rangle)$ in the Dicke basis. As shown in Fig. 1, their Majorana constellation consists of $2S$ equidistantly placed points around the equator of S_2 . A rotation around the z axis of angle $\pi/(2S)$ makes $|\text{NOON}\rangle$ orthogonal to itself, whereas for π/S it returns to itself. This nicely supports the ability of NOON states to detect small rotations.

To compare the performance of these two classes of states, let us assume we have to estimate a rotation $R(\omega, \mathbf{u})$ of angle ω around an axis $\mathbf{u}$ of spherical angles (Θ, Φ) . We consider only small rotations and take the measurement to be a projection of the rotated state onto the original one; i.e., it can be represented by $\hat{P} = |\Psi\rangle\langle\Psi|$. As discussed in Supplement 1, the respective sensitivities (defined as the ratio $\Delta\omega = \Delta\hat{P}/|\partial\langle\hat{P}\rangle/\partial\omega|$, the variance being $\Delta\hat{P} = [\langle\hat{P}^2\rangle - \langle\hat{P}\rangle^2]^{1/2}$) are

$$\Delta\omega_{\text{Kings}} = \frac{\sqrt{3}}{2} \frac{1}{\sqrt{S(S+1)}},$$

$$\Delta\omega_{\text{NOON}} = \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2S^2 \cos^2 \Theta + S \sin^2 \Theta}}. \quad (1)$$

The sensitivity of the Kings is completely independent of the rotation axis and with a Heisenberg-limit scaling $1/S$ for large S . For the NOON states, the sensitivity scales as $1/S$ when $\Theta = 0$, but can be as bad as $1/\sqrt{S}$ when $\Theta = \pi/2$. In short, it is essential to know the rotation axis to ensure that the NOON state is aligned to achieve its best sensitivity.

We stress that the measurement scheme for $\Delta\omega$ involves only second-order moments of $\hat{\mathbf{S}}$. Given their properties, one could expect that detecting higher-order moments will bring out even more advantages of the Kings.

To check these issues, we have generated these extremal states for the cases of $S = 3, 5, 6$, and 10 using orbital angular momentum (OAM) states of single photons [18], which has already proven fruitful in quantum metrology [19]. Working at the single-photon regime is not essential, but it highlights the potential implications for quantum information processing [20]. Therefore, the index m in the Dicke basis is identified with the OAM eigenvalue ℓ of a single photon along its propagation

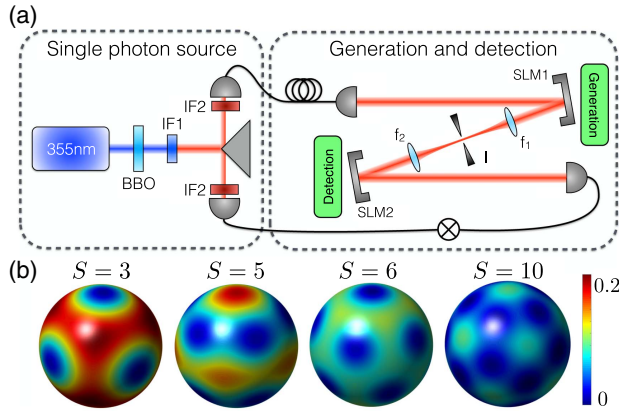


Fig. 2. (a) Sketch of the experimental setup and (b) density plots of the experimentally reconstructed Husimi Q functions for the same King states as in Fig. 1. The fidelities of these reconstructed states are (from left to right) 0.94, 0.87, 0.91, and 0.93. The differences with the theoretical Q functions cannot be visually noticed.

direction. In general, there exist many families of optical modes carrying OAM, but we choose the Laguerre–Gauss basis $LG_{\ell,p}$, where p is the radial index. Since the radial profile is irrelevant to the experimental realization of the Kings states, for the sake of simplicity, we always set the radial index to its fundamental value, i.e., $p = 0$. The resulting transverse profiles of both the Kings and the NOON states are as in Fig. 1(b).

We experimentally create the Kings by means of spontaneous parametric downconversion. A sketch of the experimental setup is shown in Fig. 2(a). A quasi-continuous wave ultraviolet (UV) laser operating with a repetition rate of 100 MHz and an average power of 150 mW at a wavelength of 355 nm is used to pump a type-I β -barium borate crystal. The single photons, signal and

idler, are subsequently coupled to single-mode fibers to filter their spatial mode. One of the photons, the idler, is used as a trigger. The other photon, the signal, is made incident on a first spatial light modulator (SLM1), where the desired quantum states were imprinted on the signal photon holographically [21]. The generated photonic Kings are subsequently imaged onto a second spatial light modulator (SLM2) by a $4f$ system. The second SLM possessing the desired hologram followed by a single-mode optical fiber perform the projective measurement on the state of the signal photon. Both photons are sent to avalanche photodiode detectors (APD), and coincidence counts are recorded by a coincidence box with a coincidence time window of 3 ns [22].

To verify the accurate experimental generation of these states, we perform quantum state tomography to reconstruct the Husimi Q function, as shown in Fig. 2(b). The average fidelity of the resulting states is around 90%; i.e., 94%, 87%, 91%, and 93%, respectively (see Supplement 1).

We now study the behavior of such states under rotations in the sphere S_2 . This is experimentally realized by projective measurements of the Kings onto themselves after a rotation ω around several axes (see Fig. 3). To demonstrate the high sensitivity to rotation of these states along arbitrary axes, we perform such rotations around each axis passing through the Majorana points and facets of the Kings constellations. For the cases of $S = 3, 6$, and 10, we find four-, five-, and three-fold symmetry axes passing through their Majorana points and three-, three-, and five-fold symmetry axes passing through the normals to the facets of their constellations, respectively. Note that, since we are dealing with OAM, these rotations correspond to rather abstract mode transformations, although the polar axis still represents a physical real-space rotation around the optical axis.

Finally, in Fig. 4 we experimentally check the sensitivity of the Kings and NOON states. As we can see, the experimental

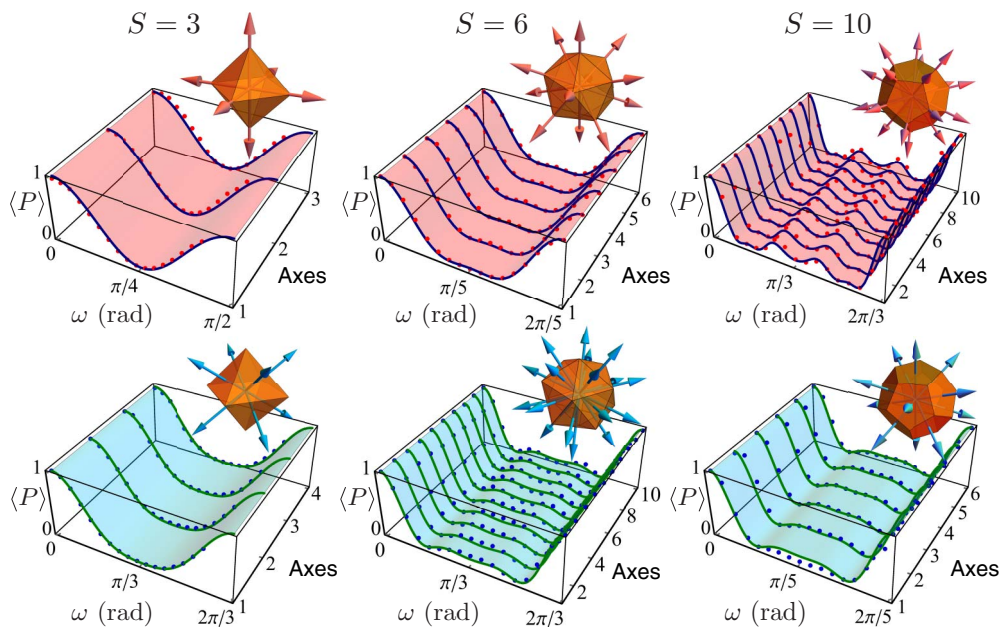


Fig. 3. Experimental results of the projection of the $S = 3, 6$, and 10 (first, second, and third column, respectively) Kings states, $|\Psi^{(S)}\rangle$, onto themselves after a rotation of ω around the axis $\mathbf{u}$, $\hat{R}(\omega, \mathbf{u})$, i.e., $\langle \hat{P} \rangle = |\langle \Psi^{(S)} | \hat{R}(\omega, \mathbf{u}) | \Psi^{(S)} \rangle|^2$. The axes are presented graphically along with the associated constellations. The first row corresponds to rotations along the axes passing through the Majorana points (pink arrows), and the second row corresponds to rotations along the axes normal to the facets of the constellations (blue arrows). The experimental results (red and blue dots) are shown along with the theoretical results (blue and green curves) for all rotation axes.

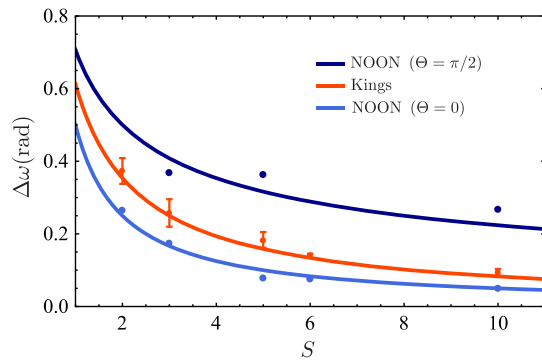


Fig. 4. Rotational sensitivity $\Delta\omega$ for the Kings (red) and NOON states (blue). The solid curves correspond to the theory predicted in Eq. (1), and the points correspond to experimental results. In the case of the Kings, we show the mean rotational sensitivity over all axes presented in Fig. 3, where the error bars correspond to variation in sensitivity from axes to axes. For the NOON states, we show the rotational sensitivity for rotation axes with $\Theta = 0$ and $\Theta = \pi/2$.

sensitivity of the Kings is completely independent of the orientation of the rotation axes (within the error bars). In the limit of small rotation angles, the NOON states overcome the Kings all the way up to $\cos \Theta = 1/\sqrt{3}$. Nonetheless, since the Kings achieve the ideal sensitivity irrespectively of the axis, they are the most appropriate to detect rotation around arbitrary axes.

The problem of the Kings is closely related to other notions as states of maximal Wehrl–Lieb entropy [23], Platonic states [24], the Queens of Quantumness [25], or the Thomson problem [26]. However, there are still many things to elucidate concerning these links. They are, however, a nice illustration of the connections between different branches of science, and on how some seemingly simple problems—distributing points in the most symmetric manner on a sphere—can illuminate such complicated optimization problems that we have just described.

Thus far, efforts were concentrated in estimating the rotation angle, which in terms of magnetometry means that we only want to know the magnetic field magnitude. The Kings will allow for a simultaneous precise determination of the rotation axis (i.e., the magnetic field direction). Our experimental results corroborate that this extra advantage can pave the way to much more refined measurement schemes.

Funding. Natural Sciences and Engineering Research Council of Canada (NSERC); Canada Foundation for Innovation (CFI); Technologická Agentura České Republiky (TAČR) (TE01020229); Grantová Agentura České Republiky (GACR) (15-03194S); Ministerio de Economía y Competitividad (MINECO) (FIS2015-67963-P).

Acknowledgment. F. B. acknowledges the support of the Vanier Canada Graduate Scholarships Program of the Natural Sciences and Engineering Research Council of Canada (NSERC). E. K. acknowledges the support of the Canada Research Chairs (CRC), and Canada Foundation for Innovation (CFI) Programs. F. B., R. W. B., and E. K. acknowledge the support of the Max Planck–University of Ottawa Centre for Extreme and Quantum Photonics. G. B. acknowledges the support of the Wenner–Gren Foundation and the Swedish Research Council (VR) through the Linnaeus Center of Excellence ADOPT.

See Supplement 1 for supporting content.

REFERENCES

1. R. J. Glauber, *Phys. Rev.* **131**, 2766 (1963).
2. A. Perelomov, *Generalized Coherent States and Their Applications* (Springer, 1986).
3. J. Zimba, *Electron. J. Theor. Phys.* **3**, 143 (2006).
4. E. Majorana, *Nuovo Cimento* **9**, 43 (1932).
5. G. Björk, A. B. Klimov, P. de la Hoz, M. Grassl, G. Leuchs, and L. L. Sánchez-Soto, *Phys. Rev. A* **92**, 031801 (2015).
6. G. Björk, M. Grassl, P. de la Hoz, G. Leuchs, and L. L. Sánchez-Soto, *Phys. Scripta* **90**, 108008 (2015).
7. W. Wasilewski, K. Jensen, H. Krauter, J. J. Renema, M. V. Balabas, and E. S. Polzik, *Phys. Rev. Lett.* **104**, 133601 (2010).
8. R. J. Sewell, M. Koschorreck, M. Napolitano, B. Dubost, N. Behbood, and M. W. Mitchell, *Phys. Rev. Lett.* **109**, 253605 (2012).
9. W. Muessel, H. Strobel, D. Linnemann, D. B. Hume, and M. K. Oberthaler, *Phys. Rev. Lett.* **113**, 103004 (2014).
10. V. Meyer, M. A. Rowe, D. Kielpinski, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, *Phys. Rev. Lett.* **86**, 5870 (2001).
11. V. D'Ambrosio, N. Spagnolo, L. Del Re, S. Slussarenko, Y. Li, L. C. Kwek, L. Marrucci, S. P. Walborn, L. Aolita, and F. Sciarrino, *Nat. Commun.* **4**, 2432 (2013).
12. L. A. Rozema, D. H. Mahler, R. Blume-Kohout, and A. M. Steinberg, *Phys. Rev. X* **4**, 041025 (2014).
13. V. Giovannetti, S. Lloyd, and L. Maccone, *Nat. Photonics* **5**, 222 (2011).
14. S. Chaturvedi, G. Marmo, and N. Mukunda, *Rev. Math. Phys.* **18**, 887 (2006).
15. A. Luis and L. L. Sánchez-Soto, *Prog. Opt.* **41**, 421 (2000).
16. K. Blum, *Density Matrix Theory and Applications* (Plenum, 1981).
17. P. de la Hoz, A. B. Klimov, G. Björk, Y. H. Kim, C. Müller, C. Marquardt, G. Leuchs, and L. L. Sánchez-Soto, *Phys. Rev. A* **88**, 063803 (2013).
18. L. Allen, S. M. Barnett, and M. J. Padgett, *Optical Angular Momentum* (Institute of Physics, 2003).
19. D. S. Simon, G. Jaeger, and A. V. Sergienko, *Quantum Metrology, Imaging, and Communication* (Springer, 2017).
20. J. Leach, M. J. Padgett, S. M. Barnett, S. Franke-Arnold, and J. Courtial, *Phys. Rev. Lett.* **88**, 257901 (2002).
21. E. Bolduc, N. Bent, E. Santamato, E. Karimi, and R. W. Boyd, *Opt. Lett.* **38**, 3546 (2013).
22. H. Qassim, F. M. Miatto, J. P. Torres, M. J. Padgett, E. Karimi, and R. W. Boyd, *J. Opt. Soc. Am. B* **31**, A20 (2014).
23. A. Baecklund and I. Bengtsson, *Phys. Scripta* **T163**, 014012 (2014).
24. P. Kolenderski and R. Demkowicz-Dobrzanski, *Phys. Rev. A* **78**, 052333 (2008).
25. O. Giraud, P. Braun, and D. Braun, *New J. Phys.* **12**, 063005 (2010).
26. J. J. Thomson, *Philos. Mag.* **7**(39), 237 (1904).

Chapter 3

Characterization of high-dimensional quantum states and processes

This chapter is based on the following papers:

1. **F. Bouchard**, N. H. Valencia, F. Brandt, R. Fickler, M. Huber, & M. Malik, “Measuring azimuthal and radial modes of photons”, *Optics Express* **26**, 31925 (2018).

DOI: <https://doi.org/10.1364/OE.26.031925>

© 2018 Optical Society of America

2. **F. Bouchard**, F. Hufnagel, D. Koutný, A. Abbas, A. Sit, K. Heshami, R. Fickler, & E. Karimi, “Quantum process tomography of a high-dimensional quantum communication channel”, *Quantum* **3**, 138 (2019).

DOI: <https://doi.org/10.22331/q-2019-05-06-138>

© 2019 Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften

3.1 Detection of spatial modes

In chapter 2, we have discussed different techniques to generate OAM modes, or more generally, spatial modes. In the case of OAM modes, only the phase must be manipulated, making their generation straightforward using refractive devices, or birefringent liquid-crystal devices based on holography or geometric phases, i.e. SLM and q -plates, respectively. More generally, for the case of spatial modes, the phase and intensity must be manipulated. Although lossy, an SLM can be used to manipulate the intensity and phase of an incoming beam by using a filtering holographic technique, known as amplitude-masking [69, 70].

Interestingly, the task of detecting spatial modes turns out to be more challenging than their generation. In particular, detection schemes can be classified into two categories, i.e. single-outcome measurement and multi-outcome measurements. In analogy to polarization, a polarizer would consist of a single-outcome measurement, whereas a polarizing beam splitter (PBS) consists of a multi-outcome measurement, where detectors can be placed in both output ports of the PBS. For OAM modes, the single-outcome measurement, or projective measurement, is known as *phase-flattening* [71] and has become the standard experimental tool to measure OAM modes. Even though phase-flattening possesses a slight mode-dependent efficiency [72], its mode fidelity is extremely high in practice. On the other hand, multi-outcome measurement schemes, known as *sorting*, have been proposed and experimentally demonstrated using interferometric configurations [73] and diffractive elements [74, 75, 76, 24]. Generally speaking, sorting typically results in lower mode fidelities, but benefits from an overall larger detection efficiency.

Nevertheless, in order to take advantage of the full transverse spatial modes of photons, one must take into account the full-field profile LG beams, namely both the azimuthal OAM modes and the radial modes [77, 78, 79]. Recently, several experimental schemes have been proposed to sort radial modes of light [80, 81, 82, 83, 84]. Nevertheless, these techniques yield non-optimal experimental mode fidelities. In the first part of this chapter, we propose a projective measurement technique that allows one to measure radial modes, or more generally, any arbitrary spatial modes with extremely high mode fidelities [85]. Due to the analogy with phase-flattening, we have named our measurement technique *intensity-flattening*, which can be seen as an extension of phase-flattening to the case of arbitrary spatial modes.

3.2 Quantum state tomography

In the previous section, we have reviewed the several measurement techniques that can be employed to detect spatial modes of single photons. Nevertheless, it is well-known that the full characterization of a single quantum state is prohibited by the uncertainty principle. Rather, in order to characterize a quantum state, the experimenter considers an ensemble of identically prepared states and subsequently performs measurements in different bases. From this set of measurements, the experimenter may reconstruct the quantum state using a technique called *quantum state tomography* (QST). Moreover, the number of identically prepared states to be measured is inversely proportional to the statistical errors of the reconstructed quantum state.

3.2.1 Density matrix

In particular, the object that is used to describe a quantum state is known as the *density matrix*. The density matrix, or density operator, is a $d \times d$ matrix, that can be represented as,

$$\hat{\rho} = \sum_{i=0}^{d-1} p_i |\psi_i\rangle \langle \psi_i|, \quad (3.1)$$

where p_i are real and positive numbers, and $|\psi_i\rangle$ corresponds to a complete and orthonormal set of states that diagonalizes the density matrix, $\hat{\rho}$. A density matrix is said to be pure if it can be written as $\hat{\rho} = |\psi\rangle \langle \psi|$, where the purity is defined as $P = \text{Tr}[\hat{\rho}^2]$. In the other extreme case, we have the completely mixed state given by $\hat{\rho} = \frac{1}{d} \sum_{i=0}^{d-1} |\psi_i\rangle \langle \psi_i|$, where the completely mixed state has the particularity of having the same representation in all bases.

In the experimental reconstruction of the density matrix using QST, several physical properties of the density matrix must be taken into consideration: (1) unit trace, (2) Hermitian, and (3) positive semidefinite. These conditions can be written formally as the following,

$$\text{Tr}[\hat{\rho}] = 1 \quad (3.2)$$

$$\hat{\rho} = \hat{\rho}^\dagger \quad (3.3)$$

$$\langle \psi | \hat{\rho} | \psi \rangle \geq 0, \quad \forall |\psi\rangle. \quad (3.4)$$

Physically, these properties can be understood as (1) the quantum state being normalized, and the probabilities being (2) real and (3) positive numbers.

3.2.2 Quantum state tomography of a qubit

Let us start by introducing QST for a qubit, using the example of polarization. In order to perform QST, one must perform a set of tomographically complete, or informationally complete, measurements, meaning that the corresponding outcome probabilities are sufficient to determine an arbitrary state. Overcomplete measurements, where the number of measurements is larger than the minimum number of measurement necessary to identify the quantum state, are often used to their simplicity or stability in experimental implementations. An example of an overcomplete set of measurements for polarization qubits is given by the following set of projective measurements: $\{\hat{\Pi}_H, \hat{\Pi}_V, \hat{\Pi}_A, \hat{\Pi}_D, \hat{\Pi}_L, \hat{\Pi}_R\}$, with corresponding outcome probabilities P_H, P_V, P_A, P_D, P_L , and P_R , respectively, where $\hat{\Pi}_\psi$ corresponds to a projective measurement of the state $|\psi\rangle$, i.e. $|\psi\rangle\langle\psi|$. The Stokes parameters can then be obtained from the outcome probabilities, i.e. $S_0 = P_L + P_R$, $S_1 = P_H - P_V$, $S_2 = P_A - P_D$, and $S_3 = P_L - P_R$. Finally, the density matrix may now be reconstructed using different techniques. The first technique is known as a direct inversion, i.e.

$$\hat{\rho} = \frac{1}{2} \sum_{i=0}^3 \frac{S_i}{S_0} \hat{\sigma}_i, \quad (3.5)$$

where $\hat{\sigma}_0$ is the 2×2 identity matrix, and $\hat{\sigma}_1, \hat{\sigma}_2, \hat{\sigma}_3$ are the Pauli matrices. The advantage of using a direct inversion method is that the density matrix may be directly obtained without needing the use of an optimization software. By taking a closer look, we find that two of the physical properties of the density matrix are naturally embedded in the direct inversion, namely that it is unit trace and Hermitian. However, this reconstruction does not guarantee the positive semidefiniteness of the density matrix. To avoid this problem, another reconstruction technique, known as the maximum likelihood estimation (MLE) method has been developed [86]. In the MLE technique, one starts with a parametrized initial physical density matrix that is unit trace, Hermitian, and positive semidefinite by construction. A numerical optimization is then carried out in order to find the parametrized density matrix that yields measurement outcomes that are the closest to the experimental measurement outcomes. Nevertheless, using MLE can also lead to systematic errors in the tomographic reconstruction [87].

3.2.3 High-dimensional quantum state tomography

QST can be extended to the case of high-dimensional states. In particular, there are several ways to generalize the expression in Eq. 3.5 to larger dimensions. The first pathway to high-dimensional QST is by generalizing the Pauli Matrices using the Gell-Mann matrices. Generalized Gell-Mann matrices are $d \times d$ matrices forming an orthogonal and complete basis, i.e. any $d \times d$ density matrix can be represented as a linear combination of the Gell-Mann matrices. The orthogonality relation for Gell-Mann matrices is given by $\text{Tr}[\hat{\sigma}_i \hat{\sigma}_j] = 2\delta_{ij}$, where δ_{ij} is the Kronecker delta symbol. Explicitly, the Gell-Mann matrices are given by the following expressions

$$\hat{\sigma}_0 = \hat{I} \quad (3.6)$$

$$\hat{\sigma}_{j,k}^X = |j\rangle\langle k| + |k\rangle\langle j| \quad (3.7)$$

$$\hat{\sigma}_{j,k}^Y = -i(|j\rangle\langle k| - |k\rangle\langle j|) \quad (3.8)$$

$$\hat{\sigma}_r^Z = \sqrt{\frac{2}{r(r+1)}} \left[\left(\sum_{j=0}^{r-1} |j\rangle\langle j| \right) - r|r\rangle\langle r| \right], \quad (3.9)$$

where i is the imaginary unit, j and k are indices that run from 0 to $d-1$, and r is an index that runs from 1 to $d-1$.

In analogy to Eq. (3.5), the reconstructed density matrix in dimension d is given by the following expression,

$$\hat{\rho} = \frac{1}{d} \left(S_0 \hat{\sigma}_0 + \sum_{j,k \in \{0,1,\dots,d-1\}, j \neq k} (S_{j,k}^X \hat{\sigma}_{j,k}^X + S_{j,k}^Y \hat{\sigma}_{j,k}^Y) + \sum_{r=1}^{d-1} S_r^Z \hat{\sigma}_r^Z \right), \quad (3.10)$$

where the generalized high-dimensional Stokes parameters are given by,

$$S_0 = 1 \quad (3.11)$$

$$S_{j,k}^X = P_{\frac{1}{\sqrt{2}}(|j\rangle+|k\rangle)} - P_{\frac{1}{\sqrt{2}}(|j\rangle-|k\rangle)} \quad (3.12)$$

$$S_{j,k}^Y = P_{\frac{1}{\sqrt{2}}(|j\rangle+i|k\rangle)} - P_{\frac{1}{\sqrt{2}}(|j\rangle-i|k\rangle)} \quad (3.13)$$

$$S_r^Z = \sqrt{\frac{2}{r(r+1)}} \left[\left(\sum_{j=0}^{r-1} P_{|j\rangle} \right) - r P_{|r\rangle} \right]. \quad (3.14)$$

We notice that in order to perform high-dimensional QST using this method, one needs to perform projective measurements in the computational basis and on qubit-like states of the form $(|j\rangle \pm |k\rangle)/\sqrt{2}$ and $(|j\rangle \pm i|k\rangle)/\sqrt{2}$, where $j, k = 0, 1, \dots, d-1$ and $j \neq k$. In dimension d , this results in an overcomplete set of $(2d^2 - d)$ measurements. For practical reasons, it is not advantageous to employ this method with

spatial modes due to the large number of measurements and lack of symmetry of the projective measurements.

As an alternative, it is possible to employ mutually unbiased bases (MUB) to perform high-dimensional QST. Formally, MUB consist of a set of orthonormal and complete bases $\{\mathcal{B}_\alpha\}$, where $\mathcal{B}_\alpha = \{\hat{\Pi}_m^{(\alpha)}\}$, $\hat{\Pi}_m^{(\alpha)} = |\psi_m^{(\alpha)}\rangle\langle\psi_m^{(\alpha)}|$ is a MUB element, $m = 0, 1, \dots, d-1$ labels the state, and $\alpha = 0, 1, \dots, d$ labels the MUB. The orthonormality and completeness relations for MUB elements are respectively given by, $\sum_{\alpha=0, m=0}^{d, d-1} \hat{\Pi}_m^{(\alpha)} / (d+1) = \hat{I}$ and $\text{Tr} [\hat{\Pi}_m^{(\alpha)} \hat{\Pi}_n^{(\beta)}] = \delta_{\alpha\beta} \delta_{mn} + (1 - \delta_{\alpha\beta})/d$. The reconstructed density matrix can then be obtained by direct inversion using the following expression,

$$\hat{\rho} = \sum_{\alpha=0}^d \sum_{m=0}^{d-1} P_m^{(\alpha)} \hat{\Pi}_m^{(\alpha)} - \hat{I}, \quad (3.15)$$

where $P_m^{(\alpha)} = \text{Tr} [\hat{\rho} \hat{\Pi}_m^{(\alpha)}]$ are the experimentally obtained outcome probabilities. MUB measurements, although overcomplete, require a smaller number of measurements compared to the previous method, namely $d(d+1)$ measurements. Nevertheless, a major limitation of high-dimensional QST with MUB is the fact that MUB are known only for dimensions that are powers of prime numbers. Therefore, for dimensions as small as $d = 6$, it is not possible to use MUB to perform high-dimensional QST. Finally, for prime dimensions, the MUB elements take a simple form for the case of $\alpha \geq 1$,

$$|\psi_m^{(\alpha)}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} (\omega_d^m)^{d-j} \left(\omega_d^{-(\alpha-1)} \right)^{s_j} |j\rangle, \quad (3.16)$$

where $\omega_d = \exp(2\pi i/d)$ and $s_j = j + \dots + (d-1)$.

3.3 Quantum process tomography

QST represents an invaluable tool for experimenters wanting to reconstruct and characterized quantum states. Interestingly, there is an analogous technique allowing the experimenter to characterize a *quantum process*. This technique is known as quantum process tomography (QPT) [88]. In particular, a quantum process is a completely positive map $\mathcal{E}$ that takes a density matrix $\hat{\rho}_{\text{in}}$ as an input and outputs a density matrix $\hat{\rho}_{\text{out}}$, i.e. $\hat{\rho}_{\text{out}} = \mathcal{E}(\hat{\rho}_{\text{in}})$. The simplest example of a quantum process is a unitary transformation, where $\mathcal{E}$ takes the form of $\mathcal{E}(\hat{\rho}) = \hat{U}\hat{\rho}\hat{U}^\dagger$. Interestingly, there

is a nice analogy that can be drawn between quantum processes and quantum states, where the unitary transformation is the quantum process analogue of the pure state. Furthermore, a more general object, the density matrix which naturally incorporates mixed states, is necessary to describe a general quantum state. The analogue of a density matrix for quantum processes is a $d^2 \times d^2$ matrix known as the *process matrix*, which can be used to describe more general de-cohering processes and noisy channels.

A general quantum process can be described as a linear combination of Kraus operators actions, i.e.

$$\mathcal{E}(\hat{\rho}) = \sum_i \hat{A}_i \hat{\rho} \hat{A}_i^\dagger, \quad (3.17)$$

where the operators $\hat{A}_i$ fully describe the quantum process, in the same way the coefficients p_i fully describes a quantum state $\hat{\rho} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. Nevertheless, it is convenient to describe the quantum process with a single matrix rather than with a set of operators. This can be done by choosing a fixed set of operators with convenient properties such as completeness and orthogonality, e.g. the Pauli matrices or Gell-Mann matrices in higher dimensions. Thus, the operators $\hat{A}_i$ are expanded as $\hat{A}_i = \sum_m a_{im} \hat{\sigma}_m$. The quantum process may now be written as,

$$\mathcal{E}(\hat{\rho}) = \sum_{m,n} \chi_{mn} \hat{\sigma}_m \hat{\rho} \hat{\sigma}_n, \quad (3.18)$$

where $\chi_{mn} = \sum_i a_{im} a_{in}^*$ is the known as the process matrix. Similar to the density matrix, the process matrix must fulfill three physical properties: (1) trace-preserving, (2) Hermitian, and (3) positive semidefinite. The trace-preserving condition is explicitly given by, $\sum_{mn} \chi_{mn} \hat{\sigma}_m \hat{\sigma}_n = \hat{I}$, where $\hat{I}$ here is the d^2 identity matrix. Finally, it is by no coincidence that QST and QPT look so similar. Hence, there is a mathematical relation, known as the *Choi-Jamiołkowski isomorphism* that formally links both objects, namely the quantum state and the quantum process, i.e.

$$\hat{\rho}_{\mathcal{E}} = \left(\hat{I} \otimes \mathcal{E} \right) |\Phi\rangle\langle\Phi|, \quad (3.19)$$

where $\hat{\rho}_{\mathcal{E}}$ is a $d^2 \times d^2$ density matrix known as the Choi matrix and $|\Phi\rangle$ is d -dimensional maximally entangled state.

In the second part of this chapter, we experimentally perform QPT in dimensions ranging from 2 to 5 [89]. Furthermore, we show that all measurements recorded while performing QPT can be used to enhance the performance and security of quantum cryptography. In particular, we find that the advantage of performing QKD using a QPT scheme becomes more advantageous in larger dimensions.



Measuring azimuthal and radial modes of photons

FRÉDÉRIC BOUCHARD,^{1,*} NATALIA HERRERA VALENCIA,^{2,3}
FLORIAN BRANDT,^{2,4} ROBERT FICKLER,² MARCUS HUBER,² AND
MEHUL MALIK^{2,4}

¹Department of Physics, University of Ottawa, 25 Templeton Street, K1N 6N5, Ottawa, Canada

²Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmannngasse 3, A-1090 Vienna, Austria

³Université d' Aix-Marseille, Centre de Saint-Jérôme, 13014, Marseille, France

⁴Institute of Photonics and Quantum Sciences (IPaQS), Heriot-Watt University, EH14 4AS, Edinburgh, UK

Abstract: With the emergence of the field of quantum communications, the appropriate choice of photonic degrees of freedom used for encoding information is of paramount importance. Highly precise techniques for measuring the polarisation, frequency, and arrival time of a photon have been developed. However, the transverse spatial degree of freedom still lacks a measurement scheme that allows the reconstruction of its full transverse structure with a simple implementation and a high level of accuracy. Here we show a method to measure the azimuthal and radial modes of Laguerre-Gaussian beams with a greater than 99 % accuracy, using a single phase screen. We compare our technique with previous commonly used methods and demonstrate the significant improvements it presents for quantum key distribution and state tomography of high-dimensional quantum states of light. Moreover, our technique can be readily extended to any arbitrary family of spatial modes, such as mutually unbiased bases, Hermite-Gauss, and Ince-Gauss. Our scheme will significantly enhance existing quantum and classical communication protocols that use the spatial structure of light, as well as enable fundamental experiments on spatial-mode entanglement to reach their full potential.

Published by The Optical Society under the terms of the [Creative Commons Attribution 4.0 License](#). Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

1. Introduction

Photons have long been a candidate of choice for many proof-of-principle experiments in quantum communications, quantum information processing, and foundations of quantum mechanics [1]. For several decades, due to its maturity in generation and detection, the polarization of photons has now become a standard experimental resource for fundamental and applied experiments, and, to this day, is still being used in a wide array of important experimental demonstrations [2–4]. Nevertheless, other photonic degrees of freedom, such as frequency and time [5,6] or position and momentum [7], offer new, yet unexploited advantages where polarization encoding is limited. One advantage of these degrees of freedom is their high-dimensional nature, whereas polarization is inherently bidimensional, i.e. *qubits*. High-dimensional quantum systems, also known as *qudits*, are both interesting at the fundamental level and useful in applications such as quantum communications and cryptography [8,9], offering an increased information capacity and greater resistance to noise [10].

A specific family of spatial modes that has gained a lot of attention in the last years is the azimuthal modes of Laguerre-Gauss (LG) beams. In particular, it was found that such solutions of the paraxial wave equation are related to an orbital angular momentum (OAM) proportional to the azimuthal mode index ℓ [11] and are characterized by a twisted helical wavefront of the form $\exp(i\ell\varphi)$, where φ is the azimuthal coordinate. Mathematically, these solutions have the

advantage of representing a set of complete and orthogonal functions, thus forming a convenient basis to expand any arbitrary azimuthal functions. Experimentally, OAM modes have been a fruitful testbed for experimental demonstrations in quantum entanglement [12, 13], quantum simulation [14] and QKD [15–17]. Due to their simple form, OAM states are readily generated using devices that shape the wavefront of an incoming beam. Spiral phase plates [18], pitch-fork gratings [19], spatial light modulators (SLM) [20], and q -plates [21] are examples of established devices to generate light beams carrying OAM. Nevertheless, none of the aforementioned techniques directly generate pure LG modes, due to difficulties in manipulating their radial component. Therefore, several generation techniques have been proposed and implemented for experimentally achieving pure LG modes. Among these, holographic amplitude-masking techniques modulating the amplitude and phase of a beam using a single phase-only SLM, although lossy, have been a useful experimental tool to generate any arbitrary desired modes with high precision [22, 23]. For instance, the amplitude modulated holograms may be straightforwardly displayed on an SLM, thus making the generation of LG modes simple and compact for table-top experiments.

Although the generation of spatial modes is relatively simple to realize, it is surprisingly not the case for their detection. A technique known as *phase-flattening* has been demonstrated and become the standard for measuring OAM states of light [24]. In this scheme, the incoming OAM beam that is to be measured is impinged onto a phase element and subsequently coupled to a single-mode fibre (SMF). For the detection of a given OAM value, a phase pattern with the opposite OAM is imprinted on the SLM, thereby flattening the phase of the incoming beam and allowing it to couple efficiently to the SMF. In all other cases, the resulting beam after the phase modulation will not match the fundamental mode of the SMF. In this way, the phase-flattening method can be used as a filter to measure the OAM content of an unknown incoming beam. This technique also possesses limitations where mode-dependent losses renders the detection of higher-order OAM states less efficient [25]. Nevertheless, phase-flattening has now become a standard method for measuring OAM and is also widely used in experiments utilizing OAM both in the classical and the quantum regime. In another approach, it is possible in principle to measure any arbitrary spatial modes with high accuracy using a large enough sequence of phase elements and free-space propagation separating the elements. For example, with this configuration, a mode sorter was realized using two phase elements [26, 27], namely an unwrapper and a phase corrector. A sorter-type scheme has the advantage of being able to measure the OAM value of the incoming beam in a single shot, rendering the detection scheme more efficient. Moreover, when considering a larger number of phase elements, a larger flexibility allows one to perform a measurement over a much larger number of modes [28] or to carry out mode transformations [29]. However, as the number of phase elements increases, small imperfections in alignment leads to significant mode cross-talks and limits the practicality of such implementations.

Here, we propose and experimentally demonstrate a method that we refer to as *intensity-flattening*. Our method extends the well-established phase-flattening method and enables us to measure arbitrary spatial modes using a simple experimental configuration that requires a single hologram. With a reasonable amount of loss, our method enables us to measure spatial modes with extremely small crosstalk values corresponding to a visibility larger than 99 %. This technique will be useful for fundamental, proof-of-concept experiments and all tasks where high-quality measurements are necessary and losses can be tolerated.

2. Theory

Let us set the stage by writing out the orthogonality condition for the Laguerre-Gauss functions, i.e.

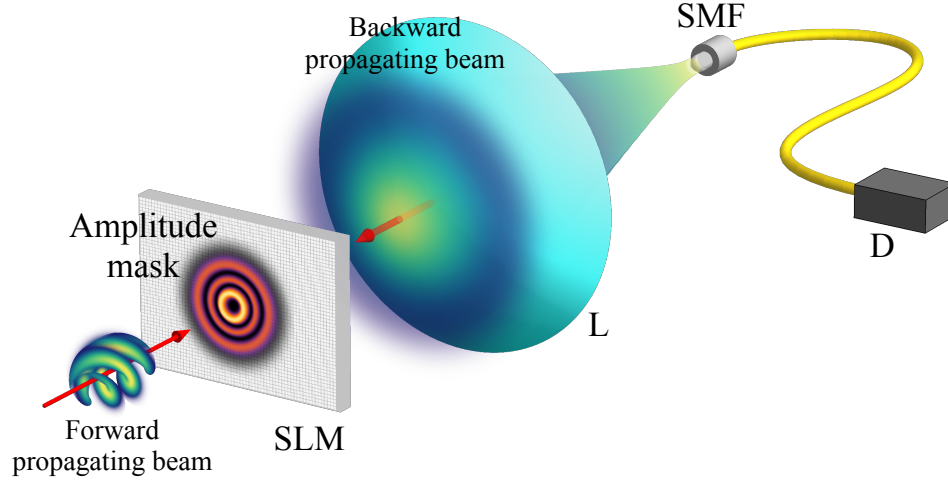


Fig. 1. Simplified experimental setup. A forward-propagating beam with an unknown spatial mode is made incident on a spatial light modulator (SLM). A hologram simultaneously modulating the phase and the amplitude of the incoming beam is displayed on the SLM. Subsequently, the outgoing beam is coupled to a single-mode fibre (SMF) after passing through a set of lenses and microscope objectives (not shown). The choice of lenses can be understood by considering a back-propagating beam exiting the SMF and made incident on the SLM from the back. According to the intensity-flattening technique presented here, this beam should be expanded on the SLM in order to flatten the intensity distribution of the Gaussian component.

$$\int_0^{2\pi} \int_0^{\infty} \text{LG}_{\ell',p'}^*(r, \varphi) \text{LG}_{\ell,p}(r, \varphi) r dr d\varphi = \delta_{\ell\ell'} \delta_{pp'}. \quad (1)$$

In the laboratory, an input LG beam, $\text{LG}_{\ell,p}(r, \varphi)$, is generated using the previously mentioned amplitude-masking method on a first SLM. The beam is now made incident on a second SLM which is displaying the mode $\text{LG}_{\ell',p'}^*(r, \varphi)$, also using the amplitude-masking technique. Finally, the beam is made to couple to an SMF and the coupled intensity or photon counts are recorded. Due to the unitarity of free-space propagation, we have the freedom to choose at which point we calculate the overlap integral after the SLMs. Thus we imagine a backward propagating beam from the SMF to the second SLM. This experimental scenario corresponds to the overlap integral,

$$\int_0^{2\pi} \int_0^{r_{\max}} \text{LG}_{\ell',p'}^*(r, \varphi) \text{LG}_{\ell,p}(r, \varphi) e^{-r^2/w_0^2} r dr d\varphi \neq \delta_{\ell\ell'} \delta_{pp'}, \quad (2)$$

where $r_{\max}$ takes into account finite numerical apertures in the experiment and w_0 is the beam waist of the SMF. We note that this integral is different from the overlap integral of LG modes, Eq. (1), due to the additional gaussian factor of the SMF [30,31]. The aim of our method is to remove the effect of this Gaussian factor to retrieve the standard orthogonality relation of LG beams. A simple but very effective way of achieving this, is by increasing the value of the backward propagating beam waist, w_0 , in Eq. (2). For a large enough w_0 , from the perspective of the LG terms in the integral, the additional Gaussian factor will appear flat over the region of interest, thus retrieving Eq. (1). This intensity-flattening technique requires minimal

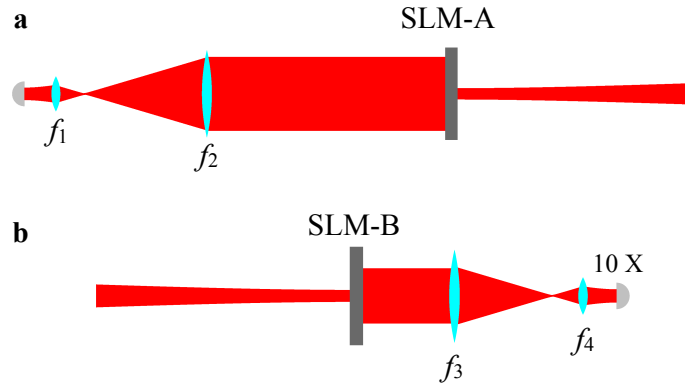


Fig. 2. Experimental details. (a) An attenuated laser diode is enlarged using a telescope with a magnification of $f_2/f_1 = (300 \text{ mm})/(50 \text{ mm}) = 6$. The beam is then made incident on a first spatial light modulator (SLM-A) which reflects the incoming beam (shown in transmission here for simplicity). The output beam has the desired intensity and phase profile after passing through a $4 - f$ system that filters out the first order of diffraction (not shown here). (b) The beam that is to be measured is made incident on SLM-B. By considering a virtually backward-propagating beam from the 10X object, the set of lenses $f_3 = 200 \text{ mm}$ and $f_4 = 50 \text{ mm}$ magnifies the backward-propagating by a factor of 4, making its beam waist much larger than the beam waist of the detection mode on the SLM-B.

modifications to standard experimental setups measuring optical spatial modes, and allows one to select the appropriate trade-off between mode visibility and losses by tuning the beam waist, see Fig. 1. In order to demonstrate this powerful idea experimentally, we build a simple experimental setup allowing us to test our intensity-flattening method in several scenarios – measuring radial modes, key rates in QKD, and quantum state tomography. We also investigate and compare the performance of the intensity-flattening technique when considering beams other than Gaussian, such as flat-top and exponential, which can be seen in the appendix-a.

3. Experimental setup

An attenuated diode laser at a wavelength of 810 nm is coupled to an SMF to clean its spatial profile to the fundamental Gaussian mode. The beam is coupled out of the SMF using a collimator resulting in a beam with a $1/e^2$ beam waist of 1.1 mm, which is then enlarged using a telescope with a magnification of $f_2/f_1 = (300 \text{ mm})/(50 \text{ mm}) = 6$, where f_1 and f_2 are the focal length of the first and the second lens in the telescope, respectively. The large collimated beam is made incident on SLM-A where the desired spatial mode is generated using an amplitude-masking technique [23]. The beam waist of the mode displayed on SLM-A is given by $w_0 = 500 \mu\text{m}$. A $4f$ -system is then used in order to filter out the first order of diffraction and to image SLM-A onto SLM-B. The beam is then sent through a second telescope with a magnification of $f_4/f_3 = (50 \text{ mm})/(200 \text{ mm}) = 0.25$ and then coupled to an SMF using a 10-X microscope objective. The choice of f_3 and f_4 becomes clearer when considering the backward-propagating beam, (Fig. 1), where the effect of the telescope is to enlarge the size of the backward-propagating beam on SLM-B to 4.2 mm, hence increasing the beam waist of the Gaussian factor in Eq. (2). A more detailed experimental setup is shown in Fig. 2.

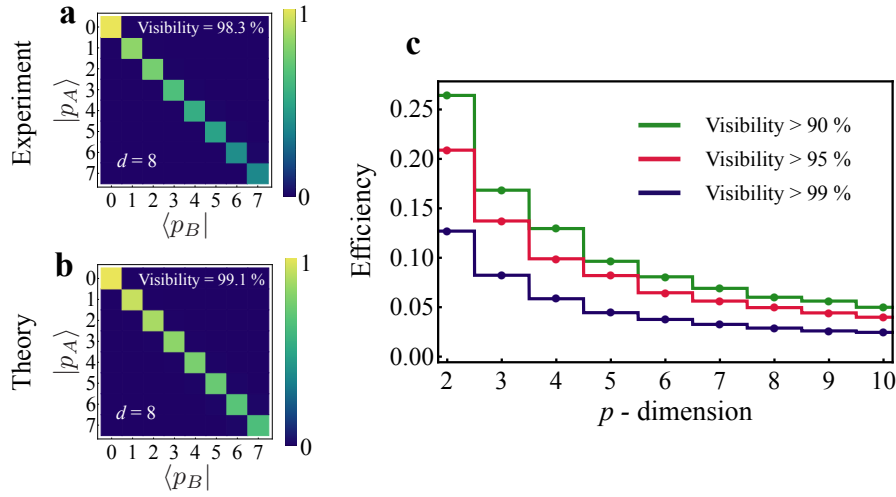


Fig. 3. Measurement of radial modes. (a) Experimentally measured and (b) simulated cross-talk matrix of radial modes ranging from $p = 0$ to $p = 7$ in a prepare-and-measure setting. The cross-talk matrix is normalized to unity by dividing each elements by the element with maximum counts. The rows and the columns correspond to the states, $|p_A\rangle$ and $|p_B\rangle$, prepared and measured by Alice and Bob, respectively. A visibility of $V = 98.3\%$ is obtained from the experimentally measured cross-talk matrix. In theory, a visibility in excess of 99 % is achieved by considering a back-propagating with a beam waist 5.4 times larger than that of the beam waist of the detection mode of the holograms. (c) The efficiency of the intensity-flattening measurement technique is shown as a function of dimensionality of radial modes. For a dimension of d , radial modes ranging from $p = 0$ to $p = d - 1$ are considered. For each dimensions, the reported efficiencies are obtained by increasing the beam waist of the back-propagating up to the point where visibilities are in excess of 99 % (dark blue), 95 % (red) and 90 % (green).

4. Radial modes

As a first experimental demonstration of our technique, let us consider the radial modes of the LG beams. These modes have recently been investigated both theoretically and experimentally in the context of quantum information [31–35] and play a key role in fully utilizing the information-carrying capacity of a photon. Since then, several experimental techniques have been proposed to measure radial modes in a sorter configuration, i.e. using a scattering medium [36] or taking advantage of the p -dependent Gouy phase in an interferometric configuration [37,38]. Such schemes have the advantage of having a higher detection efficiency in principle compared to a filter-type measurement as we propose. Nevertheless, in the first case, low transmission efficiencies prohibit its use in a realistic quantum experiment and in the second case, the stability and interferometric nature of the implementation makes these techniques challenging. In contrast, our method has the advantage of being simple, compact and stable for measuring radial modes. In order to demonstrate the quality of measurements achievable with our method, we measure the cross-talk among radial modes ranging from $p = 0$ to 7 using our intensity-flattening technique, see Fig. 3. The modal cross-talk is characterized by considering the visibility of the cross-talk matrix, which we define as $V = \sum_i C_{ii} / \sum_{ij} C_{ij}$, where C_{ij} corresponds to the cross-talk matrix. For an 8-dimensional radial mode subspace, we experimentally obtain a visibility value of $V = 98.3\%$, which is the highest experimentally achieved value so far reported (to the best of our knowledge).

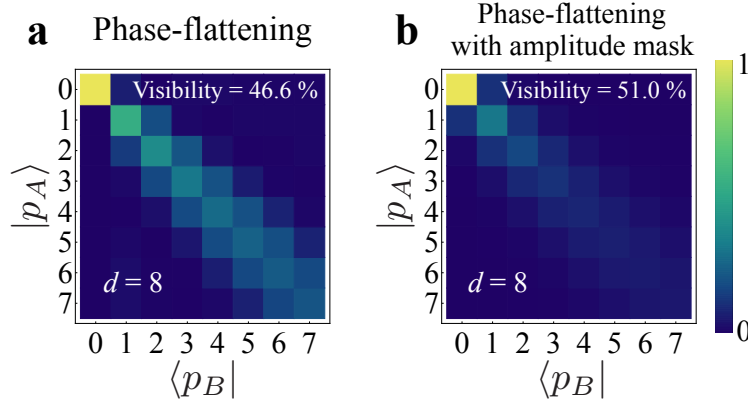


Fig. 4. Performance of phase-flattening in measuring radial modes. Simulated cross-talk matrix of radial modes measurement with (a) a phase-flattening measurement scheme and (b) a phase-flattening with amplitude mask measurement scheme.

We note that we may observe a mode-dependent efficiency in our measurements, which is attributed to the overall transmission of the amplitude mask due to the geometry of the imprinted modes, as well as the coupling to the SMF. This effect is also seen from the theory, see Fig. 3-(b), and can be straightforwardly compensated for. In order to achieve a visibility of 98.3 %, the beam waist of the virtually backward propagating beam has been chosen to be 8.4 times larger than the beam waist of the generation and measurement holograms. We experimentally measured the average efficiency of detection to be 3.2 %, for radial modes ranging from $p = 0$ to 7, where losses due to the amplitude mask and coupling to the single mode fibre are taken into account. In theory, for an 8-dimensional radial mode subspace, a visibility in excess of 99 % is achieved by enlarging the backward-propagating beam by a factor of 5.4.

By varying the size of the back-propagating beam on SLM-B we may achieve, in theory, arbitrarily high visibility values at the cost of an increase in loss. However, we demonstrate that high visibility may still be achieved with reasonable losses, rendering this technique useful for a broad range of experiments. In general, when considering higher-order modes and thus larger dimensional states, enlarged beam waists w_0 must be considered for a similar visibility value. In order to show this effect, we calculate the detection efficiency resulting from increasing the beam waist of the back-propagating beam for obtaining visibility values that are larger than 90 %, 95 % and 99 %, for several dimensions of radial subspaces, see Fig. 3-(c). We note that in the case of a 10-dimensional subspace, i.e. $p = 0$ to 9, a visibility larger than 99 % is achieved with an efficiency of 2.5 %, which is often tolerable in quantum information processing as well as classical application tasks. For the case of spontaneous parametric downconversion, coincidence count rates, summed over all modes, on the order of 10^5 Hz may be expected for a typical implementation [12]. If one were to use the intensity-flattening technique to measure pairs of entangled photons, coincidence count rates on the order of 10^2 to 10^3 Hz can be expected. We further note that our technique has the advantage of allowing the user to vary w_0 at will in order to obtain a certain visibility for a tolerable efficiency.

In order to compare our intensity-flattening with a previously established measurement technique, we investigate the performance of phase-flattening in measuring radial modes. In particular, we consider two strategies where the beam waist of the backward-propagating beam is fixed to w_0 , where w_0 is the beam waist of the generated and detected modes on the holograms of the spatial light modulators (SLM). In the first case, a phase-only hologram is employed at the

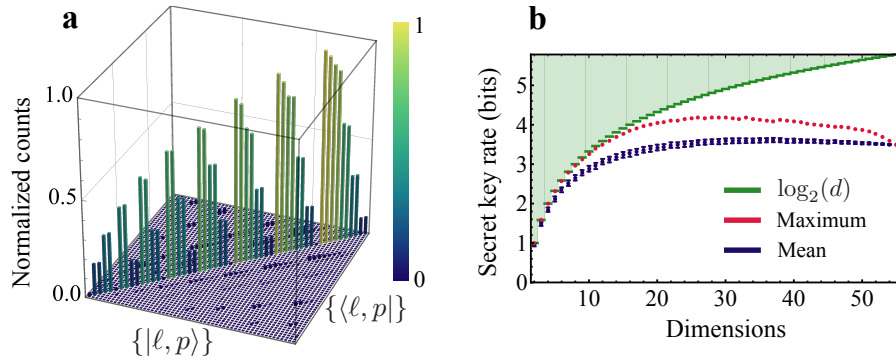


Fig. 5. Measurement of a 55-dimensional space using azimuthal and radial modes. (a) Experimentally measured cross-talk matrix for a 55-dimensional space of azimuthal and radial modes. In order to show mode-dependent efficiencies, the cross-talk matrix is normalized to unity by dividing each elements by the element with maximum counts. The list of states $\{|\ell, p\rangle\}$ are given explicitly in the appendix-c. (b) Secret key rates obtained from lower dimensional subspaces of the full 55-dimensional space. For a given subspace, a sample of 1000 different combinations is selected. For each combination of subspaces, a secret key rate is calculated from the experimental data. The mean and the standard deviation of the secret key rates over the 1000 combinations are shown in dark blue. The maximal secret key rates obtained by searching for the optimal subspace using a genetic algorithm are shown in red. The theoretical maximal values are shown in green, given by $\log_2(d)$. The shaded region corresponds to values of secret key rates inaccessible for the corresponding dimensions.

detection SLM. The corresponding phase of the mode to detect is displayed flattening the phase of the outgoing beam. However, the overlap of the phase-flattened beam with the single mode fibre leads to a modal cross-talk in the measurement of radial modes. In dimension 8, a visibility of $V = 46.6\%$ is obtained from the calculated cross-talk matrix of radial modes, see Fig. 4-(a).

Another possible strategy that we consider involves an amplitude mask, where the backward propagating beam's waist is also fixed to w_0 . This technique also leads to a large modal cross-talk and mode-dependent losses. Nevertheless, in dimension 8, a visibility of $V = 51.0\%$ is obtained from a calculated cross-talk matrix of radial modes, achieving a slightly higher visibility than the phase-only flattening technique, see Fig. 4-(b).

5. Full-field modes

As a second demonstration of our intensity-flattening method for measuring spatial modes, we consider the full-field structure of spatial modes, i.e. the joint azimuthal and radial degrees of freedom. The transverse spatial degree of freedom inherently requires two spatial coordinates to characterize the transverse plane, e.g. x and y in cartesian coordinates, or r and φ in polar coordinates. Thus in order to take full advantage of transverse spatial modes, it is becoming increasingly important to take into consideration both the azimuthal and radial modes when dealing with LG beams [39, 40]. However, due to the lack of a proper technique to measure arbitrary spatial modes in a feasible experimental implementation, only a few experiments have investigated azimuthal and radial modes jointly for quantum entanglement [12, 41] and for classical communications [42]. We now demonstrate how our intensity flattening can be applied in a full-field experiment by measuring states of light in both azimuthal and radial modes.

It has been shown repeatedly that high-dimensional states of light have various applications in

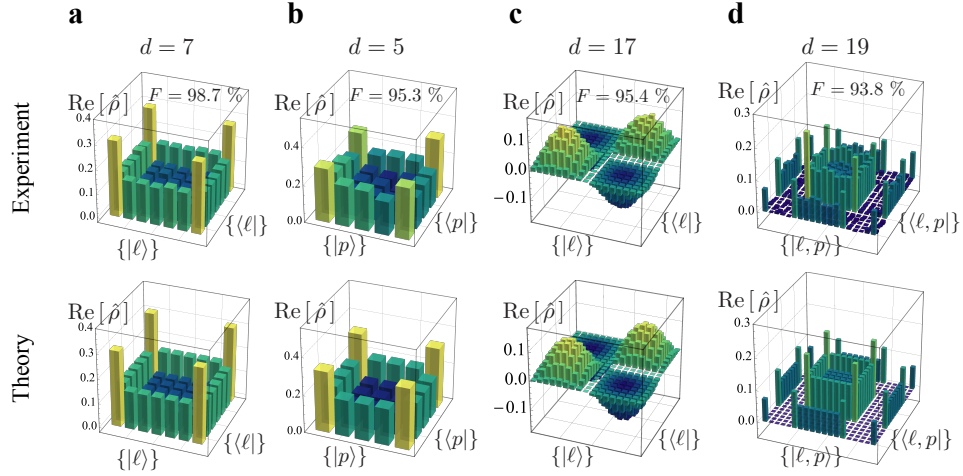


Fig. 6. High-dimensional quantum state tomography. The experimentally reconstructed density matrices for a (a) 7-dimensional OAM state, (b) 5-dimensional radial state, (c) 17-dimensional OAM state and (d) 19-dimensional full-field state, are shown in the upper row along with their corresponding theory density matrices, respectively. High-dimensional states giving rise to visually interesting density matrices were chosen in order to resemble (a)-(b) a castle, (c) a sine function, and (d) a palace, where the explicit forms of the generated states are given in appendix-d. Fidelities of $F = 98.7\%$, 95.3% , 95.4% , and 93.8% , and efficiencies of 4.7% , 5.5% , 8.3% , and 6.6% were obtained experimentally for (a)-(d), respectively.

quantum information. However, in any experimental implementations, one is rapidly confronted with the trade-off between higher dimensions and obtaining high quality measurements [12, 43]. Therefore, for a given quantum information protocol, the optimal dimensionality in experiments dealing with spatial mode is rarely the highest achievable dimension. This is commonly due to the fact that higher-order spatial modes typically result in lower measurement quality due to the complexity of the modes, pixel resolutions, or truncation due to a finite numerical aperture. By taking advantage of the mode order given by $N = 2p + |\ell| + 1$, we consider a 55-dimensional space consisting of the 55 lowest order azimuthal and radial LG modes with mode order ranging from $N = 1$ to 10, see appendix-c for the list of states employed. A visibility of 92.3% is experimentally obtained from the full 55-dimensional cross-talk matrix presented in Fig. 5-(a).

As mentioned previously, there is a trade-off in experiments between dimensionality and visibility. We now explore this interplay by considering lower dimensional subsets of the 55-dimensional cross-talk matrix shown in Fig. 5-(a). An example of a physical parameter that illustrates the trade-off between the dimensionality and the visibility is the secret key rate in a high-dimensional QKD setting. For example, the secret key rate of the high-dimensional BB84 protocol [8] is given by $R = \log_2(d) - 2h^{(d)}(e_b)$, where e_b is the quantum bit error rate and $h^{(d)}(x) := -x \log_2(x/(d-1)) - (1-x) \log_2(1-x)$ is the d -dimensional Shannon entropy. Although we do not perform QKD and only measure in the computational basis, the secret key rate formula provides us with a simple and useful parameter that takes both dimensionality and measurement errors into consideration. For a d -dimensional subset of the 55-dimensional space, there are a total of $55!/(55-d)!d!$ combinations of possible subspaces. In Fig. 5-(b), we show the average and the standard deviation of the secret key rates obtained from a set of 1000 randomly selected d -dimensional subspaces from all possible combinations. Moreover, for a given d -dimensional subspace, we search for combination of states that yields the largest secret

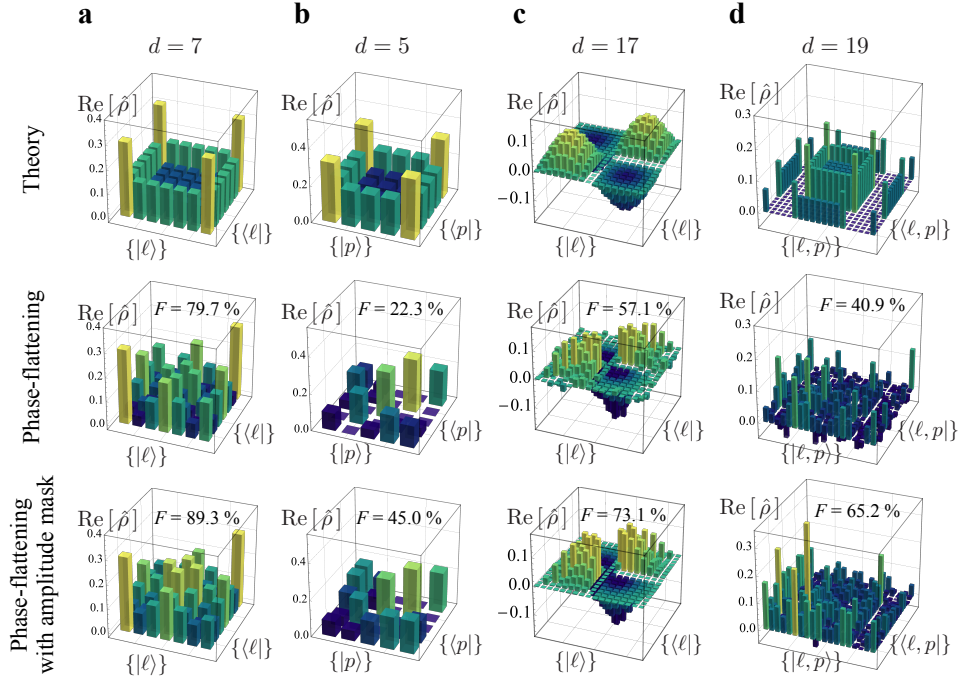


Fig. 7. Simulated tomographically reconstructed density matrices using the phase-flattening-only and the phase-flattening with amplitude masking methods. We show the tomographic reconstruction of (a) the 7-dimensional OAM castle state, (b) the 5-dimensional radial castle state, (c) the 17-dimensional OAM sine state, and (d) the 19-dimensional full-field palace state.

key rates. However, in some cases, the number of possible combinations becomes extremely large, e.g. for a 27-dimensional subset of the 55-dimensional data, there are a total of 3.8×10^{15} possible subsets. Thus, we perform an optimization, consisting of a genetic algorithm, to search among the d -dimensional subsets for the optimal secret key rates, see appendix-c. The maximal secret key rate is found to be 4.19 bits in a 30-dimensional subspace, corresponding to a visibility of 96.8 %, which is well above the error bounds for coherent eavesdropping attacks [8]. The maximum secret key rates found by the genetic algorithm are, on average, 4 standard deviations larger than the mean values from the random sampling. By doing so, we show another aspect of the potential of high-dimensional states for quantum information protocols by allowing for the careful selection of a lower dimensional subset of the complete data.

6. High-dimensional state tomography

As a final test of the versatility and effectiveness of our method, we take on the demanding task of performing high-dimensional quantum state tomography (QST). In particular, we perform our tomographic reconstruction using mutually unbiased bases (MUBs), which are known for dimensions that are power of prime numbers [44]. The measurements of MUBs is an important task in many high-dimensional quantum information protocols, such as QKD [45], channel characterization [46], and high-dimensional entanglement certification [47].

We start by performing QST of a 7-dimensional OAM space. As a non-trivial state to produce in the laboratory, we consider states that are visually interesting, see Fig. 6. In order to avoid

Table 1. Comparison of Intensity-Flattening and Phase-Flattening for Measuring Azimuthal and Radial Modes.

Measurements	d	Intensity-flattening (Experiment)	Phase-flattening (Simulation)	Phase-flattening (AM) (Simulation)
Crosstalk - Radial modes	8	$V = 98.3 \%$	$V = 46.6 \%$	$V = 51.0 \%$
Secret key rate - Full-field	30	$R = 4.19$ bits	$R = 1.34$ bits	$R = 0.92$ bits
QST - Radial modes	5	$F = 95.3 \%$	$F = 22.3 \%$	$F = 45.0 \%$
QST - Azimuthal modes	17	$F = 95.4 \%$	$F = 57.1 \%$	$F = 73.1 \%$
QST - Full-field modes	19	$F = 93.8 \%$	$F = 40.9 \%$	$F = 65.2 \%$

systematic errors in our tomographic reconstruction [48], we experimentally reconstruct the density matrix using a direct inversion given by $\hat{\rho} = \sum_{\alpha, m} P_m^{(\alpha)} \Pi_m^{(\alpha)} - \hat{\rho}$, where α labels the MUB, m labels the state, $P_m^{(\alpha)}$ corresponds to the probability of measuring the state $|\psi_m^{(\alpha)}\rangle$ from the MUB α and $\Pi_m^{(\alpha)}$ corresponds to the projector $|\psi_m^{(\alpha)}\rangle\langle\psi_m^{(\alpha)}|$. The experimental generation and reconstruction may be evaluated using the state fidelity given by $F = \left(\text{Tr} \sqrt{\sqrt{\hat{\rho}} \hat{\rho}_{\text{th}} \sqrt{\hat{\rho}}} \right)^2$, which reduces to $F = \langle \psi_{\text{th}} | \hat{\rho} | \psi_{\text{th}} \rangle$ in our case since $\hat{\rho}_{\text{th}}$ are pure states. The experimentally reconstructed 7-dimensional OAM state is shown in Fig. 6-(a), along with its theoretical counterpart. The state fidelity is given $F = 98.7 \%$, which shows the high measurement quality of our method for OAM states.

While several techniques have been proposed to measure radial modes, there has been no experimental demonstration of measurements of MUBs for radial modes. To demonstrate the extent of the capability of the intensity-flattening technique, we perform QST of a 5-dimensional state consisting of radial modes ranging from $p = 0$ to $p = 4$ using MUBs. The experimentally reconstructed density matrix, with a corresponding state fidelity of $F = 95.3 \%$, is shown in Fig. 6-(b). We note that the highest radial mode, i.e. $p = 4$, corresponds to a mode order of $N_{\text{max}} = 9$. As a comparison, we also perform QST on a 17-dimensional OAM state, where the highest OAM value is $|\ell| = 8$, corresponding to a maximal mode order of $N_{\text{max}} = 9$ as well, see Fig. 6-(c). Even in such large dimensions, a relatively high state fidelity of 95.4 % is achieved. Finally, we perform QST on a 19-dimensional state of combined azimuthal and radial modes, see Fig. 6-(d). A state fidelity of $F = 93.8 \%$ is obtained from the full-field QST showing the full experimental power of our technique.

We now compare the performance of our intensity-flattening method to the previously established phase-flattening method for measuring radial modes of light. In order to compare their performances in terms of azimuthal modes, we simulate the performance of quantum state tomography when using the phase-flattening-only and phase-flattening with amplitude masking techniques. As can be seen from Fig. 7, the state fidelities are significantly lower compared to the case of intensity-flattening, as shown in the main text. As expected, the measurements are particularly bad when measuring radial modes. However, with OAM states that lack certain symmetries, as it is the case here for the *castle*, *sine*, and *palace states*, the phase-flattening technique also performs poorly even when measuring azimuthal modes. Finally, prior to performing QST, we experimentally characterized the coupling efficiency of each measurement setting on SLM-B to compensate for the mode-dependent efficiency associated with intensity-flattening.

Table 1 summarizes how our intensity-flattening technique compares with the well-established phase-flattening methods (with and without amplitude masking), when applied to radial mode

crosstalk, QKD key rates achievable, and QST of high-dimensional states. Different sets of measurements are compared in terms of visibility (V), secret key rate (R), and state fidelity (F) for several different dimensions (d). The comparison is carried out among intensity-flattening (experimental), phase-flattening (simulated), and phase-flattening with amplitude-masking (simulated). As can be seen, the intensity-flattening method enables significant improvements on all fronts, including a four-fold increase in key rates and vastly better tomographic state fidelities.

7. Conclusion

In conclusion, we have proposed and experimentally demonstrated an intensity-flattening technique which enabled us to projectively measure arbitrary spatial modes with a high level of accuracy. Our method uses a single phase screen, and has the advantage of being simple and straightforward to implement, making it a powerful experimental tool for quantum and classical experiments with the spatial modes of light. In order to demonstrate the versatility of our technique, we have measured radial modes with higher visibilities than ever before – 98.3 % in an 8-dimensional state space. Moreover, we have characterized extremely large high-dimensional states with high visibility by combining the azimuthal and radial modes of LG beams, thus taking advantage of the full information capacity of transverse spatial modes. Finally, as an ultimate test of the generality of this technique, we have performed quantum state tomography on high-dimensional azimuthal and radial modes with significant improvements in fidelity over previous measurement techniques. By enabling the precise measurement of the azimuthal and radial modes of light, our method opens a pathway towards practical quantum and classical communication protocols with record information capacities and levels of security.

Appendix-A

Beam shaping of the backward-propagating beam: In the main text, we have primarily investigated intensity-flattening with a Gaussian backward propagating beam, which is given by the output of the single mode fibre (SMF). However, by manipulating the phase in conjugate planes of the outgoing Gaussian beam, we may shape with high-efficiency the Gaussian beam into a flat-top or an exponential beam at the detection SLM. The flat-top and exponential beams are respectively defined as,

$$E_{\text{ft}}(r, \varphi) = \begin{cases} \frac{1}{w_0} \sqrt{\frac{1}{\pi}} & \text{if } r \leq w_0 \\ 0 & \text{if } r > w_0 \end{cases} \quad (3)$$

$$E_{\text{exp}}(r, \varphi) = \frac{1}{w_0} \sqrt{\frac{2}{\pi}} \exp(-r/w_0). \quad (4)$$

For instance, the flat-top beam has the advantage of being flatter over a certain region of space, compared to the Gaussian beam. However, the fixed extent of the flat-top beam becomes problematic for the higher-order modes that have non-zero intensity at larger radii. On the other hand, the exponential beam is less flat near the origin, but has a larger extent than the Gaussian beam for larger radii. In general, a super-Gaussian beam of the form $\exp(-(r/w_0)^n)$, may be considered by varying the parameter n by optimizing the trade-off between visibility and efficiency for a given dimension. Indeed, the flat-top, Gaussian and exponential beams are all special cases of super-Gaussian beams with $n = \infty, 2$ and 1 , respectively. In Fig. 8, we compare the performance of the previously mentioned beam shapes for measurements of radial modes in dimension 5 and 10. In particular, in dimension 10, for visibilities ranging from $V = 0.98$ to 1, the flat-top beam is more efficient. In the range, $V = 0.83$ to 0.98 , the Gaussian beam is more efficient and finally in the range between $V = 0$ and 0.83 , exponential beams are more

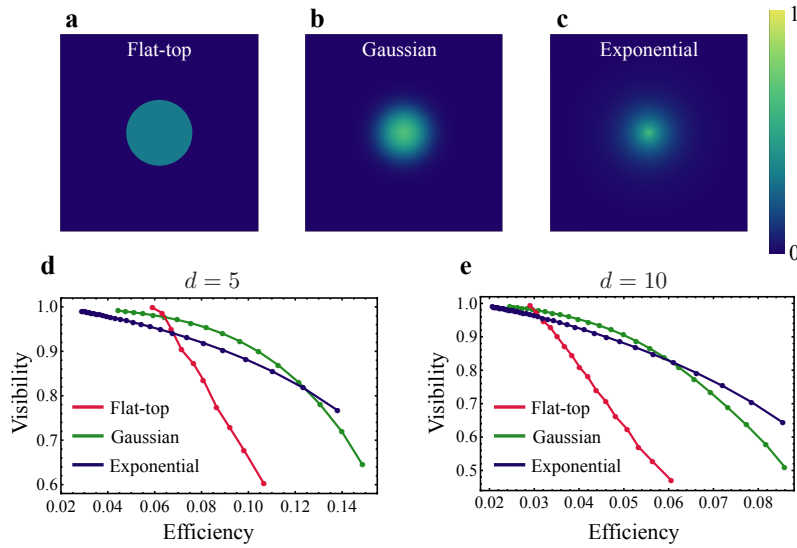


Fig. 8. Comparison of intensity-flattening with different backward-propagating beam. Normalized intensity distribution for three different types of backward propagating beams, i.e. (a) Flat-top, (b) Gaussian and (c) Exponential. The trade-off between visibility and efficiency is shown for all three types of beams in (d) and (e), for dimension 5 and 10, respectively.

efficient. Thus, for a desired range of visibilities and efficiencies, beam shaping of the backward propagating beam consist of an additional mean by which the measurement scheme may be optimized.

Appendix-B

Intensity flattening via induced losses: In the previous section, we have investigated several beam shaping strategies that allows one to achieve higher detection efficiencies for a given range of measurement visibilities. However, in this case, the requirement of beam shaping using phase elements in conjugate planes of the backward propagating beam introduces some complexity to our measurement technique. We now investigate another avenue to achieve a flattening of the backward propagating beam by carefully introducing losses at SLM-B. The losses are introduce in such a way that the Gaussian is cut such that the top region of the Gaussian is made flat. Of course, by doing so, the effect of the Gaussian factor in the overlap integral of LG beams is reduced. In general, this technique is more lossy than simply stretching the Gaussian factor. However, there are cases where a carefully chosen combination of stretching the Gaussian first, then introducing losses in order to cut only the top of the stretched Gaussian may be beneficial in terms of efficiency for a given measurement visibility, see Fig 9.

Appendix-C

Optimal subspaces: As mentioned in the main text, we perform a genetic algorithm in order to obtained the optimal set of state in a given d -dimensional subspace leading to the maximum secret key rates. Considering a population of 10 members, a mutation rate and a mutation frequency of 10 % selected with convergence after a number of iterations ranging from 10,000 and 30,000. The optimal subsets of the full 55-dimensional states are shown in Fig. 10. The list of the azimuthal and radial states considered can be found in Table 2. In Table 2, the label i ,

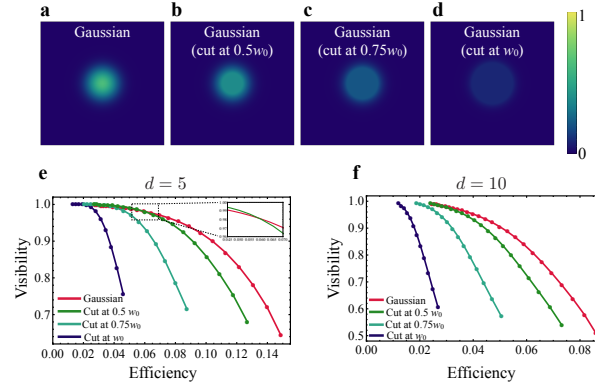


Fig. 9. Comparison of intensity-flattening with different cut of the backward-propagating beam. Normalized intensity distribution for three different types of backward propagating beams with, i.e. (a) no cut (Gaussian), (b) cut at $0.5w_0$, (c) cut at $0.75w_0$ and (d) cut at w_0 . The trade-off between visibility and efficiency is shown for all three types of beams in (e) and (f), for dimension 5 and 10, respectively. In dimension 5, we can see in the inset that for visibilities larger than 98.5 %, a cut at $0.5w_0$ increasing the efficiency of the measurement, with respect to an uncut Gaussian.

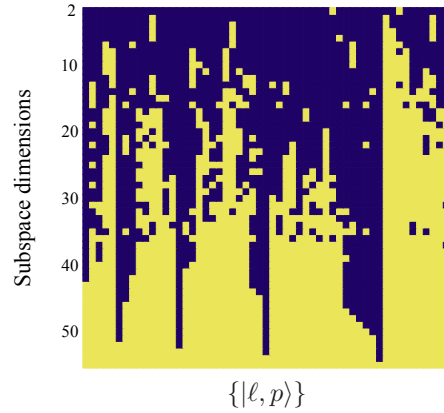


Fig. 10. Optimal d -dimensional subspaces. Representation of the optimal d -dimensional subspaces of the full 55-dimensional measurements. The states on the horizontal axis are explicitly given in Table 2. Yellow indicates the presence of the state in the corresponding subspace, and dark blue indicates its absence.

ranging from 1 to 55, indicates the state employed in order presented in Fig. 5-(a) of the main text. The mode order N , azimuthal index ℓ and radial index p are in the range of 1 to 10, -9 to 9 and 0 to 4, respectively.

Table 2. List of the States Considered in the 55-Dimensional Measurements.

i	N	ℓ	p
1	1	0	0
2	2	-1	0
3	2	1	0
4	3	-2	0
5	3	2	0
6	3	0	1
7	4	-3	0
8	4	3	0
9	4	-1	1
10	4	1	1
11	5	-4	0
12	5	4	0
13	5	-2	1
14	5	2	1
15	5	0	2
16	6	-5	0
17	6	5	0
18	6	-3	1
19	6	3	1
20	6	-1	2
21	6	1	2
22	7	-6	0
23	7	6	0
24	7	-4	1
25	7	4	1
26	7	-2	2
27	7	2	2
28	7	0	3
29	8	-7	0
30	8	7	0
31	8	-5	1
32	8	5	1
33	8	-3	2
34	8	3	2
35	8	-1	3
36	8	1	3
37	9	-8	0
38	9	8	0
39	9	-6	1
40	9	6	1
41	9	-4	2
42	9	4	2
43	9	-2	3
44	9	2	3
45	9	0	4
46	10	-9	0
47	10	9	0
48	10	-7	1
49	10	7	1
50	10	-5	2
51	10	5	2
52	10	-3	3
53	10	3	3
54	10	-1	4
55	10	1	4

Appendix-D

Castle, Sine, and Palace states: The visually interesting density matrices shown in Fig. 6 of the main text are given by the following states. The 7-dimensional OAM *castle state*, 5-dimensional radial *castle state*, the 17-dimensional OAM *sine state*, and the 19-dimensional full-field *palace states*, are respectively given by the following pure states;

$$|\psi_{\text{castle}}^{(d=7)}\rangle = \frac{1}{\sqrt{\mathcal{N}_{\text{castle}}^{(d=7)}}} \left(|\ell = -3\rangle + 0.5 |\ell = -2\rangle + 0.5 |\ell = -1\rangle \right. \\ \left. + 0.5 |\ell = 0\rangle + 0.5 |\ell = 1\rangle + 0.5 |\ell = 2\rangle \right. \\ \left. + |\ell = 3\rangle \right), \quad (5)$$

$$|\psi_{\text{castle}}^{(d=5)}\rangle = \frac{1}{\sqrt{\mathcal{N}_{\text{castle}}^{(d=5)}}} \left(|p = 0\rangle + 0.6 |p = 1\rangle + 0.6 |p = 2\rangle \right. \\ \left. + 0.6 |p = 3\rangle + |p = 4\rangle \right), \quad (6)$$

$$|\psi_{\text{sine}}^{(d=17)}\rangle = \frac{1}{\sqrt{\mathcal{N}_{\text{sine}}^{(d=17)}}} \sum_{\ell=-8}^8 \sin(2\pi\ell/17) |\ell\rangle, \quad (7)$$

$$|\psi_{\text{palace}}^{(d=19)}\rangle = \frac{1}{\sqrt{\mathcal{N}_{\text{palace}}^{(d=19)}}} \left(0.5 |\ell = 0, p = 0\rangle + 0.8 |\ell = 0, p = 1\rangle \right. \\ \left. + 0.5 |\ell = -3, p = 0\rangle + 0.5 |\ell = 3, p = 0\rangle \right. \\ \left. + 0.5 |\ell = -1, p = 1\rangle + 0.5 |\ell = 1, p = 1\rangle \right. \\ \left. + 0.5 |\ell = -4, p = 0\rangle + 0.5 |\ell = 4, p = 0\rangle \right. \\ \left. + 0.5 |\ell = -2, p = 1\rangle + 0.8 |\ell = 2, p = 1\rangle \right. \\ \left. + 0.5 |\ell = 3, p = 1\rangle \right), \quad (8)$$

where $\mathcal{N}$ are normalization coefficients.

Funding

Vanier Canada Graduate Scholarships Program; Natural Sciences and Engineering Research Council of Canada (NSERC); Austrian Science Fund (FWF) through the START project Y879-N27; Joint Czech-Austrian project MultiQUEST (I 3053-N27 and GF17-33780L); QuantERA ERA-NET Co-fund (FWF project I 3553-N36); Engineering and Physical Sciences Research Council (EPSRC) (EP/P024114/1).

Acknowledgments

We thank A. Zeilinger and E. Karimi for many fruitful discussions.

Author contributions

F.B. and N.H.V. contributed equally to this work.

References

1. A. Zeilinger, G. Weihs, T. Jennewein, and M. Aspelmeyer, "Happy centenary, photon," *Nature* **433**, 230–238 (2005).
2. M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, "Significant-loophole-free test of bell's theorem with entangled photons," *Phys. Rev. Lett.* **115**, 250401 (2015).
3. L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, "Strong loophole-free test of local realism," *Phys. Rev. Lett.* **115**, 250402 (2015).
4. J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, M. Li, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground entanglement-based quantum key distribution," *Phys. Rev. Lett.* **119**, 200501 (2017).
5. J. D. Franson, "Bell inequality for position and time," *Phys. Rev. Lett.* **62**, 2205 (1989).
6. A. K. Jha, M. Malik, and R. W. Boyd, "Exploring energy-time entanglement using geometric phase," *Phys. Rev. Lett.* **101**, 180405 (2008).
7. S. Walborn and C. Monken, "Transverse spatial entanglement in parametric down-conversion," *Phys. Rev. A* **76**, 062305 (2007).
8. N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," *Phys. Rev. Lett.* **88**, 127902 (2002).
9. M. Erhard, R. Fickler, M. Krenn, and A. Zeilinger, "Twisted photons: New quantum perspectives in high dimensions," *Light Sci. Appl.* **7**, 17146 (2018).
10. M. Krenn, M. Malik, M. Erhard, and A. Zeilinger, "Orbital angular momentum of photons and the entanglement of laguerre-gaussian modes," *Phil. Trans. R. Soc. A* **375**, 20150442 (2017).
11. L. Allen, L. M. W. Beijersbergen, R. Spreeuw, and J. Woerdman, "Orbital angular momentum of light and the transformation of laguerre-gaussian laser modes," *Phys. Rev. A* **45**, 8185 (1992).
12. M. Krenn, M. Huber, R. Fickler, R. Lapkiewicz, S. Ramelow, and A. Zeilinger, "Generation and confirmation of a (100×100)-dimensional entangled quantum system," *Proc. Natl. Acad. Sci. U.S.A.* **111**(17), 6243–6247 (2014).
13. M. Malik, M. Erhard, M. Huber, M. Krenn, R. Fickler, and A. Zeilinger, "Multi-photon entanglement in high dimensions," *Nat. Photonics* **10**, 248 (2016).
14. F. Cardano, F. Massa, H. Qassim, E. Karimi, S. Slussarenko, D. Paparo, C. de Lisio, F. Sciarrino, E. Santamato, R. W. Boyd, and L. Marrucci, "Quantum walks and wavepacket dynamics on a lattice with twisted photons," *Sci. Adv.* **1**, e1500087 (2015).
15. G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, "Free-space quantum key distribution by rotation-invariant twisted photons," *Phys. Rev. Lett.* **113**, 060503 (2014).
16. M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, "High-dimensional quantum cryptography with twisted light," *New J. Phys.* **17**, 033033 (2015).
17. A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, "High-dimensional intracity quantum cryptography with structured photons," *Optica* **4**(9), 1006–1010 (2017).
18. M. Beijersbergen, R. Coerwinkel, M. Kristensen, and J. Woerdman, "Helical-wavefront laser beams produced with a spiral phaseplate," *Opt. Commun.* **112**(5), 321–327 (1994).
19. V. Y. Bazhenov, M. Soskin, and M. Vasnetsov, "Screw dislocations in light wavefronts," *J. Mod. Opt.* **39**(5), 985–990 (1992).
20. N. Heckenberg, R. McDuff, C. Smith, and A. White, "Generation of optical phase singularities by computer-generated holograms," *Opt. Lett.* **17**(3), 221–223 (1992).
21. L. Marrucci, C. Manzo, and D. Paparo, "Optical spin-to-orbital angular momentum conversion in inhomogeneous anisotropic media," *Phys. Rev. Lett.* **96**, 163905 (2006).
22. J. P. Kirk and A. L. Jones, "Phase-only complex-valued spatial filter," *J. Opt. Soc. Am.* **61**(8), 1023–1028 (1971).
23. E. Bolduc, N. Bent, E. Santamato, E. Karimi, and R. W. Boyd, "Exact solution to simultaneous intensity and phase encryption with a single phase-only hologram," *Opt. Lett.* **38**(18), 3546–3549 (2013).
24. A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, "Entanglement of the orbital angular momentum states of photons," *Nature* **412**, 313–316 (2001).
25. H. Qassim, F. M. Miatto, J. P. Torres, M. J. Padgett, E. Karimi, and R. W. Boyd, "Limitations to the determination of a laguerre-gauss spectrum via projective, phase-flattening measurement," *J. Opt. Soc. Am. B* **31**(6), A20–A23 (2014).
26. G. C. Berkhout, M. P. Lavery, J. Courtial, M. W. Beijersbergen, and M. J. Padgett, "Efficient sorting of orbital angular momentum states of light," *Phys. Rev. Lett.* **105**, 153601 (2010).
27. M. Mirhosseini, M. Malik, Z. Shi, and R. W. Boyd, "Efficient separation of the orbital angular momentum eigenstates of light," *Nat. Commun.* **4**, 2781 (2013).
28. N. K. Fontaine, R. Ryf, H. Chen, D. T. Neilson, K. Kim, and J. Carpenter, "Optical spatial mode sorter of azimuthal and radial components," *arXiv:1803.04126* (2018).

29. J. F. Morizur, L. Nicholls, P. Jian, S. Armstrong, N. Treps, N. Hage, M. Hsu, W. Bowen, J. Janousek, and H.-A. Bachor, "Programmable unitary spatial mode manipulation," *J. Opt. Soc. Am. A* **27**(11), 2524–2531 (2010).
30. F. S. Roux and Y. Zhang, "Projective measurements in quantum and classical optical systems," *Phys. Rev. A* **90**, 033835 (2014).
31. Y. Zhang, F. S. Roux, M. McLaren, and A. Forbes, "Radial modal dependence of the azimuthal spectrum after parametric down-conversion," *Phys. Rev. A* **89**, 043820 (2014).
32. E. Karimi and E. Santamato, "Radial coherent and intelligent states of paraxial wave equation," *Opt. Lett.* **37**(13), 2484–2486 (2012).
33. E. Karimi, R. W. Boyd, P. De La Hoz, H. De Guise, J. Řeháček, Z. Hradil, A. Aiello, G. Leuchs, and L. L. Sánchez-Soto, "Radial quantum number of laguerre-gauss modes," *Phys. Rev. A* **89**, 063813 (2014).
34. E. Karimi, D. Giovannini, E. Bolduc, N. Bent, F. M. Miatto, M. J. Padgett, and R. W. Boyd, "Exploring the quantum nature of the radial degree of freedom of a photon via hong-ou-mandel interference," *Phys. Rev. A* **89**, 013829 (2014).
35. W. N. Plick and M. Krenn "Physical meaning of the radial index of laguerre-gauss beams," *Phys. Rev. A* **92**, 063841 (2015).
36. R. Fickler, M. Ginoya, and R. W. Boyd, "Custom-tailored spatial mode sorting by controlled random scattering," *Phys. Rev. B* **95**, 161108 (2017).
37. Y. Zhou, M. Mirhosseini, D. Fu, J. Zhao, S. Rafsanjani, H. Mohammad, A. E. Willner, and R. W. Boyd, "Sorting photons by radial quantum number," *Phys. Rev. Lett.* **119**, 263602 (2017).
38. X. Gu, M. Krenn, M. Erhard, and A. Zeilinger, "Gouy phase radial mode sorter for light: Concepts and experiments," *Phys. Rev. Lett.* **120**, 103601 (2018).
39. N. Zhao, X. Li, G. Li, and J. M. Kahn, "Capacity limits of spatially multiplexed free-space communication," *Nat. Photonics* **9**, 822 (2015).
40. J. M. Kahn, G. Li, X. Li, and N. Zhao, "To twist or not to twist: Capacity limits for free-space channels," In *Advanced Photonics 2016 (IPR, NOMA, Sensors, Networks, SPCom, SOF)*, SpM4E.1 (Optical Society of America, 2016).
41. V. Salakhutdinov, E. Eliel, and W. Löffler, "Full-field quantum correlations of spatially entangled photons," *Phys. Rev. Lett.* **108**, 173604 (2012).
42. A. Trichili, C. Rosales-Guzmán, A. Dudley, B. Ndagano, A. B. Salem, M. Zghal, and A. Forbes, "Optical communication beyond orbital angular momentum," *Sci. Rep.* **6**, 27674 (2016).
43. F. Bouchard, A. Sit, K. Heshami, R. Fickler, and E. Karimi, "Round-robin differential-phase-shift quantum key distribution with twisted photons," *Phys. Rev. A* **98**, 010301 (2018).
44. T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, "On mutually unbiased bases," *Int. J. Quantum Inf.* **8**(04), 535–640 (2010).
45. M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, "Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases," *Phys. Rev. A* **88**, 032305 (2013).
46. F. Bouchard, F. Hufnagel, D. Koutný, A. Abbas, A. Sit, K. Heshami, R. Fickler, and E. Karimi, "Full characterization of a high-dimensional quantum communication channel," *arXiv:1806.08018* (2018).
47. J. Bavaresco, N. H. Valencia, C. Klöckl, M. Pivoluska, P. Erker, N. Friis, M. Malik, and M. Huber, "Measurements in two bases are sufficient for certifying high-dimensional entanglement," *Nat. Phys.* **14**, 1032–1037 (2018).
48. C. Schwemmer, L. Knips, D. Richart, H. Weinfurter, T. Moroder, M. Kleinmann, and O. Gühne, "Systematic errors in current quantum state tomography tools," *Phys. Rev. Lett.* **114**, 080403 (2015).

Quantum process tomography of a high-dimensional quantum communication channel

Frédéric Bouchard¹, Felix Hufnagel¹, Dominik Koutný², Aazad Abbas¹, Alicia Sit¹, Khabat Heshami³, Robert Fickler^{1 4 5}, and Ebrahim Karimi^{1 6}

¹Department of Physics, University of Ottawa, 25 Templeton Street, Ottawa, ON, K1N 6N5, Canada.

²Department of Optics, Palacký University, 17. listopadu 12, 771 46 Olomouc, Czech Republic.

³National Research Council of Canada, 100 Sussex Drive, Ottawa, Ontario K1A 0R6, Canada

⁴Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria.

⁵Current address: Photonics Laboratory, Physics Unit, Tampere University, Tampere, FI-33720, Finland.

⁶Department of Physics, Institute for Advanced Studies in Basic Sciences, 45137-66731 Zanjan, Iran.

April 30, 2019

The characterization of quantum processes, e.g. communication channels, is an essential ingredient for establishing quantum information systems. For quantum key distribution protocols, the amount of overall noise in the channel determines the rate at which secret bits are distributed between authorized partners. In particular, tomographic protocols allow for the full reconstruction, and thus characterization, of the channel. Here, we perform quantum process tomography of high-dimensional quantum communication channels with dimensions ranging from 2 to 5. We can thus explicitly demonstrate the effect of an eavesdropper performing an optimal cloning attack or an intercept-resend attack during a quantum cryptographic protocol. Moreover, our study shows that quantum process tomography enables a more detailed understanding of the channel conditions compared to a coarse-grained measure, such as quantum bit error rates. This full characterization technique allows us to optimize the performance of quantum key distribution under asymmetric experimental conditions, which is particularly useful when considering high-dimensional encoding schemes.

1 Introduction

Quantum information science has witnessed the emergence of a wide range of new technologies and applications [1]. Quantum cryptography [2], quantum computation [3] and quantum sensing [4] are examples of promising venues for a possible next technological revolution. In order to construct complex quantum machines or quantum networks, a full characterization of its building blocks is critical. A method for reconstructing the action of a component in a quantum system is known as *quantum process tomography* (QPT) [5, 6]. Previously, QPT has been performed to characterize several quantum physical systems, such as liquid-state NMR [7, 8], photonic qubits [9], atoms in optical lattices [10], trapped ions [11], solid-state qubits [12], continuous-variable quantum states [13], semiconductor quantum dot qubits [14] and, recently, nonlinear optical systems [15]. Another class of important quantum systems that can benefit from full characterization are quantum channels and components for quantum key distribution (QKD) and quantum communications [16, 17], where, so far, quantum channels may be categorized as optical fibre [18], line-of-sight free-space [19] and ground-to-satellite (satellite-to-ground) [20] links.

The benefits of fully characterizing quantum communication channels lie at a better understanding of possible error sources and, more importantly, on the detection of the potential presence of an eavesdropper, namely *Eve*, tapping

into the quantum channel. Her presence is revealed in the form of noise introduced in the channel. The authorized partners, typically referred to as *Alice* and *Bob*, may estimate noise levels in the channel to assess the amount of leaked information to Eve. After this error assessment, Alice and Bob may perform classical post-processing protocols, such as *privacy amplification* [21], in order to remove Eve's leaked information. Conventional methods for secure key rate analysis rely on symmetry assumptions to associate an average (coarse-grained over all preparation and measurement settings) bit error rate parameter to a reduction in secure key rates. However, experimental errors often tend to break these symmetry assumptions, motivating the use of numerical techniques in QKD [22].

While usual QKD schemes rely on encoding quantum information in two-level systems, i.e. qubits, there exists a particular class of QKD schemes known as *high-dimensional* QKD protocols [23, 24]. High-dimensional schemes have the potential advantage of tolerating larger noise levels in the channel and carrying more than one bit of information per carrier. So far, a full characterization of high-dimensional processes based on QPT has not been achieved experimentally. With the emergence of high-dimensional quantum information, QPT will become an essential tool for the characterization of complex experiments dealing with high-dimensional quantum states. As a physical implementation, the orbital angular momentum (OAM) of photons represents a promising route for high-dimensional encoding due to the maturity of its generation and detection schemes [25, 26]. OAM states, corresponding to helical wavefronts of the form $\exp(i\ell\varphi)$, where the OAM value ℓ is an integer and φ is the azimuthal coordinate, may be realized using single phase elements. Computer-generated holograms displayed on a spatial light modulator (SLM) provide a simple and versatile method for generating and manipulating these modes [27]. High-dimensional QKD has been demonstrated experimentally using OAM in the laboratory [28, 29, 30], in intra-city free-space links [31, 32, 33] and, recently, in other types of quantum links [34].

Here, we demonstrate the benefits of a full characterization of a quantum channel through quantum process tomography. This full charac-

terization will allow us to complement the numerical approach in [22] to optimize secure key rates under specific experimental conditions and to develop new protocols lacking symmetry that may outperform existing approaches.

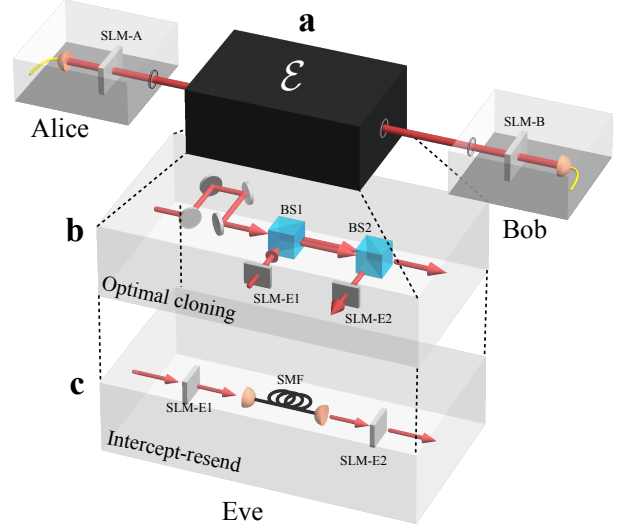


Figure 1: Simplified experimental setup. **a** Alice's preparation stage consists of a single photon source (not shown) that feeds the heralded photons to a generation apparatus consisting of a spatial light modulator (SLM-A). Alice's photon is subsequently sent into the quantum channel which is considered as a black box with quantum process $\mathcal{E}$. The output of the black box is fed to Bob's detection stage consisting of a spatial light modulator (SLM-B) and a single-mode optical fibre (SMF), via performing phase-flattening. We experimentally consider three different types of processes for our quantum channel: an ideal channel with no attack, the case of an optimal cloning attack (**b**), and the case of an intercept-resend attack (**c**). In particular, the configuration of the optimal cloning scheme consists of an SLM (SLM-E1) which generates a completely mixed state that is fed to the Hong-Ou-Mandel type interferometer at a balanced beam splitter (BS1). The *cloned* photons are then sent into a second beam splitter (BS2) in order to spatially separate them. Eve can use a second SLM (SLM-E2) to measure the state of her cloned photon while sending the other cloned photon to Bob. The experimental configuration of the intercept resend consists of two SLMs (SLM-E1 and SLM-E2) sandwiching a SMF.

2 Theory of quantum process tomography

Let us set the stage by introducing the basic concepts of QPT. The goal of QPT is to determine

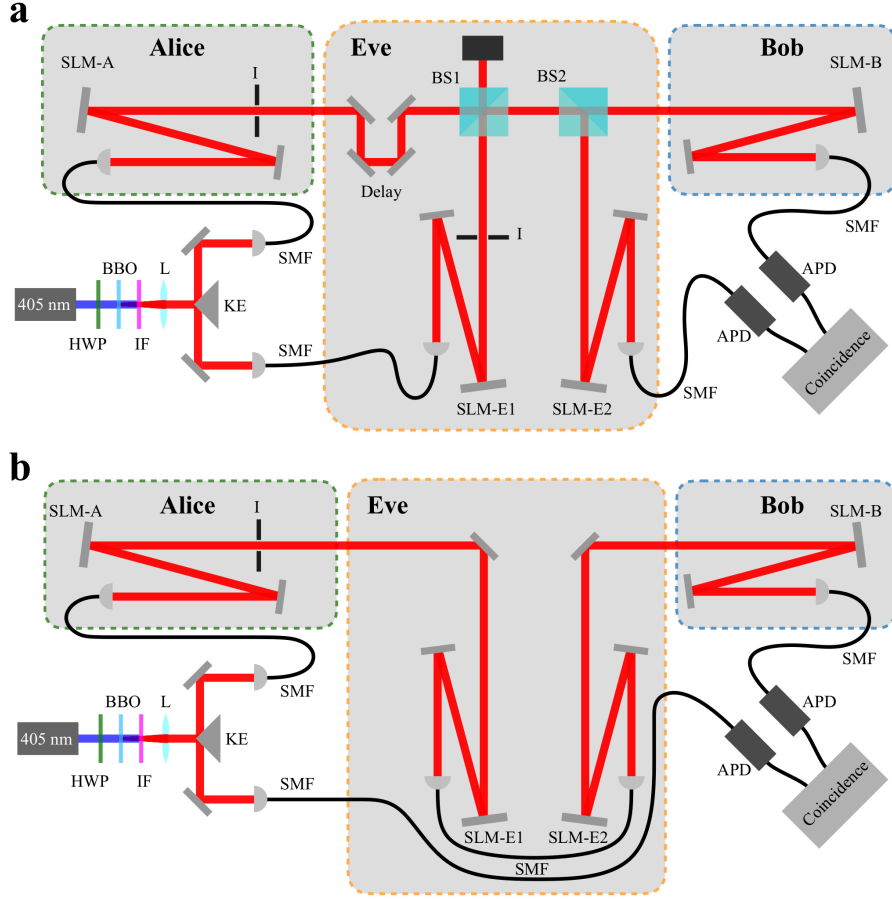


Figure 2: **Detailed experimental setup for (a) the optimal cloning attack and (b) the intercept-resend attack.** Single photons are generated, via spontaneous parametric downconversion (SPDC), by pumping a BBO crystal with a 355 nm quasi-continuous laser. The polarization of the laser is chosen in such a way to satisfy the phase-matching condition of the crystal. Subsequent to SPDC, the 355 nm laser is filtered out using an interference filter (IF). By using a lens (L), the photon pairs are split at the knife-edge (KE) mirror. The photons are then made to couple to single mode fibres (SMF) to filter their spatial modes to the fundamental Gaussian mode. Alice encodes the photon by using the spatial light modulator (SLM-A), and sends it to the quantum channel. Eve may perform an attack by using a delay line, beam splitters (BS1 and BS2), spatial light modulators (SLM-E1 and SLM-E2), and SMF. Bob measures the photon coming from the quantum channel by using his spatial light modulator (SLM-B). Photon counts are recorded at the avalanche photodiodes (APD) detectors and coincidence measurements are recorded using a coincidence box.

the completely positive map $\mathcal{E}$ representing the action of the system on any d -dimensional input state ρ_{in} . The output state is then given by $\rho_{\text{out}} = \mathcal{E}(\rho_{\text{in}})$. The process is typically represented as,

$$\mathcal{E}(\rho) = \sum_{m,n} \chi_{mn} \hat{A}_m \rho \hat{A}_n^\dagger, \quad (1)$$

where the $\hat{A}_m$ operators form a complete basis typically given by the Pauli operators or the Gell-Mann operators in higher dimensions. The trace-preserving positive Hermitian $d^2 \times d^2$ matrix χ_{mn} , defined as the *process matrix*, completely and

uniquely characterizes the action of the process $\mathcal{E}$. We may note that QPT may also be performed for non-trace-preserving maps [35].

A convenient alternative description of processes is given by the *Choi-Jamiołkowski* isomorphism (CJI), which states that every completely positive map can be represented as an operator living in a d^2 -dimensional Hilbert space. Such an operator, known as the Choi matrix $\rho_{\mathcal{E}}$, can be defined as the result of the channel acting upon one part of a maximally entangled state, $|\Phi\rangle$,

$$\rho_{\mathcal{E}} = (\hat{I} \otimes \mathcal{E}) |\Phi\rangle\langle\Phi|. \quad (2)$$

The output state is thus given accordingly by,

$$\rho_{\text{out}} = \text{Tr}_{\text{in}} \left[\left(\rho_{\text{in}}^T \otimes \hat{I} \right) \rho_{\mathcal{E}} \right], \quad (3)$$

where T denotes the transposition, $\hat{I}$ is the d -dimensional-identity operator and $\text{Tr}_{\text{in}}[\cdot]$ represents the partial trace over the input state's Hilbert space. In order to perform QPT, a set of tomographically complete states are sent into the channel and state tomography is performed on the output states. In our case, we consider states belonging to mutually unbiased bases (MUBs) in dimension d , which are known for dimensions that are powers of prime numbers [36]. A MUB projector is given by $\Pi_m^{(\alpha)}$, where $\alpha \in \{1, \dots, d+1\}$ labels one of the MUBs and $m \in \{1, \dots, d\}$ labels one of the states in this MUB. The completeness and orthogonality relations are respectively given by, $\sum_{\alpha, m} \Pi_m^{(\alpha)} / (d+1) = \hat{I}$ and $\text{Tr}(\Pi_m^{(\alpha)} \Pi_n^{(\beta)}) = \delta_{\alpha\beta} \delta_{mn} + (1 - \delta_{\alpha\beta})/d$, where δ_{ij} is the Kronecker delta. With the help of the CJI, one can derive Born rule-like expressions for probabilities,

$$\begin{aligned} p_{m,n}^{(\alpha,\beta)} &= \text{Tr} \left[\Pi_n^{(\beta)} \mathcal{E} \left(\Pi_m^{(\alpha)} \right) \right] \\ &= \text{Tr} \left[\left(\left(\Pi_m^{(\alpha)} \right)^T \otimes \Pi_n^{(\beta)} \right) \rho_{\mathcal{E}} \right]. \end{aligned} \quad (4)$$

This equation underlies the relation between quantum process tomography and quantum state tomography. The Choi matrix, $\rho_{\mathcal{E}}$, is experimentally reconstructed using the maximum-likelihood estimation. Better algorithms have also been recently proposed for QPT [37]. Finally, the process matrix is directly obtained from the Choi matrix.

In order to recover the Choi matrix, $\rho_{\mathcal{E}}$, defined in Eq. 2, for various attack scenarios, we follow maximum likelihood algorithms. The positive operator-valued measure (POVM) used to describe the process matrix consists of MUB measurements, i.e. $\Pi_j = (\Pi_m^{(\alpha)})^T \otimes \Pi_n^{(\beta)}$, where the index j runs over all the MUBs measurements performed by Alice and Bob. Theoretical probabilities given by the Born rule, $p_j = \text{Tr}[\Pi_j \rho_{\mathcal{E}}]$, observed with relative frequencies f_j , can be inverted by maximizing the log-likelihood functional

$$\log \mathcal{L} = \sum_j f_j \log \{p_j(\hat{\rho}_{\mathcal{E}})\}, \quad (5)$$

yielding the Choi matrices. Any density operator maximizing the likelihood functional satisfies the

extremal equation $\hat{R} \hat{\rho}_{\mathcal{E}} = \hat{\rho}_{\mathcal{E}}$, which leads to the well known iterative solutions [38] that takes a symmetric form,

$$\hat{\rho}_{\mathcal{E}}^{(k+1)} = \mu \hat{R} \hat{\rho}_{\mathcal{E}}^{(k)} \hat{R}, \quad (6)$$

where $\mu = \text{Tr}[\hat{R} \hat{\rho}_{\mathcal{E}}^{(k)} \hat{R}]^{-1}$ is a proper normalization constant and the operator $\hat{R}$ is defined as follows,

$$\hat{R} = \sum_j \frac{f_j}{p_j(\hat{\rho}_{\mathcal{E}})} \hat{\Pi}_j. \quad (7)$$

Typically, a few thousands of iterations are needed to observe the stationary point of the map in Eq. 6 with the maximally mixed state as a suitable choice of a starting point.

3 Experimental results

Our experiment consists of three components: the generation stage, the quantum channel and the detection stage, which are owned by Alice, Eve and Bob, respectively. We implement the prepare-and-measure QKD scheme with heralded single-photons using the OAM degree of freedom, see Fig. 1-a. The single photon pairs, consisting of the *signal* and *idler*, are generated by spontaneous parametric downconversion (SPDC) at a type I β -barium borate (BBO) crystal. The nonlinear crystal is pumped by a quasi-continuous wave laser operating at a wavelength of 355 nm. The generated photon pairs are coupled to single-mode optical fibres (SMF) in order to filter their spatial modes to the fundamental Gaussian mode. A coincidence rate of 30 kHz is measured, directly at the source, within a coincidence time window of 2 ns. We use the detection of the idler photon as the heralding trigger for the signal photon, thereby realizing a heralded single photon source with a measured second-order coherence of $g^{(2)}(0) = 0.015 \pm 0.004$. The heralded signal photon is sent to SLM-A corresponding to Alice's generation stage. The OAM states are produced using a phase-only holography technique [27]. Alice's heralded photon is subsequently sent over the quantum channel, considered here as a black box between Alice and Bob. At Bob's receiver, we perform a state-projection over the required states, which we realize by a mode filter implemented through a phase-flattening hologram and coupling into a SMF [39, 40]. In order to minimize Poissonian

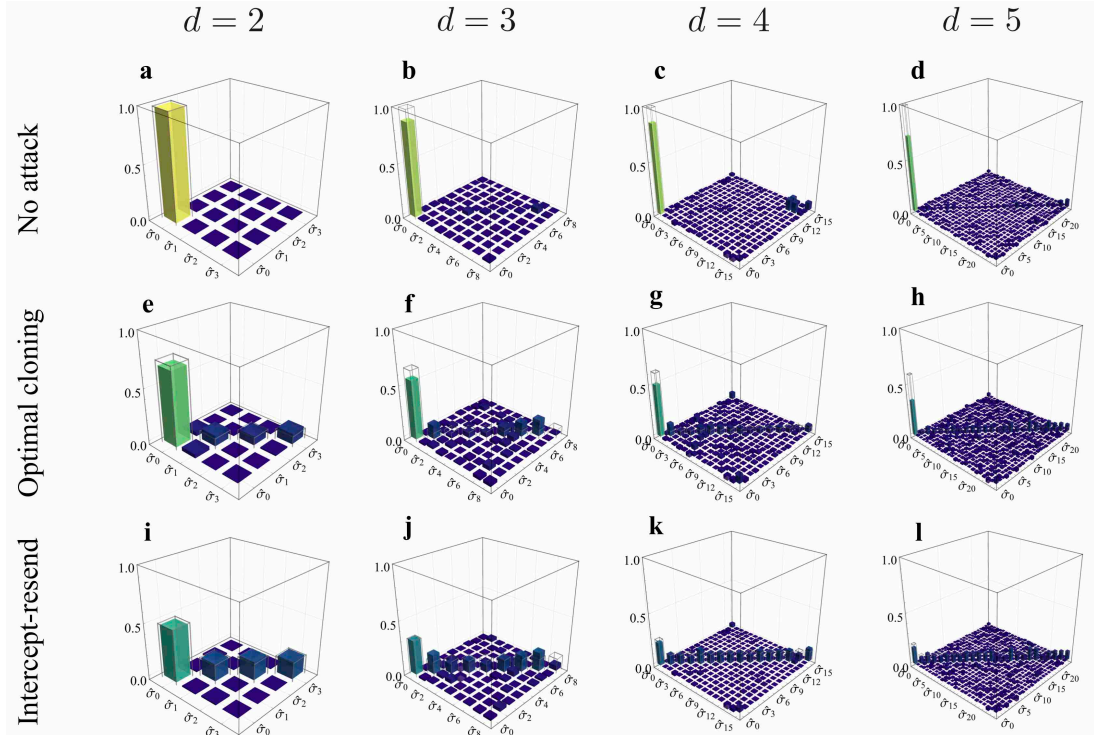


Figure 3: **Process matrix of high-dimensional quantum channels.** The real part of the experimentally reconstructed process matrices are presented for dimensions ranging from 2 to 5 in the case of (a-d) an ideal quantum channel, (e-h) a universal symmetric optimal quantum cloning attack, and (i-l) a universal intercept-resend attack. The theoretical results are represented by the wire-grid bars.

noise, the counts are accumulated over an integration time of 60 seconds per measurement setting. A detailed experimental setup is shown in Fig. 2. In particular, Alice and Bob perform QPT using MUBs [41], which are experimentally realized using OAM states. The computational bases ($\alpha = 1$) are given by $\{|\ell\rangle; \ell = -d/2, \dots, d/2; \ell \neq 0\}$ and $\{|\ell\rangle; \ell = -(d-1)/2, \dots, (d-1)/2\}$ for even and odd dimensions, respectively, for symmetry considerations. The second basis is given by the discrete Fourier transform, i.e. $\{|\phi_k\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega_d^{kj} |j\rangle; k = 0, \dots, d-1\}$, where $\omega_d = \exp(i2\pi/d)$. The explicit form of the other MUB elements can be found elsewhere [42].

3.1 Ideal quantum communication channel

In the case of an ideal quantum channel, i.e. no eavesdropper, the real parts of the experimentally reconstructed process matrices are shown in Fig. 3-(a-d) for dimensions ranging from $d = 2$ to 5. Ideal processes, where $\tilde{\mathcal{E}}(\rho) = \rho$, are described by process matrices given by $\tilde{\chi}_{ij} = \delta_{0i}\delta_{0j}$. Deviations of our reconstructed ideal process matrices

from the theory are attributed to imperfections in generation and detection of the distributed quantum states, i.e. the OAM modes. As higher dimensions are considered, larger crosstalk among the OAM modes is observed, which further deteriorates the experimentally reconstructed process matrix. Recently, we have introduced a new technique to measure spatial modes, which should improve detection fidelities [43]. In order to describe the quality or performance of the quantum channel, several figures of merit are available to describe our process [44]. One such figure is the *process fidelity* which is defined as $F_P = \text{Tr}(\chi_{\text{exp}} \tilde{\chi})$. For the ideal quantum channel, F_P can be directly obtained from the process matrix χ_{exp} , i.e. $F_P = \chi_{i=0,j=0}$. Moreover, the *average fidelity*, $\bar{F}$, of the process can be defined as the state fidelity between the output and the input averaged over all possible states with the convenient relation $\bar{F} = (dF_P + 1)/(d + 1)$. Similarly, the *average purity* is defined as the purity of the outgoing states averaged over all possible states and describes the level of mixture introduced by the process. It can be related to the average fidelity

Attack	Dimension - d	Process fidelity - F_p	Average state fidelity - $\bar{F}$	Process purity - $\bar{P}$
No attack	2	0.990 ± 0.001	0.993 ± 0.001	0.987 ± 0.001
	3	0.907 ± 0.003	0.930 ± 0.002	0.868 ± 0.004
	4	0.888 ± 0.003	0.911 ± 0.002	0.832 ± 0.004
	5	0.821 ± 0.002	0.851 ± 0.002	0.729 ± 0.003
Optimal cloning	2	0.71 ± 0.01	0.806 ± 0.006	0.687 ± 0.007
	3	0.604 ± 0.005	0.703 ± 0.003	0.538 ± 0.004
	4	0.524 ± 0.007	0.619 ± 0.006	0.432 ± 0.006
	5	0.419 ± 0.003	0.511 ± 0.003	0.321 ± 0.002
Intercept-resend	2	0.488 ± 0.006	0.659 ± 0.004	0.550 ± 0.003
	3	0.334 ± 0.002	0.500 ± 0.001	0.375 ± 0.001
	4	0.226 ± 0.002	0.381 ± 0.002	0.273 ± 0.001
	5	0.171 ± 0.001	0.309 ± 0.001	0.215 ± 0.001

Table 1: **Quality of the quantum channel processes.** Process fidelity, average fidelity and average purity of the quantum channel under different eavesdropping strategies, i.e. optimal cloning attack and intercept-resend attack, for dimensions ranging from 2 to 5.

according to $\bar{P} = (1 - 2\bar{F} + d\bar{F}^2)/(d - 1)$, respectively. The experimentally obtained process fidelities, average fidelities and average purities for the ideal channel are shown in Table 1 for dimensions ranging from $d = 2$ to 5.

3.2 Optimal quantum cloning attack

A special case of such a process is the so-called universal optimal cloning attack. In this scenario, Eve sends the incoming photon to an optimal cloning machine which produces two imperfect copies of the incoming photon, out of which she keeps one and sends the other to Bob, see Fig. 1-b. Later on, Eve may decide to perform a measurement on her copy in order to obtain information from Alice and Bob's shared photon. For the case of universal optimal cloning, Eve's copying machine has the effect of symmetrically introducing errors on the outgoing state. The cloning fidelity is defined as $F_{cl} = 1/2 + 1/(1+d)$. Universal optimal cloning machines have been realized experimentally using the symmetrization method [45, 46, 47, 48, 49], where both cloned photons possess the same cloning fidelity. At the heart of the symmetrization technique for optimal cloning is the Hong-Ou-Mandel interference effect [52]. For indistinguishable photons incident at the input port of a balanced beam splitter, a two-photon interference effect occurs which forbids the photons to exit the beam splitter from different output ports. Surprisingly, a slight

modification of the Hong-Ou-Mandel experiment leads to a universal optimal symmetric cloning machine. In this case, the second photon needs to be in a d -dimensional completely mixed state and is fed into the second input port of the beam splitter at exactly the same time. As the representation of the mixed state is the same in any basis, this scheme is universal, i.e. works for any state of the Hilbert space. When the two photons exit the beam splitter from the same output port, optimal cloning has been successful. A second beam splitter is then used to separate the two photons, e.g. one photon goes to Bob and the other one stays at Eve. We then experimentally perform the universal optimal cloning machine in the quantum channel for dimensions up to 5 and perform, again, a full characterization of the attack on the channel through QPT, see Fig. 3-(e-h) and Table 1. Leaving attacks on QKD systems aside, a full characterization of optimal quantum cloning machines is interesting in itself for applications to quantum state estimation [50, 51]. Indeed, there is an equivalence between a universal optimal cloning machine taking N input replicas and outputting an infinite number of clones and a quantum state estimation setup. A full characterization of the cloning machine would then enable a higher mode purity in the state estimation task.

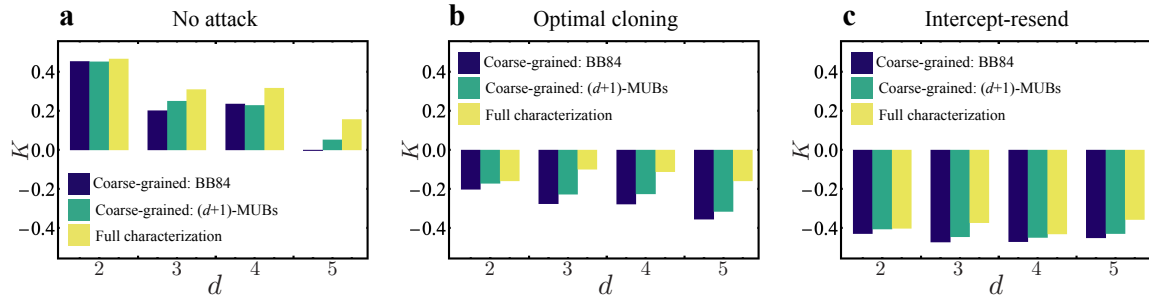


Figure 4: **Secret key rates.** Experimentally obtained secret key rates for the cases of no attack, optimal cloning and intercept-resend. The dark blue bars correspond to the BB84 protocol where the secret key rate is obtained by estimating a coarse-grained error rate. The green bars correspond to the $(d + 1)$ -MUBs protocol where the secret key rate is obtained also by estimating a coarse-grained error rate. The yellow bars correspond to a secret key rate calculated from the full characterization of the quantum channel. In all cases, a filter type measurement is considered yielding an overall efficiency of $1/d$.

3.3 Intercept-resend attack

Another eavesdropping scheme that achieves processes with lower average fidelities is the so-called intercept-resend attack, see Fig 3-(i-l). In contrast to the above described optimal cloning attack, Eve directly measures the received photon information, where she randomly performs her measurement in bases uniformly chosen at random (intercept). She then prepares a photon in the observed state and transmits it to Bob (resend). When considering the intercept-resend over all MUBs, the fidelity of the states at the output of the channel is given by $F_{\text{ir}} = 2/(1 + d)$. We experimentally perform the intercept-resend attack in our quantum channel by means of two SLMs, i.e. SLM-E1 and SLM-E2, with a SMF in between, see Fig. 1-c. The first SLM (SLM-E1) along with the SMF acts as the intercept section, while the second SLM (SLM-E2) acts as the resend. In the universal case, Eve randomly chooses $\alpha = 1, \dots, d + 1$ and $m = 1, \dots, d$ and simultaneously displays phase elements equivalent to $|\psi_m^{(\alpha)}\rangle$ and $|\psi_m^{(\alpha)}\rangle$ on the SLM-E1 and SLM-E2, respectively.

4 Secret key rates

So far, we have shown the feasibility of performing high-dimensional QPT on several quantum communication channels with our experimental implementation and provided a qualitative illustration of the effect of different eavesdropping strategies. In this section, we use the experimen-

tal outcomes obtained when performing QPT as our raw key from which we carry a formal security analysis. In particular, we show that the full characterization enables an enhanced estimation of the information leakage to an adversary eavesdropper. This results in a more accurate and favourable estimation of the achievable secret key rate, K , of the channel for a given QKD protocol. Furthermore, we demonstrate that the full characterization of the channel becomes even more advantageous when considering larger dimensions.

Traditionally, the secret key rate of a channel is calculated by evaluating the error rate, Q , from the raw key shared by Alice and Bob. Analytical formulae are derived to obtain the secret key rate as a function of the error rate. For instance, the BB84 protocol [2] in dimension d has the following simple analytical formula,

$$K^{(d)}(Q) = \log_2(d) - 2h^{(d)}(Q), \quad (8)$$

where $h^{(d)}(x) := -x \log_2(x/(d - 1)) - (1 - x) \log_2(1 - x)$ is the d -dimensional Shannon entropy. This protocol does not require a full characterization of the quantum channel and has a sifting efficiency of $1/2$. An extension of the d -dimensional BB84 protocol to tomographically complete measurements, yielding a full characterization of the channel, is known as the *six-state* protocol for the specific case of $d = 2$. For dimensions that are powers of prime numbers, all $d + 1$ MUBs are adopted. The sifting efficiency of this protocol is given by $1/(d + 1)$. Nevertheless, in the infinite key limit, the sifting efficiency

of the BB84 and the six-state protocol can approach 1, by making the basis choice extremely asymmetric [53]. This argument also holds for higher dimensions. The secret key rate of this $(d+1)$ -MUB protocol as a function of the error rate is given by,

$$K^{(d)}(Q) = \log_2(d) - h^{(d)}\left(\frac{d+1}{d}Q\right) - \frac{d+1}{d}Q \log_2(d+1). \quad (9)$$

Nonetheless, using such analytical formulae has a number of drawbacks. First, it only considers sifted data and assumes perfect unbiasedness among different MUBs. This assumption may increase the resulting secret key rate, but does not consist of an adequate representation of the channel and may lead to an underestimation of Eve's leaked information. Moreover, the secret key rate is obtained from a coarse-graining of the individual error rates per measurement settings. Thus, given this single parameter, a pessimistic estimation of the secret key rate is obtained due to the limited knowledge of the channel. Instead, we propose a protocol based on QPT where all the measurement outcomes, both from matching and non-matching bases, are considered in the secret key rate analysis. This protocol based on full characterization of the channel outperforms the counterpart coarse-grained protocols particularly for the case of asymmetric errors, which is often the case in experiments.

In our analysis, the secret key rate of a channel is estimated by considering the Devetak-Winter formula [54]. To do so, we recast our prepare-and-measure QKD protocol into an entanglement-based scheme using the source-replacement scheme [55], where Alice and Bob share pairs of entangled photons represented by the density matrix ρ_{AB} . In general, the secret-key rate is obtained according to,

$$K = \min_{\rho_{AB} \in \mathcal{C}} [H(Z_A|E) - H(Z_A|Z_B)], \quad (10)$$

where $\mathcal{C}$ is the set of physical density matrices that is consistent with the experimental constraints, e.g. error rates or measurement outcomes; $H(X|Y) := H(\rho_{XY}) - H(\rho_Y)$ is the conditional von Neumann entropy, with $H(\rho) := -\text{Tr}[\rho \log_2 \rho]$; Z_A and Z_B are the sets of positive operator valued measures (POVM) associated with Alice's and Bob's measurement settings, respectively. Finally, $\rho_{Z_A Z_B}$ and $\rho_{Z_A E}$ are

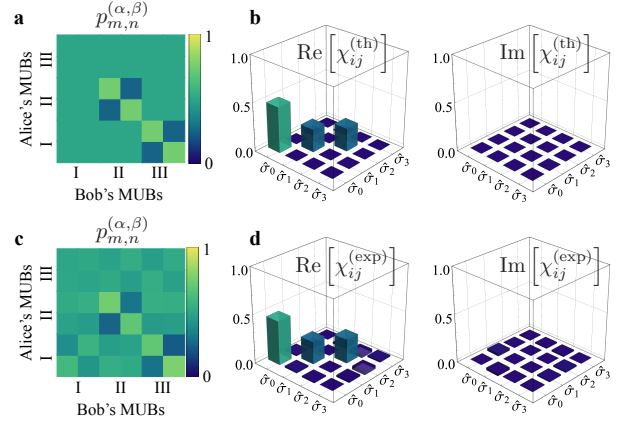


Figure 5: Asymmetric intercept-resend. **a** Theoretical and **c** experimental probability of detection matrices, as given in Eq. 4, corresponding to the asymmetric process of an intercept-resend eavesdropping strategy over MUB II and III in dimension 2. **b** Theoretical and **d** experimental real and imaginary part of the process matrix.

given by,

$$\rho_{Z_A Z_B} = \sum_{j,k} \text{Tr} \left[\left(Z_A^j \otimes Z_B^k \right) \rho_{AB} \right] |j\rangle\langle j| \otimes |k\rangle\langle k|, \quad (11)$$

$$\rho_{Z_A E} = \sum_j |j\rangle\langle j| \otimes \text{Tr}_A \left[\left(Z_A^j \otimes \hat{I} \right) \rho_{AE} \right], \quad (12)$$

where ρ_{ABE} is the tripartite density matrix shared by Alice, Bob and Eve, respectively. Hence, every additional experimental measurement is included in the minimization, which results in a greater, or equal, secret key rate. In the limiting case where we have a full characterization of the channel, ρ_{AB} is fully reconstructed and is given by the Choi matrix, $\rho_{\mathcal{E}}$, mentioned earlier. Thus the secret key rate may be directly calculated from ρ_{AB} ,

$$K = H(Z_A|E) - H(Z_A|Z_B), \quad (13)$$

where all experimental measurements are taken into consideration, even for the case of mismatching MUBs.

In the prepare-and-measure scheme, we can now determine the set of POVMs corresponding to Alice and Bob's generation and measurement apparatuses. At Alice's preparation stage, we have $Z_A = \{|0\rangle\langle 0|, \dots, |d-1\rangle\langle d-1|\}$, since Alice has the freedom to generate any state at random. However, at Bob's measuring stage, we consider two different sets of POVMs, i.e. $Z_B^{\text{sort}} =$

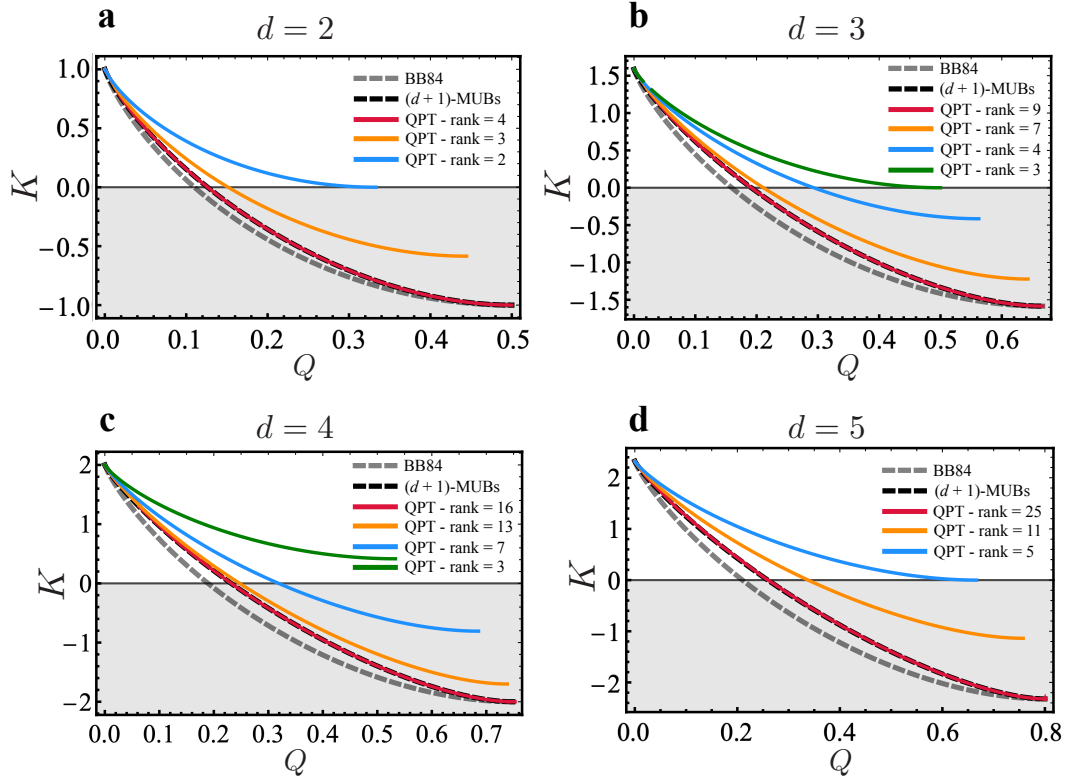


Figure 6: **Security analysis for noise models with varying levels of symmetry.** **a-d** The secret key rate is calculated for different scenarios in dimensions ranging from 2 to 5. The secret key rate for the BB84 and the $(d+1)$ -MUBs protocols are directly calculated from Eq. 8 and Eq. 9, respectively, where the level of noise is characterized using the error rate. Using the process matrix representation, we then consider noisy channels corresponding to diagonal trace-preserving process matrices of different ranks. The secret key rate is directly calculated using Eq. 13, and an error rate is determined for comparison with the coarse-grained protocols. For the case of a process matrix of rank $r = d^2$ with constant diagonal elements, i.e. Eq. 14, we retrieve the case of completely symmetric noise, i.e. Eq. 9. Asymmetric noise is then simulated by considering process matrices of lower ranks.

$\{|0\rangle\langle 0|, \dots, |d-1\rangle\langle d-1|\}$ and $Z_B^{\text{filter}} = \{|i\rangle\langle i|\}$, where the former corresponds to a sorting-type measurement and the latter corresponds to a filter-type measurement, and Alice and Bob post-select on the event where Bob successfully obtains a measurement of the state $|i\rangle\langle i|$ with $i \in \{0, \dots, d-1\}$. When carrying out the security analysis, one can see that the secret key rate, K , for the cases of Z_B^{sort} and Z_B^{filt} only differs from an overall efficiency of $1/d$. Thus, we carry out the high-dimensional QKD protocols based on QPT with a filter-type measurement scheme at Bob's stage using an SLM. There exists efficient sorters for the OAM computational and discrete Fourier transform basis [56]; however, the establishment of arbitrary multi-outcome measurement devices remains an open challenge for quantum applications [57].

For the full characterization of our high-

dimensional quantum channel via QPT with no explicit eavesdropping strategy applied, we calculate the corresponding secret key rate and compare it to a coarse-grained estimation of the channel, see Fig. 4 a. In the case of explicit eavesdropping strategies, such as optimal cloning and intercept-resend, the secret key rate will obviously be negative, see Fig. 4 b-c, and no secret key can be exchanged between Alice and Bob. We observe that for larger dimensions, the full characterization secret key rate performs better compared to the achievable secret key rate obtained from a coarse-graining of the channel. This may be due to the fact that, as one considers higher-dimensional states, the symmetry assumption involved in coarse-graining is increasingly not fulfilled. Therefore, full characterization of quantum channels may offer a means by which the full potential of high-dimensional protocols is exploited.

In highly asymmetric scenarios, which is often the case due to systematic errors such as misalignments, full characterization may even surpass the performance of coarse-grained protocols, such as the BB84 protocol, when considering the lower sifting efficiency of the full characterization protocol in the finite-key scenario.

Finally, in order to better understand the advantage of full characterization protocols compared to their coarse-grained counterparts, we carry out a security analysis for different noise models. In particular, we take advantage of the process matrix representation of the quantum channel to simulate different levels of symmetry in noise. In the limit, where the noise is completely symmetric over all states of all bases, the process matrix of the channel can be described as following,

$$\chi_{ij}^{r=d^2} = \frac{F(d+1)-1}{d} \delta_{0i} \delta_{0j} + \frac{(1-F)}{2(d-1)} (\delta_{ij} - \delta_{0i} \delta_{0j}), \quad (14)$$

where $\chi_{ij}^{r=d^2}$ is a $d^2 \times d^2$ diagonal matrix with a rank of $r = d^2$, and F determines the level of noise in the channel. For instance, the result of such a process on an input state, say $\rho_{\text{in}} = |0\rangle\langle 0|$, is given by the output state $\rho_{\text{out}} = F|0\rangle\langle 0| + (1-F)/(d-1) \sum_{i=1}^{d-1} |i\rangle\langle i|$. The processes of universal optimal cloning and universal intercept-resend fall under this category of process matrices, as can be seen in Fig. 3, with fidelities $F_{\text{cl}} = 1/2 + 1/(1+d)$ and $F_{\text{ir}} = 2/(1+d)$, respectively. Here, we consider another type of eavesdropping strategy that is not considered universal. We experimentally perform QPT of an intercept-resend attack where the eavesdropper only consider 2 out of the 3 MUBs available to Alice and Bob in dimension 2, see Fig. 5. This would be an appropriate attack in the case of BB84, where only two MUBs are utilized by Alice and Bob. However, in this case the noise added by the process to the output state is no longer symmetric. We observe state- and basis-dependent state fidelities which can be understood as asymmetric noise. Interestingly, the process matrix of the 2-MUB intercept-resend attack, see Fig. 5, has only 3 non-zero diagonal elements compared to 4 non-zero diagonal elements for the case of universal attacks, see Fig. 3, in dimension 2. Inspired, by the shape of the process matrix in this

simple case, we investigate different asymmetric noise models by varying the rank of the process matrix

For a process matrix of rank $r = d^2$, we retrieve the secret key rate formula for the coarse-grained $(d+1)$ -MUBs protocol, i.e. Eq. 9, as can be seen in Fig. 6. In dimension 2, we may then consider channels with process matrices of other ranks, corresponding to different degrees of noise symmetry. In particular, we consider trace-preserving process matrices of rank 3, i.e. $\chi_{ij}^{d=2, r=3} = F\delta_{0i}\delta_{0j} + (1-F)/2(\delta_{1i}\delta_{1j} + \delta_{2i}\delta_{2j})$, and rank 2, i.e. $\chi_{ij}^{d=2, r=2} = F\delta_{0i}\delta_{0j} + (1-F)(\delta_{1i}\delta_{1j})$. As can be seen in Fig. 6-a, noise corresponding to a process matrix of rank 2 or 3, leads to a significant improvement in secret key rate compared to a coarse-grained characterization of the channel using the error rate. Interestingly, for the case of the rank 2 process matrix of the form given above, i.e. $\chi_{ij}^{r=2}$, although the resulting error rate is well above the traditional error threshold, the secret key rate remains positive all the way up to $Q = 0.33$. We consider trace-preserving process matrices of rank 7, 4, and 3, in dimension 3, rank 13, 7, and 3, in dimension 4, and rank 11 and 5, in dimension 5, i.e.

$$\begin{aligned} \chi_{ij}^{d=3, r=7} &= F\delta_{0i}\delta_{0j} + \frac{1}{4}(1-F) \sum_{k=1}^6 \delta_{ki}\delta_{kj} \\ \chi_{ij}^{d=3, r=4} &= F\delta_{0i}\delta_{0j} + \frac{1}{2}(1-F) \sum_{k=1}^3 \delta_{ki}\delta_{kj} \\ \chi_{ij}^{d=3, r=3} &= F\delta_{0i}\delta_{0j} + \frac{3}{4}(1-F) (\delta_{1i}\delta_{1j} + \delta_{8i}\delta_{8j}) \\ \chi_{ij}^{d=4, r=13} &= F\delta_{0i}\delta_{0j} + \frac{1}{16}(1-F) \sum_{k=1}^{12} \delta_{ki}\delta_{kj} \\ \chi_{ij}^{d=4, r=7} &= F\delta_{0i}\delta_{0j} + \frac{1}{3}(1-F) \sum_{k=1}^6 \delta_{ki}\delta_{kj} \\ \chi_{ij}^{d=4, r=3} &= F\delta_{0i}\delta_{0j} + (1-F)(\delta_{1i}\delta_{1j} + \delta_{12i}\delta_{12j}) \\ \chi_{ij}^{d=5, r=11} &= F\delta_{0i}\delta_{0j} + \frac{1}{4}(1-F) \sum_{k=1}^{10} \delta_{ki}\delta_{kj} \\ \chi_{ij}^{d=5, r=5} &= F\delta_{0i}\delta_{0j} + \frac{1}{4}(1-F) \sum_{k=21}^{24} \delta_{ki}\delta_{kj}, \quad (15) \end{aligned}$$

respectively. In all cases, we can observe a clear advantage of using a full characterization

scheme compared to the error rate channel assessment. Interestingly, for all dimensions we find cases where after the transmission, the coarse-grained errors would label the channel as insecure, while our more detailed analysis still enables a secure communication. This advantage is possible because our analysis allows to distinguish between cases where an eavesdropper has not gained enough information about the state although they have transformed it such that Alice and Bob will have large error rates.

5 Conclusion

In summary, full characterization of quantum processes via QPT is an invaluable tool for high-dimensional quantum information processing. In particular, the complexity resulting from the generation and detection of the high-dimensional states involved may be fully characterized. In the study of quantum channels for quantum communications, full characterization via QPT turns out to be a beneficial resource that allows one to take full advantage of the potential high-dimensional nature of the protocols at play to increase the overall secret key rate.

Acknowledgments This work was supported by Canada Research Chair (CRC); Canada Foundation for Innovation (CFI); Canada Excellence Research Chairs, Government of Canada (CERC); Canada First Research Excellence Fund (CFREF); Natural Sciences and Engineering Research Council of Canada (NSERC). D.K. would like to acknowledge the project no IGA-PrF-2018-003.

References

- [1] Dowling, J. P. & Milburn, G. J. Quantum technology: the second quantum revolution, *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* **361**, 1655–1674 (2003).
- [2] Bennett, C. H. & Brassard, G., Quantum cryptography: Public key distribution and coin tossing, Proceedings of the IEEE international conference on computers, systems, and signal processing, bangalore, india, 1984 (1984).
- [3] Nielsen, M. A. & Chuang, I. Quantum computation and quantum information. Cambridge: Cambridge University Press (2002).
- [4] Degen, C., Reinhard, F. & Cappellaro, P. Quantum sensing. *Rev. Mod. Phys.* **89**, 035002 (2017).
- [5] Chuang, I. L. & Nielsen, M. A. Prescription for experimental determination of the dynamics of a quantum black box. *J. Mod. Opt.* **44**, 2455–2467 (1997).
- [6] Poyatos, J., Cirac, J. I. & Zoller, P. Complete characterization of a quantum process: the two-bit quantum gate. *Phys. Rev. Lett.* **78**, 390 (1997).
- [7] Nielsen, M. A., Knill, E. & Laflamme, R. Complete quantum teleportation using nuclear magnetic resonance. *Nature* **396**, 52 (1998).
- [8] Childs, A. M., Chuang, I. L. & Leung, D. W. Realization of quantum process tomography in NMR. *Phys. Rev. A* **64**, 012314 (2001).
- [9] O’Brien, J. L. *et al.* Quantum process tomography of a controlled-not gate. *Phys. Rev. Lett.* **93**, 080502 (2004).
- [10] Myrskog, S. H., Fox, J. K., Mitchell, M. W. & Steinberg, A. M. Quantum process tomography on vibrational states of atoms in an optical lattice. *Phys. Rev. A* **72**, 013615 (2005).
- [11] Riebe, M., Kim, K., Schindler, P., Monz, T., Schmidt, P. O., Korber, T. K., Hansel, W., Haffner, H., Roos, C. F. & Blatt, R. Process tomography of ion trap quantum gates. *Phys. Rev. Lett.* **97**, 220407 (2006).
- [12] Howard, M. *et al.* Quantum process tomography and linblad estimation of a solid-state qubit. *New Journal of Physics* **8**, 33 (2006).
- [13] Lobino, M. *et al.* Complete characterization of quantum-optical processes. *Science* **322**, 563–566 (2008).
- [14] Kim, D. *et al.* Quantum control and process tomography of a semiconductor quantum dot hybrid qubit. *Nature* **511**, 70 (2014).

- [15] Jacob, K. V., Mirasola, A. E., Adhikari, S. & Dowling, J. P. Direct characterization of linear and quadratically nonlinear optical systems. *Phys. Rev. A* **98**, 052327 (2018).
- [16] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
- [17] Bienvenu, N., Perez-Garcia, B., Roux, F. S., McLaren, M., Rosales-Guzman, C., Zhang, Y., Mouane, O., Hernandez-Aranda, R. I., Konrad, T. & Forbes, A. Characterizing quantum channels with non-separable states of classical light. *Nat. Phys.* **13**, 397 (2017).
- [18] Muller, A., Zbinden, H. & Gisin, N. Underwater quantum coding. *Nature* **378**, 449 (1995).
- [19] Buttler, W. T., Hughes, R. J., Kwiat, P. G., Lamoreaux, S. K., Luther, G. G., Morgan, G. L., Nordholt, J. E., Peterson, C. G. & Simmons, C. M. Practical free-space quantum key distribution over 1 km. *Phys. Rev. Lett.* **81**, 3283 (1998).
- [20] Yin, J., Cao, Y., Li, Y. H., Ren, J. G., Liao, S. K., Zhang, L., Cai, W. Q., Liu, W. Y., Li, B., Dai, H., Li, M., Huang, Y. M., Deng, L., Li, L., Zhang, Q., Liu, N. L., Chen, Y. A., Lu, C. Y., Shu, R., Peng, C. Z., Wang, J. Y. & Pan, J. W. Satellite-to-ground entanglement-based quantum key distribution. *Phys. Rev. Lett.* **119**, 200501 (2017).
- [21] Bennett, C. H., Brassard, G., Crépeau, C. & Maurer, U. M. Generalized privacy amplification. *IEEE T. Inform. Theory* **41**, 1915–1923 (1995).
- [22] Coles, P. J., Metodiev, E. M. & Lütkenhaus, N. Numerical approach for unstructured quantum key distribution. *Nature Commun.* **7**, 11712 (2016).
- [23] Bechmann-Pasquinucci, H. & Tittel, W. Quantum cryptography using larger alphabets. *Phys. Rev. A* **61**, 062308 (2000).
- [24] Cerf, N. J., Bourennane, M., Karlsson, A. & Gisin, N. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.* **88**, 127902 (2002).
- [25] Molina-Terriza, G., Torres, J. P. & Torner, L. Twisted photons. *Nature Physics* **3**, 305 (2007).
- [26] Erhard, M., Fickler, R., Krenn, M. & Zeilinger, A. Twisted photons: New quantum perspectives in high dimensions. *Light: Sci. & Appl.* **7**, 17146 (2018).
- [27] Forbes, A., Dudley, A. & McLaren, M. Creation and detection of optical modes with spatial light modulators. *Advances in Optics and Photonics* **8**, 200–227 (2016).
- [28] Mafu, M., Dudley, A., Goyal, S., Giovannini, D., McLaren, M., Padgett, M. J., Konrad, T., Petruccione, F., Lutkenhaus, N. & Forbes, A. Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Phys. Rev. A* **88**, 032305 (2013).
- [29] Mirhosseini, M. *et al.* High-dimensional quantum cryptography with twisted light. *New J. Phys.* **17**, 033033 (2015).
- [30] Bouchard, F. *et al.* Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons. *Quantum* **2**, 111 (2018).
- [31] Vallone, G., D'Ambrosio, V., Sponselli, A., Slussarenko, S., Marrucci, L., Sciarrino, F. & Villoresi, P. Free-space quantum key distribution by rotation-invariant twisted photons. *Phys. Rev. Lett.* **113**, 060503 (2014).
- [32] Krenn, M., Handsteiner, J., Fink, M., Fickler, R. & Zeilinger, A. Twisted photon entanglement through turbulent air across Vienna. *PNAS* **112**, 14197–14201 (2015).
- [33] Sit, A. *et al.* High-dimensional intracity quantum cryptography with structured photons. *Optica* **4**, 1006–1010 (2017).
- [34] Bouchard, F. *et al.* Quantum cryptography with twisted photons through an outdoor underwater channel. *Opt. Exp.* **26**, 22563–22573 (2018).
- [35] Bongioanni, I., Sansoni, L., Sciarrino, F., Vallone, G. & Mataloni, P. Experimental quantum process tomography of non-trace-preserving maps. *Phys. Rev. A* **82**, 042307 (2010).
- [36] Wootters, W. K. & Fields, B. D. Optimal state-determination by mutually unbiased measurements. *Annals of Physics* **191**, 363–381 (1989).

- [37] Knee, G. C., Bolduc, E., Leach, J. & Gauger, E. M. Quantum process tomography via completely positive and trace-preserving projection. *Phys. Rev. A* **98**, 062336 (2018).
- [38] Ježek, M., Fiurášek, J. & Hradil, Z. Quantum inference of states and processes. *Phys. Rev. A* **68**, 012305 (2003).
- [39] Mair, A., Vaziri, A., Weihs, G. & Zeilinger, A. Entanglement of the orbital angular momentum states of photons. *Nature* **412**, 313–316 (2001).
- [40] Qassim, H. *et al.* Limitations to the determination of a Laguerre–Gauss spectrum via projective, phase-flattening measurement. *J. Opt. Soc. Am. B* **31**, A20–A23 (2014).
- [41] Fernández-Pérez, A., Klimov, A. B. & Saavedra, C. Quantum process reconstruction based on mutually unbiased basis. *Phys. Rev. A* **83**, 052332 (2011).
- [42] Durt, T., Englert, B.-G., Bengtsson, I. & Życzkowski, K. On mutually unbiased bases. *Int. J. Quantum Inf.* **8**, 535–640 (2010).
- [43] Bouchard, F., Valencia, N. H., Brandt, F., Fickler, R., Huber, M., & Malik, M., Measuring azimuthal and radial modes of photons. *Optics Express* **26**, 31925 (2018).
- [44] Gilchrist, A., Langford, N. K. & Nielsen, M. A. Distance measures to compare real and ideal quantum processes. *Phys. Rev. A* **71**, 062310 (2005).
- [45] Irvine, W. T. M., Linares, A. L., deDood, M. J. A. & Bouwmeester, D. Optimal quantum cloning on a beam splitter. *Phys. Rev. Lett.* **92**, 047902 (2004).
- [46] Ricci, M., Sciarrino, F., Sias, C. & DeMartini, F. Teleportation scheme implementing the universal optimal quantum cloning machine and the universal not gate. *Phys. Rev. Lett.* **92**, 047901 (2004).
- [47] Nagali, E. *et al.* Optimal quantum cloning of orbital angular momentum photon qubits through Hong–Ou–Mandel coalescence. *Nature Photonics* **3**, 720 (2009).
- [48] Nagali, E., Giovannini, D., Marrucci, L., Slussarenko, S., Santamato, E. & Sciarrino, F. Experimental optimal cloning of four-dimensional quantum states of photons. *Phys. Rev. Lett.* **105**, 073602 (2010).
- [49] Bouchard, F., Fickler, R., Boyd, R. W. & Karimi, E. High-dimensional quantum cloning and applications to quantum hacking. *Science Adv.* **3**, e1601915 (2017).
- [50] Bruß, D. & Macchiavello, C. Optimal state estimation for d-dimensional quantum systems. *Phys. Lett. A* **253**, 249–251 (1999).
- [51] Thekkadath, G. S., Saaltink, R. Y., Giner, L. & Lundeen, J. S. Determining complementary properties with quantum clones. *Phys. Rev. Lett.* **119**, 050405 (2017).
- [52] Hong, C.-K., Ou, Z.-Y. & Mandel, L. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 2044 (1987).
- [53] Lo, H.-K., Chau, H. F., & Ardehali, M. Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security. *Journal of Cryptology* **18**, 133–165 (2005).
- [54] Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 461, 207–235 (The Royal Society, 2005).
- [55] Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).
- [56] Berkhout, C. G. *et al.* Efficient sorting of orbital angular momentum states of light. *Phys. Rev. Lett.* **105**, 153601 (2010).
- [57] Fontaine, N. K. *et al.* Laguerre-Gaussian mode sorter. *arXiv preprint arXiv:1803.04126v2* (2018).

Chapter 4

High-dimensional quantum cryptography through free-space and underwater quantum channels

This chapter is based on the following papers:

1. A. Sit, **F. Bouchard**, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Gunthner, B. Heim, C. Marquardt, G. Leuchs, R.W. Boyd, & E. Karimi, “High-Dimensional intra-city quantum cryptography with structured photons”, *Optica* **4**, 1006 (2017).

DOI: <https://doi.org/10.1364/OPTICA.4.001006>

© 2017 Optical Society of America

2. **F. Bouchard**, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. W. Boyd, & E. Karimi, “Quantum cryptography with twisted photons through an outdoor underwater channel”, *Optics Express* **26**, 22563-22573 (2018).

DOI: <https://doi.org/10.1364/OE.26.022563>

© 2018 Optical Society of America

4.1 Quantum cryptography in realistic conditions

In previous chapters, we have reviewed and investigated important components of a quantum communication system. Here, we are interested in implementing quantum communication systems in realistic conditions, i.e. in a free-space intra-city link and in an outdoor underwater link. At the beginning of quantum cryptography, polarization-based QKD systems were first developed in the laboratory over fibres or in free-space. Then, longer fibre links, i.e. several kilometres, and longer free-space links, i.e. several hundreds of meters, have been experimentally investigated and demonstrated in order to assess the feasibility of fully deployed quantum networks. Practical QKD systems are being implemented in existing fibre networks over metropolitan areas and over hundreds of kilometres in free-space.

Today, OAM-based QKD systems are still in their early development stage. A number of experimental demonstrations have been reported considering aspects of the implementation. Although there still is a lot of work to be done in the lab in order to determine the optimal generation schemes, quantum cryptographic protocols, dimensionality, and detection schemes, we are at a point where some of these implementations can be tested in realistic conditions. In this chapter, we report the first experimental demonstration of high-dimensional quantum cryptography in several realistic quantum communication links.

4.2 High-dimensional quantum cryptography

High-dimensional QKD was first proposed 20 years ago [21, 90, 91, 22]. In the first work [21], it was noticed that high-dimensional encoding, rather than using qubits, would lead to an enhancement in key generation. In particular, a 4-dimensional version of the BB84 protocol with 2 MUB was considered. Moreover, a first security analysis was carried by considering the effect of an eavesdropper performing an intercept-resend attack. Although the intercept-resend attack is perhaps one of the less sophisticated of the attacks available to the eavesdropper, the authors noticed that such an attack in higher dimensions results in a higher error rate, thus making the eavesdropper more detectable. In the second work [90], the others considered the specific case of a 3-dimensional QKD scheme. The authors noticed that higher-dimensional encoding schemes allowed for more flexibility in the protocol, i.e. a larger number of MUB could be used. In the third work [91], the authors generalized the

previous results for d -dimensional QKD using M bases and investigated various incoherent and coherent individual eavesdropping attacks as a function of the dimension. Finally, in the fourth work [22], a more formal security analysis of high-dimensional QKD was laid out by considering cloning and collective attacks for arbitrary dimensions and by deriving upper bounds on error rates. In the previous works, non-optimal individual attacks, where the photons sent by Alice to Bob are attacked individually, were considered, whereas in this work, collective attacks, where the eavesdropper is allowed to perform the attack on all the sent photons coherently, were considered. The security analysis was carried for two scenarios, namely for 2 MUB and $(d + 1)$ MUB.

Since then, high-dimensional QKD has been first experimentally investigated using position and momentum [92], OAM modes [93], and energy-time entanglement [94]. Subsequent experimental investigations of high-dimensional QKD with OAM modes were carried out in the laboratory for dimensions ranging from 2 to 5 [95], in dimension 7 [96], in dimensions ranging from 3 to 64 using a novel type of high-dimensional QKD protocol [97], and finally in dimensions ranging from 2 to 8 using a large number of different protocols [98]. The last two demonstrations will be the subject of the next chapter. At this stage, generation and detection techniques and devices must be developed in order to push the secret key rates of OAM-based high-dimensional QKD systems. For instance, recent technological advances in photon detection allowed the demonstration of high-rate high-dimensional QKD systems using time-bins qudits [99].

4.3 Free-space quantum communications

In the previous section, we have reviewed the recent efforts of high-dimensional QKD in laboratory conditions. We are now interested in performing the first proof-of-principle experimental demonstration of high-dimensional QKD link. Due to the versatility of the generation and detection devices available, we choose to consider the OAM and polarization degree of freedom to form a 4-dimensional Hilbert space. Modes combining OAM and polarization are also known as structured light or space-varying polarized light beams due to their non-uniform polarization patterns. In particular, OAM itself has been recognized as a useful means by which information can be distributed through a free-space [100]. Classically, OAM modes have been experimentally sent across intra-city free-space links in Los Angeles (120 m) [101],

Venice (420 m) [102], Vienna (3 km) [103], between two Canary island (143 km) [104] and recently Erlangen (1.6 km) [105]. At the quantum level, only two experiments with OAM modes in free-space have been demonstrated, namely in a hall in Padua (210 m) [106] and through the intra-city link in Vienna (3 km) [107]. Nevertheless, in both cases, a two-dimensional Hilbert space was considered. In this chapter, we establish a 300 m free-space intra-city link using high-dimensional structured photons. Although OAM modes are extremely robust to truncation from circular apertures, atmospheric turbulence remains one of the main challenges in free-space links. The effect of turbulence on QKD increases with distance. Thus, in order to extend the achievable distance of OAM-based free-space links, active adaptive optics systems compensating for turbulence will be necessary.

4.4 Underwater quantum communications

In very recent years, a new type of channel for quantum communications has been proposed, namely underwater channels. For instance, one can imagine applications in terms of submarine-to-satellite links, or short free-space links between underwater vehicles. From a more fundamental standpoint, it is interesting to study underwater quantum channels. Indeed, they represent a versatile testbed to study practical QKD schemes in strong environmental perturbations, i.e. losses and turbulence, over short distances compared to free-space links. Underwater QKD has first been numerically investigated in [108], where absorption and scattering of photons in the water channel were simulated, resulting in maximal achievable distances on the order 100 m in the clearest type of water. However, the effect of turbulence on the secret key rate as a function of distance was not taken into consideration. Not long after, a first experimental demonstration of the distribution of single photons encoded in polarization was demonstrated [109]. The experiment was carried out in a 3 m long glass tube filled with water in laboratory conditions. Nevertheless, due to the stable and controlled environmental conditions, no turbulence was observed.

Suspecting that turbulence will play an important role in underwater quantum channels, we decided to perform a proof-of-principle experiment demonstrating QKD in an uncontrolled outdoor underwater link. In general, beam wandering and scintillations caused by turbulence may have two separate effects on a QKD system. In the first place, the detection probability decreases due to a lower spatial overlap with the detecting apparatus. In the second place, when using encoding schemes such as

OAM or spatial modes, beam wandering or optical aberrations results in a modification of the input mode, leading to significant cross-talk in the detected modes. This effect is even more pronounced than losses since it affects both the overall efficiency of detection, as well as the error rate. In this chapter, we perform QKD using OAM modes in dimensions 2 and 3 over a 3 m outdoor underwater link and perform an extensive analysis of the turbulence present in a 5 m outdoor underwater link. The turbulence was analyzed using a phase retrieval algorithm to reconstruct the effect of the turbulence in a single phase screen approximation, and by tracking the singularity splitting of OAM modes with different azimuthal mode indices. Since then, several investigations of underwater quantum communications have been carried using polarization [110, 111] and spatial modes [112], as well as numerical investigations [113, 114, 115].

High-dimensional intracity quantum cryptography with structured photons

ALICIA SIT,¹ FRÉDÉRIC BOUCHARD,¹ ROBERT FICKLER,¹ JÉRÉMIE GAGNON-BISCHOFF,¹ HUGO LAROCQUE,¹ KHABAT HESHAMI,² DOMINIQUE ELSE,^{3,4} CHRISTIAN PEUNTINGER,^{3,4} KEVIN GÜNTNER,^{3,4} BETTINA HEIM,^{3,4} CHRISTOPH MARQUARDT,^{3,4} GERD LEUCHS,^{1,3,4} ROBERT W. BOYD,^{1,5} AND EBRAHIM KARIMI^{1,6,*} 

¹Physics Department, Centre for Research in Photonics, University of Ottawa, Advanced Research Complex, 25 Templeton, Ottawa, Ontario K1N 6N5, Canada

²National Research Council of Canada, 100 Sussex Drive, Ottawa, Ontario K1A 0R6, Canada

³Max-Planck-Institut für die Physik des Lichts, Staudtstraße 2, 91058 Erlangen, Germany

⁴Institut für Optik, Information und Photonik, Universität Erlangen-Nürnberg, Staudtstraße 7/B2, 91058 Erlangen, Germany

⁵Institute of Optics, University of Rochester, Rochester, New York 14627, USA

⁶Department of Physics, Institute for Advanced Studies in Basic Sciences, 45137-66731 Zanjan, Iran

*Corresponding author: ekarimi@uottawa.ca

Received 5 June 2017; revised 20 July 2017; accepted 25 July 2017 (Doc. ID 297325); published 24 August 2017

Quantum key distribution (QKD) promises information-theoretically secure communication and is already on the verge of commercialization. The next step will be to implement high-dimensional protocols in order to improve noise resistance and increase the data rate. Hitherto, no experimental verification of high-dimensional QKD in the single-photon regime has been conducted outside of the laboratory. Here, we report the realization of such a single-photon QKD system in a turbulent free-space link of 0.3 km over the city of Ottawa, taking advantage of both the spin and orbital angular momentum photonic degrees of freedom. This combination of optical angular momenta allows us to create a 4-dimensional quantum state; wherein, using a high-dimensional BB84 protocol, a quantum bit error rate of 11% was attained with a corresponding secret key rate of 0.65 bits per sifted photon. In comparison, an error rate of 5% with a secret key rate of 0.43 bits per sifted photon is achieved for the case of 2-dimensional structured photons. We thus demonstrate that, even through moderate turbulence without active wavefront correction, high-dimensional photon states are advantageous for securely transmitting more information. This opens the way for intracity high-dimensional quantum communications under realistic conditions. © 2017 Optical Society of America

OCIS codes: (270.5568) Quantum cryptography; (060.2605) Free-space optical communication; (050.4865) Optical vortices.

<https://doi.org/10.1364/OPTICA.4.001006>

1. INTRODUCTION

Secure quantum communication, i.e., quantum key distribution (QKD), is on the forefront of the commercialization of future quantum technologies. Since its first theoretical proposal [1], it has been one of the major driving forces to investigate and apply quantum features for future information processing schemes [2,3]. While this process of developing commercial quantum cryptography devices has already started, possible next-generation QKD schemes, such as high-dimensional encoding, have come under scrutiny in quantum information research. Although different proof-of-principle experiments have shown the superiority of such schemes in terms of noise resistance and data capacity [4–8], their applicability still has to be demonstrated under real-world conditions. Here, another key question that needs to be addressed is the most suited photonic degree of freedom that allows encoding of high-dimensional quantum states.

In addition to polarization and wavelength, a light wave may carry orbital angular momentum (OAM) [9], corresponding to

helical wavefronts. Polarization is naturally bidimensional, i.e., $\{|L\rangle, |R\rangle\}$, and the associated angular momentum can take the values of $\pm\hbar$ per photon, where $\hbar$ is the reduced Planck constant, and $|L\rangle$ and $|R\rangle$ are left- and right-handed circular polarizations, respectively. In contrast, OAM is inherently unbounded, such that a photon with ℓ intertwined helical wavefronts, $|\ell\rangle$, carries $\ell\hbar$ units of OAM, where ℓ is an integer [10]. Quantum states of light resulting from an arbitrary coherent superposition of different polarizations and spatial modes, e.g., OAM, are referred to as *structured photons*; these photons can be used to realize higher-dimensional states of light [11]. Aside from their fundamental significance in quantum physics [12,13], single photons encoded in higher dimensions provide an advantage in terms of security tolerance and encrypting alphabets for quantum cryptography [4,5,8] and classical communications [14]. The behavior of light-carrying OAM through turbulent conditions has been studied theoretically and simulated in the laboratory scale [15–18]. Experimentally, OAM states have been tested in classical

communications across intracity links in Los Angeles (120 m) [19], Venice (420 m) [20], Erlangen (1.6 km) [21], Vienna (3 km) [22], and between two Canary Islands (143 km) [23], which is the longest link thus far. With attenuated lasers, OAM states and vector vortex beams have been respectively implemented in high-dimensional and 2-dimensional BB84 protocols, where the former was performed in a laboratory [8] and the latter in a hall in Padua (210 m) [24]. Though not QKD, the entanglement distribution of bidimensional twisted photons has been recently studied across the Vienna link [25]. Note that no true single-photon high-dimensional QKD experiment has been performed outside of the laboratory thus far.

In this paper, we combine polarization $\{|H\rangle, |V\rangle\}$ and an OAM subspace of $\{|\ell\rangle, |-\ell\rangle\}$ to form 4-dimensional quantum states $|k\rangle$, for $k = 1, 2, 3, 4$, belonging to the set $\{|H, \ell\rangle, |V, \ell\rangle, |H, -\ell\rangle, |V, -\ell\rangle\}$, where $|H\rangle = (|L\rangle + |R\rangle)/\sqrt{2}$ and $|V\rangle = -i(|L\rangle - |R\rangle)/\sqrt{2}$ are horizontal and vertical polarization states, respectively. We can create two sets of mutually unbiased bases (MUBs) from $|k\rangle$, defined as $|\psi\rangle^i = \mathcal{M}_0^{ik}|k\rangle$ and $|\varphi\rangle^j = \mathcal{M}_1^{jk}|k\rangle$, where $|\langle\psi|\psi\rangle^j|^2 = |\langle\varphi|\varphi\rangle^j|^2 = \delta_{ij}$, and $|\langle\psi|\varphi\rangle^j|^2 = 1/4$ for $i, j = 1, 2, 3, 4$ (see Supplement 1 for $\mathcal{M}_0$ and $\mathcal{M}_1$). Figure 1 illustrates the spatial structure of these MUBs for the case of $\ell = 2$. The information encoded within these modes lies in the transverse polarization and phase distributions; however, all of these modes possess a “doughnut”-shaped intensity distribution. The polarization distributions contain only linearly polarized states, and such beams are commonly called vector vortex beams [26]; in the case of $\{|\varphi\rangle^j\}$, the linear polarizations vary across the transverse plane. $\{|\psi\rangle^i\}$ and $\{|\varphi\rangle^j\}$ are conjugate quantities, and based on quantum complementarity they cannot be measured simultaneously; this forms the backbone of security in quantum cryptography. Specifically, in the BB84 protocol [1], the bases of preparation and measurement are randomly chosen between two MUBs by a sender and receiver, traditionally called Alice and Bob, respectively. We used the two MUBs of structured modes, $\{|\psi\rangle^i\}$ and $\{|\varphi\rangle^j\}$, to perform a high-dimensional BB84 protocol [4,5].

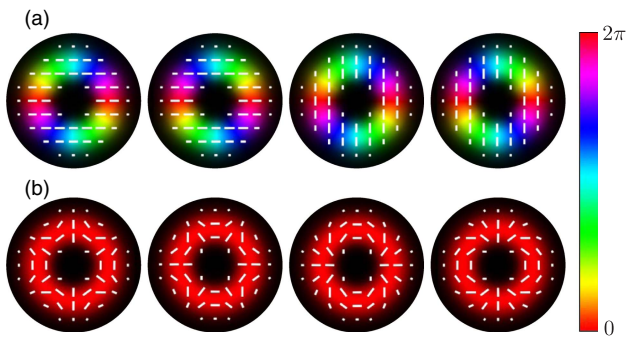


Fig. 1. Mode structure of mutually unbiased bases for $\ell = 2$. (a) $\{|\psi\rangle^i\}$ and (b) $\{|\varphi\rangle^j\}$ are examples of two bases of structured states of light, encoding in both polarization and OAM of $\ell = 2$. Each basis is orthonormal, and the two bases are mutually unbiased with respect to each other such that $|\langle\psi|\varphi\rangle^j|^2 = 1/4$. These MUBs have the advantage of possessing identical intensity profiles—“doughnut” shaped—and are shape-invariant upon free-space propagation. The information, therefore, is encoded in the transverse polarization and phase distributions, denoted by the white lines and the hue, respectively.

There are different approaches used to generate and sort these structured modes of light. We utilize liquid crystal devices known as q -plates [27], which coherently couple optical spin angular momentum to OAM. Q -plates are advantageous as they are placed in-line, are efficient in comparison to diffractive elements, and can be used to create arbitrary complex modal structures [28]. These q -plates used in conjunction with a carefully chosen sequence of wave plates can generate $\{|\psi\rangle^i\}$ and $\{|\varphi\rangle^j\}$ (see Supplement 1 for details). Furthermore, it is possible to rapidly switch between the states in $\{|\psi\rangle^i\}$ and $\{|\varphi\rangle^j\}$, of the order of 1 MHz, by replacing the wave plates with Pockels cells. Since q -plates are coherent and linear devices, they also work in the single-photon regime [29].

2. EXPERIMENT

We built a free-space link between the rooftops of two buildings, 0.3 km apart and 40 m above the ground, on the University of Ottawa campus; see Fig. 2. Two enclosures were constructed to contain and protect all of the optics and equipment at the sender and receiver. The sender unit is comprised of both the heralded single-photon source and the setup where Alice can prepare states. The receiver unit contains Bob’s state measurement setup and the single-photon detection system. No active adaptive optics or vibration isolation systems were implemented.

In the heralded single-photon source, photon pairs are generated via the spontaneous parametric downconversion process in a 5 mm long ppKTP crystal pumped by a 405 nm laser diode (200 mW). Nondegenerate wavelengths for the signal ($\lambda_s = 850$ nm) and idler ($\lambda_i = 775$ nm) photons are chosen in order to efficiently separate the two; only the signal photon is encoded with information. The signal and idler are each coupled into a separate single-mode fiber (SMF) to spatially filter the photons into the fundamental mode. Bandpass filters, 850 ± 5 nm and 775 ± 20 nm, are placed in front of the fiber couplers to select the correct photon pairs. The singles count rates at the source after the SMFs, detected with avalanche photodiodes (APDs), are 4 MHz and 10 MHz for the signal and idler, respectively. The idler photon heralds the presence of the signal photon, as determined by a coincidence logic box. This procedure gives a coincidence rate of around 1 MHz for a coincidence window of 5 ns with ≤ 0.2 MHz of accidental coincidence detections.

Alice takes the signal photon and prepares it in one of the states of the different MUBs through the use of an appropriate sequence of wave plates and q -plates. She then recombines the signal and idler photons on a dichroic mirror and enlarges the spatial structure of both beams such that they can be sent in the same beam across the link to Bob and to minimize divergence upon propagation, respectively. At the last lens (f_2) of the sending unit, the beam waist is approximately 12 mm. After propagation over the 0.3 km distance, we find the beam waist to be enlarged to approximately 20 mm as a consequence of atmospheric influences and imperfect optics. In order to measure the received quantum states, Bob demagnifies the photon’s structure with another set of lenses and separates the information-carrying signal photon from the heralding idler photon with another dichroic mirror. The idler photon is directly coupled into a SMF to act as a herald for the signal photon. With a sequence of wave plates, q -plates, PBSs, and SMFs, mirrored to that of Alice’s, Bob can make a measurement on the signal photon by projecting it onto one of the states from one of the MUBs. In such a way, Bob has a spatial

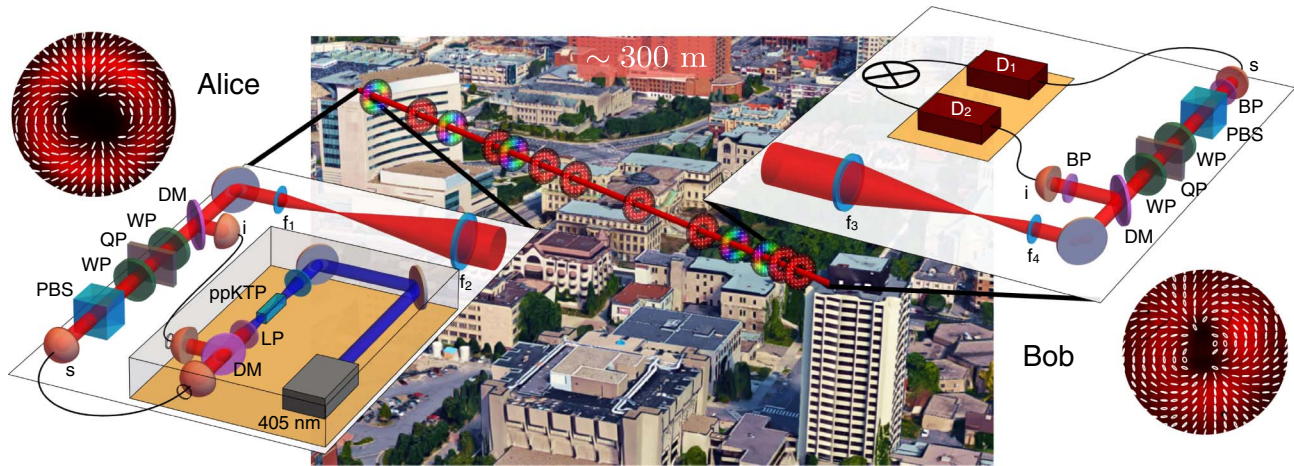


Fig. 2. Ottawa intracity quantum communication link. Schematic of the sender (left) with a heralded single-photon source (signal, s , and idler, i) and Alice's state preparation setup. Alice prepares a state from $\{|\psi^j\rangle\}$ or $\{|\varphi^j\rangle\}$ using a polarizing beam splitter (PBS), wave plates (WP), and a q -plate (QP). The signal and idler photons are recombined on a dichroic mirror (DM) before being sent to Bob. Two telescopes comprised of lenses with focal lengths of $f_1 = 75$ mm, $f_2 = f_3 = 400$ mm (diameter of 75 mm), and $f_4 = 50$ mm are used to enlarge and collect the beam, minimizing its divergence through the 0.3 km link. Bob, receiver (right), can then perform measurements on the sent states and record the coincidences between the signal and idler photons with detectors D_1 and D_2 at a coincidence logic box. Enclosures are built around the sender and receiver to shelter them from the wind and weather, as well as to shield them from background light. Examples of experimentally reconstructed polarization distributions for a structured mode from $\{|\varphi^j\rangle\}$ using a continuous wave laser that Alice prepared (top left) and Bob measured (bottom right) are shown in the insets. ppKTP, periodically poled KTP crystal; LP, long-pass filter; BP, bandpass filter. Map data: Google Maps, 2016.

mode filter such that, if he projects onto the same state that Alice sent, the signal photon will be phase-flattened and optimally detected. By using APDs and a coincidence logic box (5 ns coincidence window), the received idler photon acts as a trigger for the arrival of the signal photon and the coincidence rates are recorded. The best performance of our free-space link after coupling to the SMFs on Bob's side gave count rates for the signal and idler photons of 0.75 MHz and 2.5 MHz, respectively, with an optimal coincidence rate of approximately 50 kHz. However, due to large temperature and turbulence differences from night to night, the numbers varied throughout the various experimental runs. Overall, from sender to receiver, there are approximately 20% and 25% coupling efficiencies (equivalently 7 dB and 6 dB of losses) for the signal and idler photons, respectively, which gives an approximately 5% success rate for recording coincidences.

Since no adaptive optics were utilized, a portion of the raw data points sampled are greatly perturbed by the turbulence. The most dominant effect of the atmospheric turbulence given the range of our measured atmospheric structure constant, C_n^2 , between $2.5 \times 10^{-15} \text{ m}^{-2/3}$ and $6.4 \times 10^{-16} \text{ m}^{-2/3}$ (see Section 3) is beam wandering [30]. Under stable conditions, the idler photon remains in the fundamental mode and always couples to the SMF; however, when there is turbulence, it does not optimally couple. Since the signal photon is coaxially propagating with the idler photon, it experiences the same atmospheric turbulence; we can thus use the idler photon as not only a herald for the signal photon but also as a “target” to gauge the beam wandering in Bob's setup. This helps to correct our measurements for turbulence in postprocessing. During a BB84 protocol, Alice is preparing each signal photon into a state from a randomly chosen MUB and then sends it with its heralding idler photon to Bob. Once each pair reaches Bob, turbulence may have caused them to wander from the optical axis. Each measurement consists of coincidence counts acquired for 200 ms, repeated 50 times,

and then averaged. If there is excessive turbulence, the accumulated idler counts will have dropped. Therefore, Bob only keeps the coincidence measurements whose corresponding idler counts are near the optimal value, i.e., when there is little to no turbulence. Otherwise, he discards his measurement. As a target beam, the idler photon helps to sift out turbulence-affected pairs, decreasing the quantum bit error rate and thereby increasing the amount of securely transmitted information per sifted photon.

It is important to note that despite sending two photons across the link simultaneously, our scheme is still immune to photon-number-splitting attacks since the idler photon *does not* contain any of the polarization or OAM information of the signal photon. Apart from being able to monitor the turbulence, the only other information that the idler photon contains is timing information for heralding purposes, which could alternatively be communicated over a classical channel. Therefore, even if an eavesdropper had full access to the idler photon, she would not be able to access the signal information. A full security proof would be able to take into account the signal and idler photons, including bounds on possible side information of this particular setup. However, this is beyond the scope of this work and will be further investigated in the future.

3. TURBULENCE CHARACTERIZATION

To characterize the Ottawa intracity free-space link, we investigate the turbulence by evaluating its characteristic properties, such as the atmospheric structure constant C_n^2 and the Fried parameter r_0 [30–32]. We do so by sending a Gaussian-shaped laser beam (850 nm) over the 0.3 km long link and record its arrival position with a CCD camera. Because atmospheric turbulence changes on a millisecond time scale, short-term exposure images can reveal beam wandering, which is caused by fast-moving air cells, each having slightly different pressures, and thus small differences in

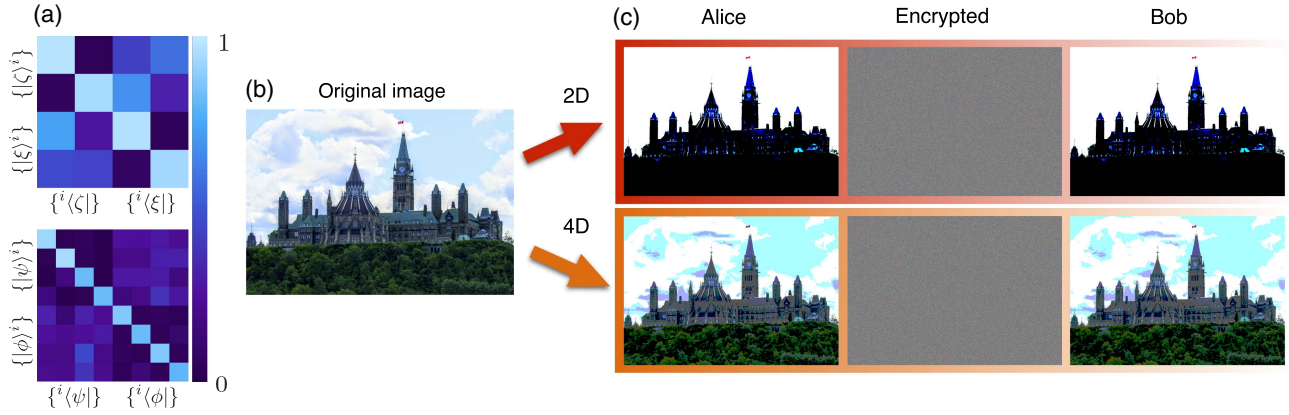


Fig. 3. Simulated encryption of an image with structured photons. (a) Experimentally measured probability-of-detection matrices, $P^{ij} = |\langle\alpha|\beta\rangle|^2$, where $\alpha, \beta = \{\psi, \phi\}$, for 2D (top row) and 4D (bottom row) structured photons with turbulence. These matrices have the corresponding bit error rates of $Q^{2D} = 5\%$ and $Q^{4D} = 11\%$, respectively. (b) Image of the Parliament of Canada that Alice encrypts and sends to Bob through a classical channel using their shared secret key. (c) Alice discretizes her intended image (left column) with d levels, where d is the encryption dimension, such that each pixel corresponds to three single photons (RGB values, leading to d^3 colors per pixel) that she sends to Bob. Using the experimentally measured probability-of-detection matrices (a), Alice then adds the shared secret key, generated from a BB84 protocol, on top of her discretized image to encrypt it (middle column). Bob decrypts Alice's sent image with his shared key to recover the image (right column). Implementing a 4-dimensional state clearly allows the ability to send more information per photon, where, in the ideal case, Alice can send twice the amount of information with respect to 2-dimensional states. However, due to noise present in the channel, we experimentally obtain an increase of 1.51 in the amount of information sent by Alice with respect to the case of 2-dimensional states. Image credit: Norman Bouchard.

refractive indices. The stronger the turbulence and the larger the distance of the link, the larger are the deflections from the optical axis. The latter can be deduced by taking an average over many short-term exposure images, which effectively leads to an atmospherically broadened Gaussian beam profile. During different measurement nights, we record 500 short exposure images (0.07 ms each), from which we calculate a Fried parameter between 18 cm and 41 cm, which corresponds to an atmospheric structure constant C_n^2 ranging from around $2.5 \times 10^{-15} \text{ m}^{-2/3}$ to $6.4 \times 10^{-16} \text{ m}^{-2/3}$, assuming Kolmogorov theory for atmospheric turbulence. Hence, the link shows moderate turbulence effects on the transmitted light fields.

4. RESULTS AND DISCUSSION

In QKD, a secret key may be established between Alice and Bob with a secret key rate, defined as the number of bits of secret key established divided by the number of sifted photons, given by $R(Q) = \log_2(d) - 2h(Q)$, where Q is the quantum bit error rate and $h(\cdot)$ is the Shannon entropy in dimension d . Hence, there is a threshold value of Q_0 above which a nonzero shared secure key cannot be generated. In dimension 2, this threshold value is the well-known $Q_0^{2D} = 11.0\%$, while it almost doubles to $Q_0^{4D} = 18.9\%$, in dimension 4 [5]. This clearly exhibits the robustness of high-dimensional quantum cryptography.

We perform a 4-dimensional BB84 protocol under different atmospheric conditions. Probability-of-detection matrices for the 4-dimensional structured photonic states, $\{|\psi\rangle^i\}$ and $\{|\phi\rangle^j\}$ with $\ell = 2$, of the BB84 protocol are shown in Fig. 3(a) (bottom row). In dimension 4, from the raw probability-of-detection matrix, the quantum bit error rate is $Q = 14\%$, and is below the threshold value of Q_0^{4D} , resulting in a positive corresponding secret key rate of $R = 0.39$ bits per sifted photon. Thus, without any corrections, a securely transmitted high-dimensional key can be established. By considering the idler as a target beam, which

accounts for turbulence, the quantum bit error rate is reduced to $Q^{4D} = 11\%$ with a secret key rate of $R^{4D} = 0.65$ bits per sifted photon. The secret key rate is lower than the maximum theoretical value of 2 bits per sifted photon, which is due to imperfections in transmission.

For a comparison, we perform a BB84 protocol with two-dimensional structured photons in the MUBs of $|\zeta\rangle = \{(|L, -1\rangle \pm |R, 1\rangle)/\sqrt{2}\}$ and $|\xi\rangle = \{(|L, -1\rangle \pm i|R, 1\rangle)/\sqrt{2}\}$; see Fig. 3(a) (top row). A quantum bit error rate and secret key rate of $Q^{2D} = 5\%$ and $R^{2D} = 0.43$ bits per sifted photon were obtained, respectively, using the target as compensation. Indeed, R^{4D} is larger than R^{2D} , showing the potential for transmitting more secure information per sifted photon in higher dimensions. This is visually shown in Fig. 3(c) (top and bottom rows): the image that Alice sends Bob [Fig. 3(b)] can be discretized with more steps in dimension 4 (bottom row) as compared to dimension 2 (top row). Due to turbulence, the quantum bit error rate for dimension 4 on many nights was above Q_0^{4D} . An example of one of these nights is shown in the Supplement 1 with a calculated quantum bit error rate of $Q_{\text{noisy}}^{4D} = 27\%$ calculated from the probability-of-detection matrix. However, allowing for two-way classical communications, the tolerable error bit rate increases to $31.5\% > Q_{\text{noisy}}^{4D}$ in dimension 4 [33] (see Supplement 1).

5. CONCLUSION

We have shown the feasibility of increasing the secure data transmission rate using high-dimensional quantum states compared to bidimensional states despite a noisy channel. Indeed, protocols based on higher-dimensional states are more advantageous in noisier channels because the security threshold can tolerate more errors. This paves the road toward high-dimensional intracity quantum cryptography via quantum key distribution.

In addition, our results lay the groundwork for intracity quantum teleportation with structured photons, which is an essential component of a free-space quantum network. We anticipate that these demonstrations can be extended over longer distances provided with adequate active turbulence monitoring and compensation.

Funding. Canada Research Chairs; Canada Foundation for Innovation (CFI); Canada Excellence Research Chairs, Government of Canada (CERC); Canada First Research Excellence Fund (CFREF).

Acknowledgment. All authors would like to thank Peter Banzer and Thomas Bauer for insightful discussions and acknowledge the support of the Max Planck—University of Ottawa Centre for Extreme and Quantum Photonics. E.K. would like to thank Guy LeBlanc, Donald Hopkins, David Needham, and Sean Kirkwood for their help on establishing the free-space link over the city of Ottawa. A.S. thanks Harold and Thérèse Sit for their continuous support and encouragement. The authors thank Norman Bouchard for providing the photo of the parliament of Canada. A.S. and H.L. acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC). F.B. acknowledges the support of the Vanier Canada Graduate Scholarships Program of the NSERC. R.F. acknowledges the support of the Banting postdoctoral fellowship of the NSERC.

See [Supplement 1](#) for supporting content.

REFERENCES

- C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *International Conference on Computer System and Signal Processing* (IEEE, 1984), pp. 175–179.
- V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
- H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photonics* **8**, 595–604 (2014).
- H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," *Phys. Rev. A* **61**, 062308 (2000).
- N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," *Phys. Rev. Lett.* **88**, 127902 (2002).
- S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, "Experimental quantum cryptography with qutrits," *New J. Phys.* **8**(5), 75 (2006).
- M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, "Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases," *Phys. Rev. A* **88**, 032305 (2013).
- M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, "High-dimensional quantum cryptography with twisted light," *New J. Phys.* **17**, 033033 (2015).
- L. Allen, M. W. Beijersbergen, R. Spreeuw, and J. Woerdman, "Orbital angular momentum of light and the transformation of Laguerre–Gaussian laser modes," *Phys. Rev. A* **45**, 8185–8189 (1992).
- A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, "Entanglement of the orbital angular momentum states of photons," *Nature* **412**, 313–316 (2001).
- E. Nagali, L. Sansoni, L. Marrucci, E. Santamato, and F. Sciarrino, "Experimental generation and characterization of single-photon hybrid ququarts based on polarization and orbital angular momentum encoding," *Phys. Rev. A* **81**, 052317 (2010).
- G. Molina-Terriza, J. P. Torres, and L. Torner, "Twisted photons," *Nat. Phys.* **3**, 305–310 (2007).
- F. Cardano, F. Massa, H. Qassim, E. Karimi, S. Slussarenko, D. Paparo, C. de Lisio, F. Sciarrino, E. Santamato, R. W. Boyd, and L. Marrucci, "Quantum walks and wavepacket dynamics on a lattice with twisted photons," *Sci. Adv.* **1**, e1500087 (2015).
- A. E. Willner, H. Huang, Y. Yan, Y. Ren, N. Ahmed, G. Xie, C. Bao, L. Li, Y. Cao, Z. Zhao, J. Wang, M. P. J. Lavery, M. Tur, S. Ramachandran, A. F. Molisch, N. Ashrafi, and S. Ashrafi, "Optical communications using orbital angular momentum beams," *Adv. Opt. Photon.* **7**, 66–106 (2015).
- C. Paterson, "Atmospheric turbulence and orbital angular momentum of single photons for optical communication," *Phys. Rev. Lett.* **94**, 153901 (2005).
- M. Malik, M. O'Sullivan, B. Rodenburg, M. Mirhosseini, J. Leach, M. P. Lavery, M. J. Padgett, and R. W. Boyd, "Influence of atmospheric turbulence on optical communications using orbital angular momentum for encoding," *Opt. Express* **20**, 13195–13200 (2012).
- O. J. Faras, V. D'Ambrosio, C. Taballione, F. Bisesto, S. Slussarenko, L. Aolita, L. Marrucci, S. P. Walborn, and F. Sciarrino, "Resilience of hybrid optical angular momentum qubits to turbulence," *Sci. Rep.* **5**, 8424 (2015).
- S. K. Goyal, A. H. Ibrahim, F. S. Roux, T. Konrad, and A. Forbes, "The effect of turbulence on entanglement-based free-space quantum key distribution with photonic orbital angular momentum," *J. Opt.* **18**, 064002 (2016).
- J. Wang, J.-Y. Yang, I. M. Fazal, N. Ahmed, Y. Yan, H. Huang, Y. Ren, Y. Yue, S. Dolinar, M. Tur, and A. E. Willner, "Terabit free-space data transmission employing orbital angular momentum multiplexing," *Nat. Photonics* **6**, 488–496 (2012).
- F. Tamburini, E. Mari, A. Sponselli, B. Thidé, A. Bianchini, and F. Romanato, "Encoding many channels on the same frequency through radio vorticity: first experimental test," *New J. Phys.* **14**, 033001 (2012).
- M. P. Lavery, B. Heim, C. Peuntinger, E. Karimi, O. S. Magaña-Loaiza, T. Bauer, C. Marquardt, R. W. Boyd, M. Padgett, and G. Leuchs, "Study of turbulence induced orbital angular momentum channel crosstalk in a 1.6 km free-space optical link," in *CLEO: Science and Innovations* (Optical Society of America, 2015), paper STu1L–4.
- M. Krenn, R. Fickler, M. Fink, J. Handsteiner, M. Malik, T. Scheidl, R. Ursin, and A. Zeilinger, "Communication with spatially modulated light through turbulent air across Vienna," *New J. Phys.* **16**, 113028 (2014).
- M. Krenn, J. Handsteiner, M. Fink, R. Fickler, R. Ursin, M. Malik, and A. Zeilinger, "Twisted light transmission over 143 km," *Proc. Natl. Acad. Sci. USA* **113**, 13648–13653 (2016).
- G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, "Free-space quantum key distribution by rotation-invariant twisted photons," *Phys. Rev. Lett.* **113**, 060503 (2014).
- M. Krenn, J. Handsteiner, M. Fink, R. Fickler, and A. Zeilinger, "Twisted photon entanglement through turbulent air across Vienna," *Proc. Natl. Acad. Sci. USA* **112**, 14197–14201 (2015).
- Q. Zhan, "Cylindrical vector beams: from mathematical concepts to applications," *Adv. Opt. Photon.* **1**, 1–57 (2009).
- L. Marrucci, C. Manzo, and D. Paparo, "Optical spin-to-orbital angular momentum conversion in inhomogeneous anisotropic media," *Phys. Rev. Lett.* **96**, 163905 (2006).
- H. Larocque, J. Gagnon-Bischoff, F. Bouchard, R. Fickler, J. Upham, R. W. Boyd, and E. Karimi, "Arbitrary optical wavefront shaping via spin-to-orbit coupling," *J. Opt.* **18**, 124002 (2016).
- E. Nagali, F. Sciarrino, F. De Martini, L. Marrucci, B. Piccirillo, E. Karimi, and E. Santamato, "Quantum information transfer from spin to orbital angular momentum of photons," *Phys. Rev. Lett.* **103**, 013601 (2009).
- N. Ageorges and C. Dainty, *Laser Guide Star Adaptive Optics for Astronomy* (Springer, 2013), Vol. **551**.
- A. N. Kolmogorov, "The local structure of turbulence in incompressible viscous fluid for very large Reynolds numbers," *Dokl. Akad. Nauk SSSR* **30**, 301–305 1941.
- D. L. Fried, "Optical resolution through a randomly inhomogeneous medium for very long and very short exposures," *J. Opt. Soc. Am.* **56**, 1372–1379 (1966).
- G. M. Nikolopoulos, K. S. Ranade, and G. Alber, "Error tolerance of two-basis quantum-key-distribution protocols using qudits and two-way classical communication," *Phys. Rev. A* **73**, 032325 (2006).



Quantum cryptography with twisted photons through an outdoor underwater channel

FRÉDÉRIC BOUCHARD,¹ ALICIA SIT,¹ FELIX HUFNAGEL,¹ AAZAD ABBAS,¹ YINGWEN ZHANG,¹ KHABAT HESHAMI,² ROBERT FICKLER,¹ CHRISTOPH MARQUARDT,^{3,4} GERD LEUCHS,^{1,3,4} ROBERT W. BOYD,^{1,3,5} AND EBRAHIM KARIMI^{1,3,*}

¹Department of Physics, University of Ottawa, Advanced Research Complex, 25 Templeton Street, Ottawa ON, K1N 6N5, Canada

²National Research Council of Canada, 100 Sussex Drive, Ottawa ON, K1A 0R6, Canada

³Max-Planck-Institut für die Physik des Lichts, Staudtstraße 2, 91058 Erlangen, Germany

⁴Institut für Optik, Information und Photonik, Universität Erlangen-Nürnberg, Staudtstraße 7/B2, 91058 Erlangen, Germany

⁵Institute of Optics, University of Rochester, Rochester, New York, 14627, USA

*ekarimi@uottawa.ca

Abstract: Quantum communication has been successfully implemented in optical fibres and through free-space. Fibre systems, though capable of fast key and low error rates, are impractical in communicating with destinations without an established fibre link. Free-space quantum channels can overcome such limitations and reach long distances with the advent of satellite-to-ground links. However, turbulence, resulting from local fluctuations in refractive index, becomes a major challenge by adding errors and losses. Recently, an interest in investigating the possibility of underwater quantum channels has arisen. Here, we investigate the effect of turbulence on an underwater quantum channel using twisted photons in outdoor conditions. We study the effect of turbulence on transmitted error rates, and compare different quantum cryptographic protocols in an underwater quantum channel, showing the feasibility of high-dimensional encoding schemes. Our work may open the way for secure high-dimensional quantum communication between submersibles, and provides important input for potential submersibles-to-satellite quantum communication.

© 2018 Optical Society of America under the terms of the [OSA Open Access Publishing Agreement](#)

1. Introduction

Quantum key distribution (QKD) allows two individuals, conventionally referred to as *Alice* and *Bob*, to communicate information in a secure and secret manner [1]. Since the proposal of the first protocol by Bennett and Brassard in 1984 (BB84) [1], various protocols and methods, for example Ekert91 [2] and six-state [3], have been further proposed and experimentally investigated. Notably, one class of quantum cryptographic schemes, namely high-dimensional QKD protocols, makes use of *qudits* rather than qubits, wherein the encoded quantum states belong to a higher-dimensional Hilbert space [4,5]. Such schemes have many potential advantages: in the case of an error-free channel, more than one bit of information can be distributed per carrier. Moreover, they tolerate larger error-thresholds due to the difficulties that an eavesdropper *Eve* has in getting information about the high-dimensional state [6]. This may allow for the implementation of QKD links in noisy environments with high quantum bit error rates (QBER). So far, various quantum channels have been studied in realistic conditions: free-space [7–9], including shorter line-of-sight intra-city links [8, 10], fibre networks [11] and ground-to-satellite links [12–15]. Recently, underwater quantum channels have been proposed and investigated theoretically [16, 17]. The first experimental demonstration of entanglement distribution through a 3 m-long water tube was recently achieved using polarization [18]. Insofar, secure communication through an

underwater quantum channel has yet to be demonstrated in an outdoor environment or in higher dimensions.

2. Experimental results

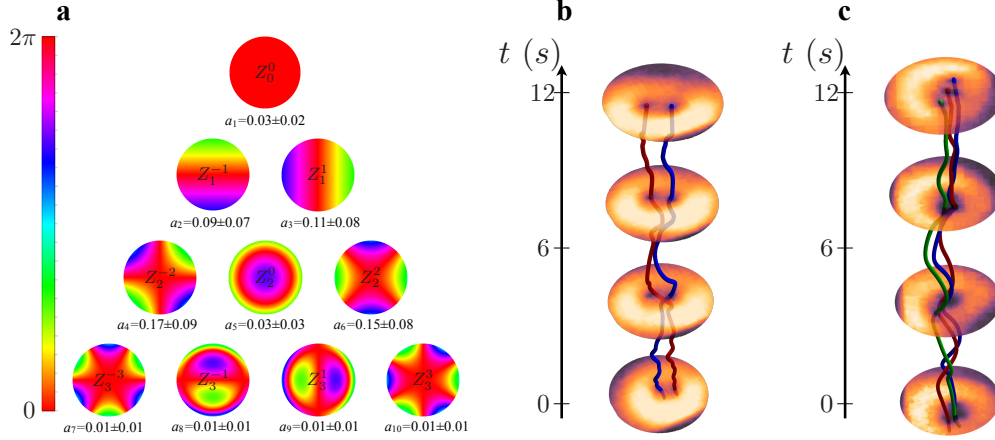


Fig. 1. Experimental characterization of underwater turbulence. (a) Calculated coefficients for the lowest ten Zernike polynomials from intensity images of a Gaussian beam after propagation through 3 m of water to characterize the turbulence in one particular set of conditions at the time of measurement. The dominant coefficients correspond to oblique and vertical astigmatism (a_4 and a_6), followed by tip and tilts effects (a_2 and a_3). The Zernike decomposition was carried out over a disk with a radius of 2.1 mm, which corresponds to $2w_0$, where $w_0 = 1.05$ mm is the beam radius at the input of the channel. (b) - (c) Evolution of vortex splitting over a 12 s period for a $\ell = 2$ and $\ell = 3$ modes, respectively, sent through 5 m of water. The red, blue, and green lines represent the trajectories of the individual singularities, highlighting their splitting and wandering that occurs due to the turbulence.

Photons are the carriers of choice for quantum communication, possessing multiple degrees of freedom with which information can be encoded. Polarization [1], time-bins [19], and spatial modes [20] are the most prevalent encryption methods, with the last two being common methods for achieving high-dimensional protocols. One family of spatial modes with mature preparation and measurement techniques is the OAM of light, also referred to as twisted photons [21, 22]. These modes possess a helical wavefront given by $\exp(i\ell\varphi)$, where ℓ is an integer and φ is the transverse azimuthal coordinate. The OAM states of photons is one realization of a Hilbert space with unbounded dimensionality. Since the modes form a complete orthonormal basis, these states can be used for high-dimensional QKD schemes [23–25]. In this Article, we report the effect of water turbulence on OAM modes of light in an outdoor swimming pool, and study its effect in quantum cryptographic schemes, performing a high-dimensional BB84 protocol with twisted photons.

Since the underwater quantum channel is an outdoor link, uncontrolled turbulent conditions can be expected, as in the case of free-space links, introducing additional errors and losses to the system [26]. Turbulence is observed in the form of beam distortions and beam wandering after propagating through a turbulent media. The effect of turbulence on the propagation of OAM modes through free-space air has been studied for various distances. In the Kolmogorov theory of turbulence in free-space, the turbulence is associated with a local variation in the refractive index due to temperature and pressure variations [27]. However, temperature gradients

in the atmosphere represent the main contribution to atmospheric turbulence. Water is an incompressible fluid and thus the main contribution to the optical turbulence is derived from local variations in temperatures. Recently, propagation of OAM modes through water has been reported in controlled laboratory conditions [28, 29]. Our experiments were performed in a 60,000 litres outdoor, in-ground pool, see the appendix-B for more details. The water was exposed to temperatures between 27°C during the day to 17°C at night. This creates a temperature gradient between the top and bottom of the pool, which was inhomogeneously mixed by built-in water jets. Further details of the experimental setup are presented in the appendix-B.

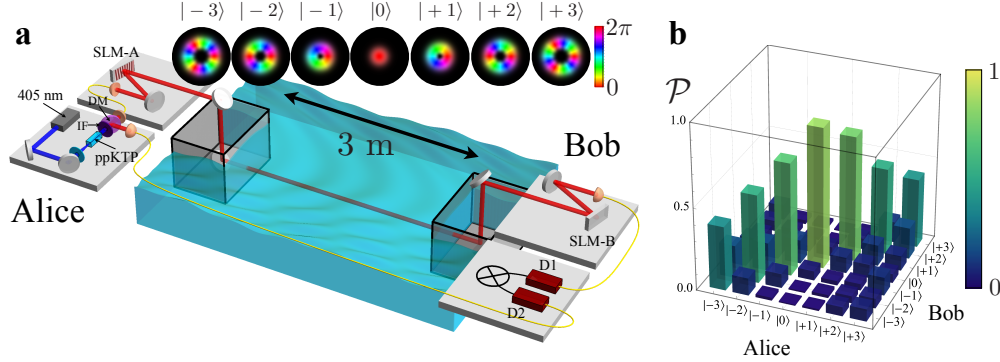


Fig. 2. Experimental setup and state cross-talk measurements. (a) Photon pairs (signal $\lambda_s = 710 \text{ nm}$, idler $\lambda_i = 943 \text{ nm}$) are generated via spontaneous parametric downconversion pumped from a periodically poled KTP (ppKTP) crystal by a 405 nm diode laser. A long pass filter (IF) blocks the UV and transmits the photon pairs, which are then split at a dichroic mirror (DM). The idler photon is directly detected by a single photon detector (D2) and acts as a heralding trigger for the information-carrying signal photon. Alice prepares the signal photon into a particular state, for example one from the insets, using SLM-A, then sends it to Bob through the 3 m underwater link. Bob performs a measurement on the received state using SLM-B and a single mode optical fibre connected to D1. Coincidence events between D1 and D2 are recorded. (b) Measured cross-talk matrix between the OAM states ($\ell = -3$ to 3) that Alice sends and Bob measures. Higher order states experience more cross-talk as compared to lower order states, seen as off-diagonal detection probabilities.

A characterization of the level of turbulence, assuming the single phase screen approximation, in our 3 m underwater channel is performed by sending a 635 nm Gaussian-shaped laser beam through the water and record the transmitted intensity patterns (see Turbulence Characterization in Methods for more details). We employ the Gerchberg-Saxton algorithm (GSA), a phase retrieval algorithm using fast Fourier transforms [30], to reconstruct the phase of the beam after propagating through the water. The obtained phase profile, $\Phi(r, \varphi)$, is then decomposed in terms of Zernike polynomials, which forms a set of orthonormal polynomials on the unit disk [31],

$$\Phi(r, \varphi) = \sum_j a_j Z_j(r, \varphi), \quad (1)$$

where r and φ are the radial and azimuthal coordinates, respectively, a_j are the Zernike coefficients, $Z_j(r, \varphi) = Z_n^m(r, \varphi)$ are the Zernike polynomials (defined in the Methods), $j = 1 + (n(n+2) + m)/2$ is the Noll index, and n and m are the radial and azimuthal degree, respectively.

The average values of measured expansion coefficients a_j as well as their corresponding Zernike polynomials are shown in Fig. 1-a. In particular, low-order Zernike polynomials have specific meaning in terms of optical aberrations. First order aberrations, $n = 1$ ($j = 2, 3$),

correspond to a tip-tilt in the wavefront. In the weak atmospheric turbulence regime, tip-tilt is the major contribution and results in beam wandering. Second order optical aberrations, $n = 2$, are related to astigmatism ($j = 4, 6$) and defocusing ($j = 5$). It can be seen from Fig. 1-(a), that the contribution of astigmatism in our turbulent underwater link is the largest. Further analysis of the turbulence is presented in the appendix-A.

In particular, one effect of astigmatism on OAM modes is the singularity splitting for OAM values of $|\ell| > 1$; this splitting effect has also recently been studied in free-space [32]. The effect of vortex splitting in our underwater link is shown in Fig. 1-(b) and Fig. 1-(c), where an $\ell = 2$ and $\ell = 3$ mode respectively, each generated by a phase-only spatial light modulator (SLM), is sent through a slightly longer distance of 5 m. Hence, underwater channels may give rise to turbulent conditions that are fundamentally different from those present in a free-space channel. However, the turbulence was observed to change on a much slower time-scale as opposed to free-space, on the order of 10 Hz compared to 100 Hz. Thus, implementing a SLM in an adaptive optics type system might be fast enough to correct for the aberrations.

Our experimental setup, see Fig. 2-(a), for investigating QKD consists of a heralded single photon source (for more details see Experimental Setup in Methods), Alice's state preparation setup, Bob's measurement setup, and a 3 m-outdoor underwater link. In the near-infrared region, light is strongly absorbed by water; ideally, it is desirable to produce signal photons with a λ_s in the blue-green window (≈ 400 -600 nm) which experiences the least amount of absorption. In the heralded single-photon source, the signal ($\lambda_s = 710$ nm) and idler ($\lambda_i = 940$ nm) photons are generated by spontaneous parametric downconversion, and are coupled to single-mode optical fibres (SMOF) in order to filter their transverse spatial modes to the fundamental Gaussian mode. A coincidence rate of 432 kHz, within a coincidence time window of 5 ns, is measured after the SMOFs at the source. The idler photon is sent through a fibre delay line to Bob, acting as the heralding photon, and the signal photon is sent to Alice's generation apparatus. In order to eliminate the distortions that an air-water interface would introduce to the wavefront of the transmitted and received photons, we use periscopes to guide the photons into/out of glass tanks that are partially immersed in the water on either end of the link. The advantage of using such a configuration is that the photons pass through first a flat air-glass then a glass-water interface, and *vice versa*, without significant alterations to their wavefronts. For the quantum cryptographic tests, Alice prepares the signal photon into an OAM state using a SLM, then sends it across the underwater link. Bob uses a SLM and SMOF to project the received signal photons onto a given OAM state and records a coincidence event between the result and the heralding photon at a coincidence box [33].

We perform a cross-talk measurement of several OAM states ranging from -3 to 3 , i.e. $\{|\ell\rangle; \ell = -3, -2, -1, 0, 1, 2, 3\}$, see Fig. 2-(b), where $|\ell\rangle$ represents the quantum state with helical wavefront of $\exp(i\ell\varphi)$. The cross-talk measurements are a good indicator of the level of errors (QBER) that one could expect in a QKD protocol. Practical implementations are seen to dictate the optimal dimensionality of the qudits used in a specific high-dimensional quantum cryptographic scheme. The OAM mode that experiences the least amount of cross-talk is the fundamental Gaussian mode ($\ell = 0$), with a cross-talk of $< 15\%$ with its neighbouring modes ($\ell = \pm 1$). This cross-talk could lead to sufficiently low QBER to securely transmit information, given a small OAM encryption subspace. As we go to larger OAM values, the modes suffer larger cross-talk, which makes the extension to higher-dimensions challenging. Explicitly, the effect of turbulence on a QKD protocol is twofold: it introduces errors and losses. Loss in the underwater channel can be attributed to absorption from the water, but also from the turbulence. An approximate absorption coefficient at 710 nm was measured in the lab to be 1.2 m^{-1} , which is on the same order of magnitude of tabulated values [34]. This corresponds to approximately 3% transmission after 3 m of underwater propagation. On the other hand, turbulence can also cause loss by beam wandering and distortion effects, characterized by the Zernike coefficients in

Fig. 1-(a), wherein the photons are shifted or stretched outside of the collection area of Bob's optics. Most QKD protocols are robust against losses at the cost of a reduced key rate. However, the effect of errors is more critical since the protocol must be aborted if the error level exceeds a set threshold.

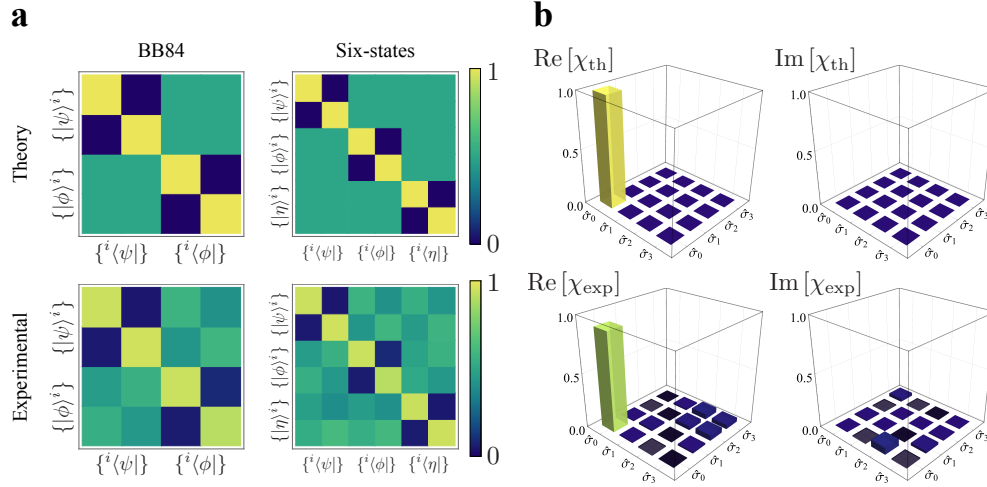


Fig. 3. Probability-of-detection matrices for $d=2$ BB84 and Six-states protocols, and the channel process matrix. (a) Theoretical and experimentally measured probability-of-detection matrices for BB84 (left column) and Six-states (right column) protocols in $d = 2$. We measured QBERs of $Q = 6.57\%$ and $Q = 6.35\%$, respectively, for these two protocols, corresponding to secret key rates of $R = 0.301$ and $R = 0.395$. (b) The six-state protocol is a tomographic protocol and can be used to reconstruct the process tomography matrix; the real and imaginary parts of the theoretical matrix are shown in the top row. The experimentally measured process matrix is shown in the bottom row with a process fidelity of $\mathcal{F} = 0.905$.

3. Discussion

As a first test of our underwater QKD link, we perform a 2-dimensional BB84 protocol. Alice uses the OAM subspace consisting of $\ell = \pm 1$ to encode the information. In the BB84 protocol, two mutually unbiased bases (MUBs) are required for Alice and Bob to encode and measure the states of the photons. The first MUB here is given by the logical basis, $|\psi\rangle^i \in \{|-1\rangle, |+1\rangle\}$, and the second MUB is given by $|\varphi\rangle^i \in \{|+\rangle, |-\rangle\}$, where $|\pm\rangle = (|-1\rangle \pm |+1\rangle)/\sqrt{2}$. The experimental probability-of-detection matrix is shown in Fig. 3-(a) (left column) along with its theoretical counterpart. The secret key rate per sifted photon, R , may be calculated using the following formula, $R(Q) = 1 - 2h(Q)$, where Q is the QBER and $h(\cdot)$ is the Shannon entropy. From the probability-of-detection matrix, a QBER of $Q = 6.57\%$ is calculated, which is below the error threshold of $Q_{\text{threshold}}^{2D} = 11\%$ for the 2-dimensional BB84 protocol, corresponding to a positive secret key rate of $R = 0.301$ bits per sifted photon.

An extension of the BB84 protocol in dimension $d = 2$ is achieved by considering a third MUB, i.e. $|\eta\rangle^i \in \{|+i\rangle, |-i\rangle\}$, where $|\pm i\rangle = (|-1\rangle \pm i|+1\rangle)/\sqrt{2}$. This protocol, also known as the *Six-states* protocol [35], can tolerate slightly larger error thresholds of around $Q = 12.6\%$. The probability-of-detection matrix is shown in Fig. 3-(a) (right column), where a QBER of $Q = 6.35\%$ is measured resulting in a secret key rate of $R = 0.395$ bits per sifted photon. However, when considering sifting, the *six-states* protocol suffers from a lower sifting rate, i.e.

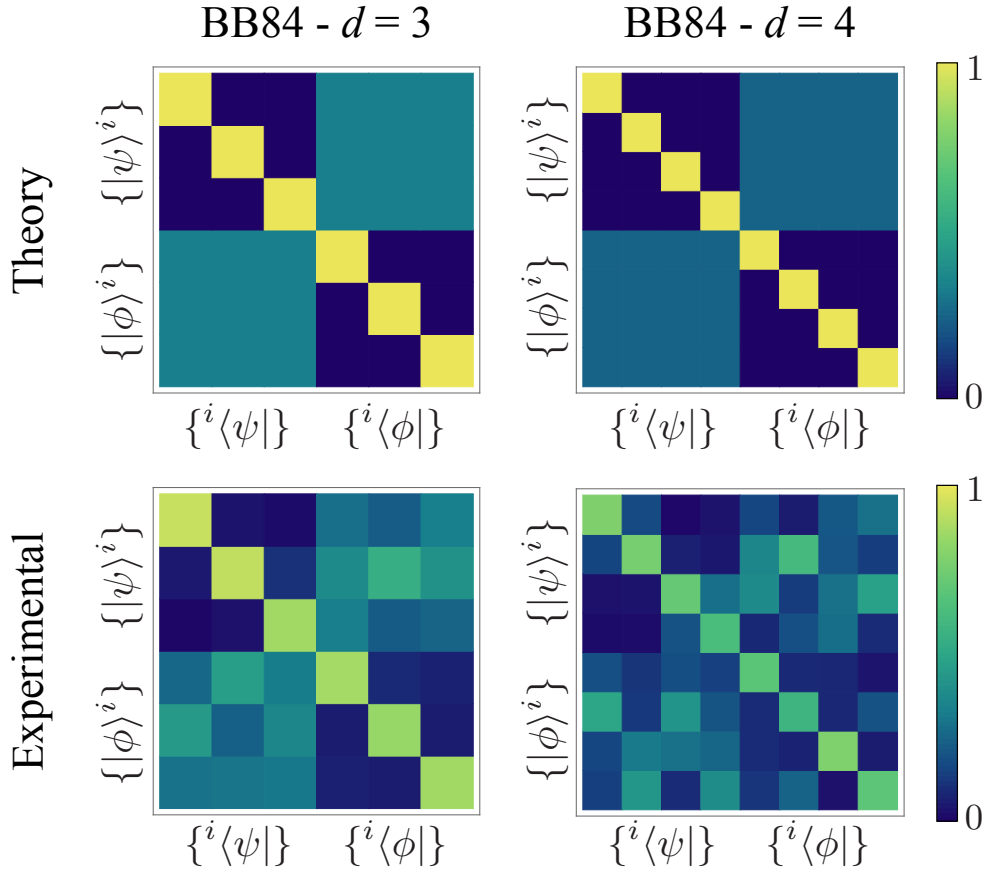


Fig. 4. High-dimensional probability-of-detection matrices. Theoretical (top row) and experimentally measured (bottom row) probability-of-detection matrices for BB84 protocols in $d = 3$ and $d = 4$. We measured QBER of $Q^{3D} = 11.73\%$ and $Q^{4D} = 29.77\%$, respectively. The QBER in $d = 3$ is below the tolerable error threshold, allowing for the establishment of a secret key rate of $R^{3D} = 0.307$ bits per sifted photon. However, the QBER in $d = 4$ exceeds the threshold of $Q_{\text{threshold}}^{4D} = 18.9\%$.

1/3, in comparison to the BB84 protocol, which has a sifting rate of 1/2. Nevertheless, the *six-states* protocol is a tomographic protocol: the measurements by Alice and Bob can be used to fully characterize the quantum channel and reconstruct the process matrix of the link via quantum process tomography. Let the channel be characterized by a process ε , which relates the input and output states in the following manner, $\hat{\rho}_{\text{out}} = \varepsilon(\hat{\rho}_{\text{in}})$. The process may be described by the process matrix χ_{mn} , where $\varepsilon(\hat{\rho}) = \sum_{mn} \chi_{mn} \hat{\sigma}_m \hat{\rho} \hat{\sigma}_n^\dagger$, and $\hat{\sigma}_m$ are the Pauli matrices. The reconstructed process matrix, χ_{exp} , along with the theoretical ideal process matrix, χ_{th} , is shown in Fig. 3-(b). A process fidelity of $\mathcal{F} = 0.905$ is measured from the process matrix, where the process fidelity is defined as $\mathcal{F} = \text{Tr}[\chi_{\text{exp}} \cdot \chi_{\text{th}}] / \text{Tr}[\chi_{\text{th}} \cdot \chi_{\text{th}}]$.

The versatility of our experimental configuration allows us to test different types of QKD protocols in our underwater link. As a next step, we perform a high-dimensional quantum cryptographic scheme. The standard BB84 protocol is naturally extended using high-dimensional states, where two d -dimensional bases are employed. The first MUB is given by the logical basis, $|\psi\rangle^i \in \{|i\rangle; i = 1, 2, \dots, d\}$, and the second MUB is given by the discrete Fourier transform $|\varphi\rangle^i \in \{\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega_d^{ij} |j\rangle\}$, where $\omega_d = \exp(i2\pi/d)$. We perform the 3- and 4-dimensional BB84 protocol using the OAM modes with $\ell = 0, \pm 1$ and $\ell = \pm 1, \pm 2$, respectively, in our underwater link. The results are shown in Fig. 4, where QBERs of $Q^{3D} = 11.73\%$ and $Q^{4D} = 29.77\%$ were measured for the case of $d = 3$ and $d = 4$, respectively. For the 3-dimensional BB84 ($Q_{\text{threshold}}^{3D} = 15.95\%$), a secret key rate of $R^{3D} = 0.307$ bits per sifted photon was obtained, which is slightly larger than the 2-dimensional BB84 secret key rate. For the 4-dimensional case, the QBER is above the error threshold, i.e. $Q_{\text{threshold}}^{4D} = 18.93\%$, meaning no secret key can be distributed across the turbulent underwater link with a 4-dimensional BB84 protocol with twisted



Fig. 5. Image of outdoor underwater link in an in-ground swimming pool. The single photon source, on the sender's side, is enclosed within a black box. The sender's setup is mounted on an optical breadboard and consists of a microscope objective stage, a spatial light modular, mirrors and a periscope which brings the beam in an air-filled aquarium that is half-way under the water. In order to stabilize the aquariums, they are secured to a ladder that is placed above the underwater link, but is not in direct contact with the optical breadboards. The idler photon is sent from the sender to the receiver through a single mode fiber that is mounted along the ladder. The receiver's setup is mounted on an optical breadboard and also consists of a periscope, mirrors, a spatial light modular and a microscope objective. Red lines were added to outline the beam's path.

photons. These errors originate from the aberrations induced by the underwater turbulence, introducing more cross-talk between higher OAM states. As mentioned previously, the frequency of the turbulence was on the order of tens of Hertz, which opens up the possibility to implement an adaptive optics system using the implemented SLMs on Alice's or Bob's side for correcting the aberrations. This procedure would provide a means for reducing the QBER below the error thresholds in higher-dimensions.

In summary, we have characterized the predominant turbulence effects in our underwater quantum channel to be astigmatism, outlining a notable difference between an air free-space and an underwater link. We have performed and compared different QKD protocols through this underwater link using twisted photons. For a short distance, i.e. 3 m, we were able to successfully achieve a positive secret key rate using a 2- and 3-dimensional BB84 protocol.

Appendix-A

Turbulence Characterization: A characterization of the level of turbulence in our underwater channel is done by sending a Gaussian laser beam, at a wavelength of 635 nm, over our 3 m underwater link, see Fig. 5. Short exposure images (0.07 ms) of the beam at the output of the link are recorded using a CCD camera. The water turbulence is characterized using a single phase screen approximation, i.e. we assumed the effect of turbulence can be described as a varying phase screen at the input of the link followed by uniform propagation. Assuming a Gaussian input beam, we use the intensity images recorded at the output of the link to reconstruct the phase of the input beam. The reconstructed input phase profile corresponds to the input single phase screen that models the turbulence of the channel. In order to obtain the phase of the output beam, we perform the Gerchberg-Saxton algorithm (GSA), a phase retrieval algorithm using fast Fourier transforms [30]. The obtained phase profile, $\Phi(r, \varphi)$, is then decomposed in terms of Zernike polynomials, which forms a set of orthonormal polynomials on the unit disk, $\Phi(r, \varphi) = \sum_j a_j Z_j(r, \varphi)$ as defined in the main text. Explicitly, the Zernike polynomials are

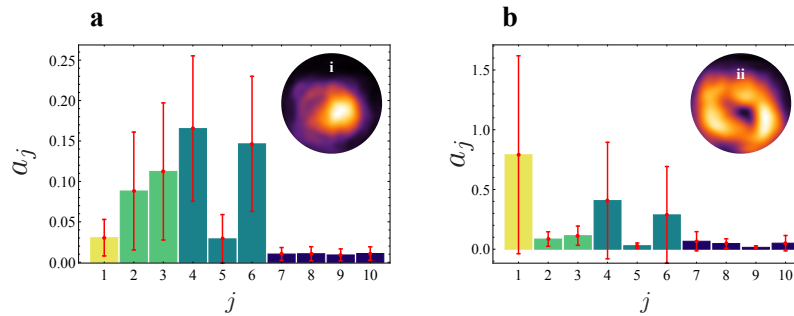


Fig. 6. Characterization of underwater turbulence. (a) Experimentally obtained coefficients for an input gaussian ($\ell = 0$) mode. Inset i, shows an example of a distorted gaussian beam profile at the output of the channel. The Zernike decomposition was carried over a disk with a radius of 2.1 mm, which corresponds to $2w_0$, where $w_0 = 1.05$ mm is the beam size at the input of the channel. (b) Experimentally obtained coefficients for an input orbital angular momentum beam ($\ell = 1$). Inset ii, shows an example of a distorted donut beam profile at the output of the channel. The Zernike decomposition was carried over a disk with a radius of 2.97 mm, which corresponds to $4w_0/\sqrt{2}$, where $w_0/\sqrt{2} = 0.74$ mm corresponds to the radius of maximum intensity of the donut beam at the input of the channel.

written in terms of the radial polynomial $R_n^m(r)$ [31],

$$Z_{\text{even } j}(r, \varphi) = \sqrt{n+1} R_n^m(r) \sqrt{2} \cos(m\varphi), \quad m \neq 0, \quad (2)$$

$$Z_{\text{odd } j}(r, \varphi) = \sqrt{n+1} R_n^m(r) \sqrt{2} \sin(m\varphi), \quad m \neq 0, \quad (3)$$

$$Z_j(r, \varphi) = \sqrt{n+1} R_n^0(r), \quad m = 0. \quad (4)$$

The GSA and Zernike polynomial decomposition is subsequently carried over all 143 images recorded at the output of the link. An example of experimentally obtained coefficients for $\ell = 0$ and $\ell = 1$ modes are shown in Fig. 6.

Appendix-B

In the heralded single photon source, a 405 nm diode laser (200 mW) pumps a periodically-poled potassium titanyl phosphate (ppKTP) crystal to produce single photon pairs via spontaneous parametric downconversion. A non-degenerate set of wavelengths is chosen to produce signal photons at $\lambda_s = 710$ nm, with corresponding idler photons at $\lambda_i = 943$ nm, see Fig. 7. We note that the wavelength of the signal photon could be adjusted to lie in the desired blue-green window with a different crystal along with commercially available single photon detectors which work at the IR. The signal and idler photons are coupled to single-mode optical fibres (SMOF) in order to filter their transverse spatial modes to the fundamental Gaussian mode. A coincidence rate of 432 kHz, within a coincidence time window of 5 ns, is measured after the SMOFs at the source. The corresponding single photon count rates for the signal and idler photons are given by 5 MHz and 1.5 MHz, respectively. The idler photon is sent through a fibre delay line to Bob, acting as the heralding photon, and the signal photon is sent to Alice's generation apparatus. The

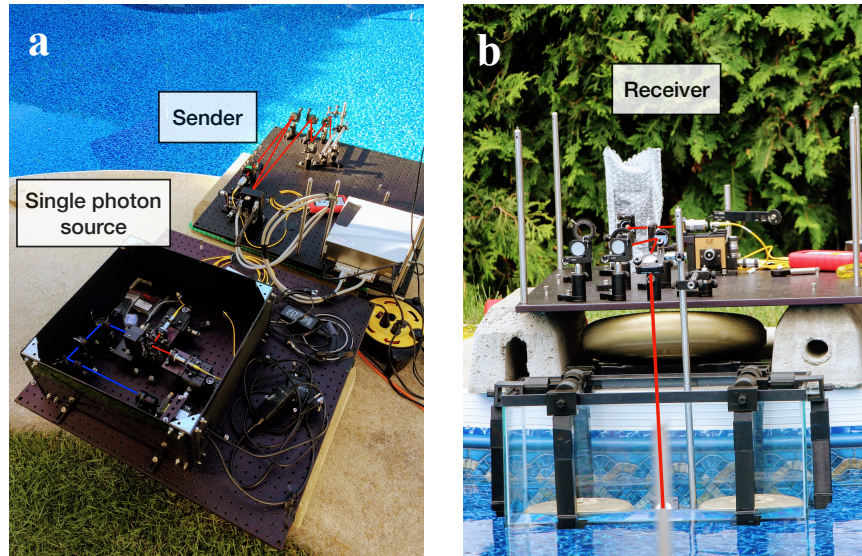


Fig. 7. Sender and receiver setup of the outdoor underwater link. (a) Close-up of the single photon source and the sender's setup. The blue line represents the pump beam and the red lines represent the signal and idler beams. (b) Close up of the receiver's aquarium, periscope and setup.

experiment was carried out during the night under the following weather conditions: temperature, relative humidity, wind speed and atmospheric pressure were measured as 17°C, 91%, 2 km/h and 100.79 kPa, respectively. The depth of the pool is 1.1 m and the beam was situated at 12 cm under the surface. The pH, Phosphate concentration, and water hardness were measured as 6.9, 318 ppb and 331 ppm, respectively.

Funding

Canada Research Chairs; Canada Foundation for Innovation (CFI); Canada Excellence Research Chairs, Government of Canada (CERC); Canada First Research Excellence Fund (CFREF); Natural Sciences and Engineering Research Council of Canada (NSERC); Max Planck-University of Ottawa Centre for Extreme and Quantum Photonics.

Acknowledgments

All authors would like to thank Norman Bouchard and Marie-France Langlois for access to their in-ground pool.

References

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," *Proc. IEEE Int. Conf. on Comput. Syst. Signal Process. Bangalore, India* **175**, 8 (1984).
2. A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.* **67**, 661 (1991).
3. Y. C. Liang, D. Kaszlikowski, B.-G. Englert, L. C. Kwek, and C. H. Oh, "Tomographic quantum cryptography," *Phys. Rev. A* **68**, 022324 (2003).
4. H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," *Phys. Rev. A* **61**, 062308 (2000).
5. N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," *Phys. Rev. Lett.* **88**, 127902 (2002).
6. F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, "High-dimensional quantum cloning and applications to quantum hacking," *Sci. Adv.* **3**, e1601915 (2017).
7. A. Muller, J. Breguet, and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km," *EPL (Europhysics Lett.)* **23**, 383 (1993).
8. W. Buttler, R. Hughes, P. Kwiat, S. Lamoreaux, G. Luther, G. Morgan, J. Nordholt, C. Peterson, and C. Simmons, "Practical free-space quantum key distribution over 1 km," *Phys. Rev. Lett.* **81**, 3283 (1998).
9. J. Rarity, P. Tapster, and P. Gorman, "Secure free-space key exchange to 1.9 km and beyond," *J. Mod. Opt.* **48**, 1887 (2001).
10. K. Resch, M. Lindenthal, B. Blauensteiner, H. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter, and A. Zeilinger, "Distributing entanglement and single photons through an intra-city, free-space quantum channel," *Opt. Express* **13**, 202 (2005).
11. R. Valivarthi, M. G. Puigibert, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak, W. Tittel, "Quantum teleportation across a metropolitan fibre network," *Nat. Photonics* **10**, 676 (2016).
12. J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-based entanglement distribution over 1200 kilometers," *Science* **356**, 1140 (2017).
13. J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, M. Li, Y.-M. Huang, L. Deng, L. Li, Qi. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-Ground Entanglement-Based Quantum Key Distribution," *Phys. Rev. Lett.* **119**, 200501 (2017).
14. J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, K.-X. Yang, X. Han, Y.-Q. Yao, J. Li, H.-Y. Wu, S. Wan, L. Liu, D.-Q. Liu, Y.-W. Kuang, Z.-P. He, P. Shang, C. Guo, R.-H. Zheng, K. Tian, Z.-C. Zhu, N.-L. Liu, C.-Y. Lu, R. Shu, Y.-A. Chen, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Ground-to-satellite quantum teleportation," *Nature* **549**, 70 (2017).
15. S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, "Satellite-Relayed Intercontinental Quantum Network," *Phys. Rev. Lett.* **120**, 030501 (2018).
16. P. Shi, S.-C. Zhao, W.-D. Li, and Y.-J. Gu, "Feasibility of underwater free space quantum key distribution," *arXiv preprint arXiv:1402.4666* (2014).

17. Y.-Y. Zhou and X.-J. Zhou, "Performance analysis of quantum key distribution based on air-water channel," *Optoelectronics Lett.* **11**, 149 (2015).
18. L. Ji, J. Gao, A.-L. Yang, Z. Feng, X.-F. Lin, Z.-G. Li, and X.-M. Jin, "Performance analysis of quantum key distribution based on air-water channel," *Opt. Express* **25**, 19795 (2017).
19. N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, "Provably secure and high-rate quantum key distribution with time-bin qudits," *Sci. Adv.* **3**, e1701491 (2017).
20. S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, "Experimental quantum cryptography with qutrits," *New J. Phys.* **8**, 75 (2006).
21. G. Molina-Terriza, J. P. Torres, and L. Torner, "Twisted photons," *Nat. Phys.* **3**, 305 (2007).
22. M. Erhard, R. Fickler, M. Krenn, and A. Zeilinger, "Twisted Photons: New Quantum Perspectives in High Dimensions," *Light. Sci. & Appl.* **7**, 17146 (2018).
23. M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, "High-dimensional quantum cryptography with twisted light," *New J. Phys.* **17**, 033033 (2015).
24. G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, "Free-space quantum key distribution by rotation-invariant twisted photons," *Phys. Rev. Lett.* **113**, 060503 (2014).
25. A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, "High-dimensional intracity quantum cryptography with structured photons," *Optica* **4**, 1006 (2017).
26. L. C. Andrews and R. L. Phillips, *Laser beam propagation through random media*, vol. 1 (SPIE Press, 2005).
27. A. N. Kolmogorov, "The local structure of turbulence in incompressible viscous fluid for very large reynolds numbers," *Doklady Akademii Nauk SSSR* **30**, 299–303 (1941).
28. Y. Ren, L. Li, Z. Wang, S. M. Kamali, E. Arbabi, A. Arbabi, Z. Zhao, G. Xie, Y. Cao, N. Ahmed, Y. Yan, C. Liu, A. J. Willner, S. Ashrafi, M. Tur, A. Faraon, and A. E. Willner, "Orbital angular momentum-based space division multiplexing for high-capacity underwater optical communications," *Sci. Reports* **6**, 33306 (2016).
29. J. Baghdady, K. Miller, K. Morgan, M. Byrd, S. Osler, R. Ragusa, W. Li, B. M. Cochenour, and E. G. Johnson, "Multi-Gigabit/s underwater optical communication link using orbital angular momentum multiplexing," *Opt. Express* **24**, 9794 (2016).
30. J. R. Fienup, "Phase retrieval algorithms: a comparison," *Appl. Opt.* **21**, 2758 (1982).
31. R. J. Noll, "Zernike polynomials and atmospheric turbulence," *J. Opt. Soc. Am.* **66**, 207 (1976).
32. M. Lavery, C. Peuntinger, K. Günthner, P. Banzer, D. Elser, R. Boyd, M. Padgett, C. Marquardt, and G. Leuchs, "Free-space propagation of high-dimensional structured optical fields in an urban environment," *Sci. Adv.* **3**, e1700552 (2017).
33. H. Qassim, F. M. Miatto, J. P. Torres, M. J. Padgett, E. Karimi, and R. W. Boyd, "Limitations to the determination of a Laguerre–Gauss spectrum via projective, phase-flattening measurement," *J. Opt. Soc. Am. B* **31**, A20 (2014).
34. S. A. Sullivan, "Experimental study of the absorption in distilled water, artificial sea water, and heavy water in the visible region of the spectrum," *J. Opt. Soc. Am.* **53**, 962-968 (1963).
35. D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Phys. Rev. Lett.* **81**, 3018 (1998).

Chapter 5

Quantum key distribution protocols in high dimensions

This chapter is based on the following papers:

1. **F. Bouchard**, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, & E. Karimi, “Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons”, *Quantum* **2**, 111 (2018).

DOI: <https://doi.org/10.22331/q-2019-05-06-138>

© 2019 Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften

2. **F. Bouchard**, A. Sit, K. Heshami, R. Fickler, & E. Karimi, “Round-Robin Differential Phase-Shift Quantum Key Distribution with Twisted Photons”, *Physical Review A* **96**, 010301(R) (2018).

DOI: <https://doi.org/10.1103/PhysRevA.98.010301>

© 2018 American Physical Society

5.1 Quantum key distribution protocols

In the previous chapters, we have investigated several important components of a high-dimensional QKD system and performed proof-of-principle experimental demonstrations of such systems in a free-space and underwater link. In all cases, we use the standard QKD protocol, namely BB84 generalized to higher dimensions. However, there are many options when it comes to choosing a QKD protocol, with all of them having their own advantages and inconveniences. Moreover, an advantage of using a larger encoding alphabet in high-dimensional QKD is the new possibilities to design new types of QKD protocols inaccessible with qubits.

Not long after the BB84 protocol was introduced [10], several QKD protocols using qubits were proposed. In 1991, Ekert independently proposed a quantum cryptographic protocol based on entanglement, known as the E91 protocol [7]. Such a protocol is now known as an *entanglement-based* protocol, whereas the BB84 is referred to as a *prepared-and-measure* protocol. Nevertheless, both types of protocols are completely equivalent using the source-replacement scheme. Moreover, it is often convenient to recast a prepare-and-measure protocol into its entanglement-based version for simplicity in the security proof [116]. One year later in 1992, Bennett showed that security can be achieved with only two non-orthogonal quantum states, e.g. $|H\rangle$ and $|D\rangle$, in his protocol now known as the B92 protocol [117]. Although important for our understanding of quantum cryptography, the B92 protocol suffered practicality due to its low tolerance to losses. This can be understood by considering a probabilistic cloning machine [118], where perfect clones may be created non-deterministically for linearly-independent quantum states such as $\{|H\rangle, |D\rangle\}$. Hence, an eavesdropper can send the perfect clones to Bob when the probabilistic cloning was successful, and discard the other photons. Thus, Alice and Bob must also monitor losses in addition to errors in order to detect the eavesdropper, which leaves the B92 protocol quite impractical. Since the set $\{|H\rangle, |V\rangle, |A\rangle, |D\rangle\}$ is not linearly-independent, the BB84 protocol does not require monitoring losses for eavesdropping purposes.

5.2 Tomographic protocols

In 1998, Bruß proposed an extension of the BB84 protocol, known as the *six-states* protocol [119], where all 3 MUB are used to encode information on the photons. In particular, the six-states protocol yields a channel characterization that is tomograph-

ically complete, as described in chapter 3. In this case, the effect of the eavesdropper is fully characterized, and a larger error rate can be tolerated. A few years later, the high-dimensional version of the six-states protocol was also proposed and analyzed [22], where $(d + 1)$ MUB are considered for dimensions that are powers of prime numbers. Nevertheless, MUBs are also known to be overcomplete, meaning a more efficient tomographically complete QKD protocol could exist. For instance, it is the symmetric informationally complete (SIC) positive operator-valued measures (POVMs) that achieve optimal QST, or equivalently QPT. Hence, a protocol known as the *Singapore* protocol [120] uses SIC POVMs and achieves a mutual information value that is higher than that of the six-states protocol. Moreover, it is believed that SIC POVMs exist for all dimensions including those that are not powers of prime numbers, allowing for tomographic QKD protocols in arbitrary dimensions.

5.3 Practical quantum key distribution

The first QKD protocols, i.e. BB84, E91 and B92, demonstrated the elegance and simplicity of quantum cryptography using highly symmetric schemes. Nevertheless, as the number of experimental demonstrations grows, new types of QKD protocols are required, namely *practical QKD*. In practical QKD, protocols based on pure formal elegance are not considered anymore. Rather, more complicated protocols are required to take into account real effects in implementations. A great example of such a practical QKD protocol is the SARG04 protocol introduced in 2004 by Scarani, Acín, Ribordy, and Gisin [121]. Surprisingly, a slight modification in the encoding scheme, i.e. the bits are encoded in the bases rather than in the states for the case of BB84, led to an increase in robustness to *photon number splitting attacks* [122]. Therefore, SARG04 was particularly designed for QKD implementations using attenuated laser sources. Not long after, a protocol known as the *decoy state* protocol [123], where different intensities are used, showed that attenuated laser sources and heralded single photon source can be as secure. Moreover, the decoy state protocol can be used with any other protocols since it only deals with the intensity of Alice's laser source.

5.4 Distributed-phase-reference protocols

An important class of practical QKD protocol that was inspired by actual experimental implementations is known as *distributed-phase-reference protocols* (DPR). In

particular, DPR protocols involve a train of weak coherent pulses where the information is essentially encoded in the relative phase of the pulses in the overall train of pulses. The advantage of DPR protocols resides in the fact that the generation of such states can be realized straightforwardly using a continuous-wave laser with a sequence of amplitude and phase modulators. Thus, relatively high secret key rate can be achieved through relatively long distances in fibres. The first proposal of such protocol is known as the *differential phase shift* (DPS) protocol [124]. In this protocol, Alice prepares a single photon in a superposition of three time-bins where the information is randomly encoded in the relative phase of the time-bins. Upon receiving Alice's sent photon, Bob feeds it through an unbalanced Mach-Zehnder interferometer, where the difference in path length of both arms of the interferometer is given by the time delay between successive time-bins. By measuring the time-of-arrival of the input photon as well as the output port from which the photon exits the interferometer, Bob determines the relative phase between two of the successive time-bins. Interestingly, the DPS protocol can be regarded as a high-dimensional ($d = 3$) protocol. Nevertheless, only one bit of secret key per photon is shared between Alice and Bob. Thus, the advantage of high-dimensional encoding is not used towards a larger information capacity. Rather, the high-dimensional protocol results in a larger key creation efficiency, i.e. $2/3$, where for the case of BB84 it is given by $1/2$ because of sifting, i.e. basis reconciliation between Alice and Bob. Not long after, another DPR protocol known as the *coherent one way* (COW) protocol [125] was introduced, where a simple experimental implementation resulted in a high key rate generation.

5.4.1 Round-robin differential phase shift protocol

Recently, new high-dimensional DPR protocols were proposed with new functionalities. In 2014, a protocol known as the *round-robin differential phase shift* (RRDPS) protocol was proposed, where for the first time the amount of information leaked to an eavesdropper is bound regardless of the disturbances in the channel. For instance, in the BB84 protocol, Alice and Bob must first monitor the signal disturbance in the channel using the error rate to estimate the amount of information leaked to the eavesdropper. Only after this step can they perform the proper amount of privacy amplification. Interestingly, the RRDPS protocol is also a high-dimensional protocol, where, as in the case of the original DPS protocol, only one bit of information is distributed per photon. In particular, Alice prepares a single photon in a superposition of L pulses, where the information is encoded in the relative phase of each pulse in

the superposition. Bob's detection apparatus is similar to that of the DPR protocol, with the exception that the time delay introduced by the unbalanced interferometer is randomly varied for each detection event. The advantage of high-dimensional encoding here is used towards removing the requirement of monitor signal disturbance. Furthermore, as the dimension of the protocol, i.e. the number of pulses for a single photon state, is increased, the amount of information leaked to the eavesdropper decreases. Since its proposal, several experimental demonstrations have been reported for dimensions of 5 [126], 65 [127], and 128 [128] using an active configuration, and for a dimension even up to 10^5 [129] using a passive configuration. In this chapter, we present a proof-of-principle experiment investigating the RRDPS protocol using superpositions of OAM modes instead of time-bins [97]. By doing so, we find that all of the generation and detection apparatuses can be replaced by a single phase element, respectively, allowing us to perform the protocol in dimensions ranging from 3 to 64, which is a record for OAM-based QKD.

5.4.2 Chau15 protocol

In an attempt to simplify the experimental implementation of the RRDPS protocol, a new protocol known as the Chau15 protocol [130, 131] was proposed. In this case, the information is encoded in the relative phase between two time-bins picked at random, resulting in a *qubit-like* qudit state of the form $(|i\rangle \pm |j\rangle)/\sqrt{2}$, for $i \neq j$, and $i, j = 0, \dots, d-1$. A surprising result of the Chau15 protocol, is that for a small enough dit error rate, i.e. for Bob measuring the values of i and j as prepared by Alice, a bit error rate of up to 50 % can be tolerated, which is by far the largest error threshold for a QKD protocol. Around the same time, two experimental demonstrations of the Chau15 protocol have been reported [132, 98]. The first one was achieved using time-bins, as proposed in the original theory paper, and the second used superpositions of OAM modes. The latter is the subject of this chapter, where we have performed the Chau15 protocol in dimensions 4 and 8, as well as compared its performances with other high-dimensional protocols, such as the high-dimensional BB84 protocol, the $(d+1)$ MUB protocol, and the Singapore protocol. In particular, all experiments were carried using the same experimental configuration. This allows us to determine the advantages of different protocols for varying conditions with a given experimental apparatus.

Round-robin differential-phase-shift quantum key distribution with twisted photons

Frédéric Bouchard,^{1,*} Alicia Sit,¹ Khabat Heshami,² Robert Fickler,¹ and Ebrahim Karimi^{1,3}¹*Department of Physics, University of Ottawa, Advanced Research Complex, 25 Templeton Street, Ottawa, ON, Canada K1N 6N5*²*National Research Council of Canada, 100 Sussex Drive, Ottawa, ON, Canada K1A 0R6*³*Department of Physics, Institute for Advanced Studies in Basic Sciences, 45137-66731 Zanjan, Iran*

(Received 6 March 2018; published 25 July 2018)

Quantum key distribution (QKD) offers the possibility for two individuals to communicate a securely encrypted message. A common technical requirement is the monitoring of signal disturbance in a QKD system to bound the information leakage toward an unwanted eavesdropper. Recently, the round-robin differential-phase-shift (RRDPS) protocol, which encodes bits of information in a high-dimensional state space, was proposed to introduce an upper bound on the amount of *Eve's* information based on dimensionality of prepared quantum states and randomized measurement settings. Since its introduction, many realizations of the RRDPS protocol were demonstrated using trains of coherent pulses (time bin encoding). Given that this realization of the protocol requires active and random choice of many delays in a delayed Mach-Zehnder interferometer, its implementation can be technically demanding. Here, we propose and experimentally demonstrate an implementation of the RRDPS protocol using the photonic orbital angular momentum degree of freedom in dimensions $L = 3-8, 16, 32$, and 64 . In particular, we show that Alice's generation stage and Bob's detection stage can each be reduced to a single phase element, greatly simplifying the implementation. Our scheme offers a practical path to using RRDPS protocol in free-space quantum channels.

DOI: [10.1103/PhysRevA.98.010301](https://doi.org/10.1103/PhysRevA.98.010301)

The early protocols of quantum key distribution (QKD), such as the BB84 protocol and others [1–4], demonstrated the power of quantum cryptography using simple and elegant schemes. Security can be ensured by the Heisenberg uncertainty principle where any eavesdropping attempt induces noise by disturbing the quantum state of the photons. This leads to common features of conventional QKD protocols where the guaranteed security is given by an upper bound on information leakage to a potential eavesdropper, *Eve*, based on the amount of signal disturbance. Monitoring the signal disturbance is performed by sacrificing a fraction of the transmitted photons. To ensure security, it is necessary to assume the worst-case scenario: estimated noises are the result of an adversary, *Eve*, eavesdropping on the channel. It has become increasingly evident that excessive signal monitoring in noisy quantum channels and other technical difficulties in implementations can become prohibitive in establishing a secure quantum communication link [5]. This motivates more practical protocols that are designed toward specific implementations, and also provides theoretical tools for a complete security analysis of a QKD system.

A promising avenue to increasing error tolerability in noisy environments is the use of high-dimensional systems, known as *qudits*, rather than *qubits* [6–8]. Additionally, high-dimensional QKD protocols are shown to transmit more information per carrier. A natural extension of the BB84 protocol leads to a secret key rate, in the infinite-sized-key limit, of $R = \log_2(d) - 2h^{(d)}(e_b)$, where d is the dimension, e_b is the QBER, and $h^{(d)}(\cdot)$ is the d -dimensional Shannon

entropy. Another class of high-dimensional QKD protocols are the *distributed-phase-reference* (DPR) schemes which, unlike the high-dimensional BB84 protocol, encode only one bit of information per carrier. This reduction in transmitted information comes with the benefit of increased error tolerance. The original differential-phase-shift (DPS) protocol [9] employs superpositions of high-dimensional states where the information is encoded in the relative phase of the qudits. In the differential phase *Chau15* protocol [10,11], the information is encoded in the relative phase of a “qubitlike” high-dimensional state [12]. The Chau15 protocol has the particular advantage of tolerating error rates of up to 50%. It is also possible to achieve a DPR scheme where more than one bit of information is transmitted [13]. However, monitoring the signal disturbance is still required to ensure security in these protocols.

Recently, a QKD scheme has been proposed in which the amount of information leakage is bounded by Alice's state preparation stage and Bob's measurement unit, and therefore eliminates the requirement for monitoring the signal disturbance [14]. This scheme, known as *round-robin differential-phase-shift* (RRDPS) QKD, is based on encoding a random bit sequence of length L in the phase of a coherent L -dimensional superposition state. After transmission through a quantum channel accessible to *Eve*, Bob randomly selects the setting of his interferometric measurement to record one classical bit from a phase difference measurement between two modes of the L -dimensional input state. In this Rapid Communication, we propose and experimentally demonstrate an implementation of RRDPS QKD based on the transverse mode of photons, in particular using the orbital angular momentum (OAM) degree of freedom. Our proposed scheme simplifies

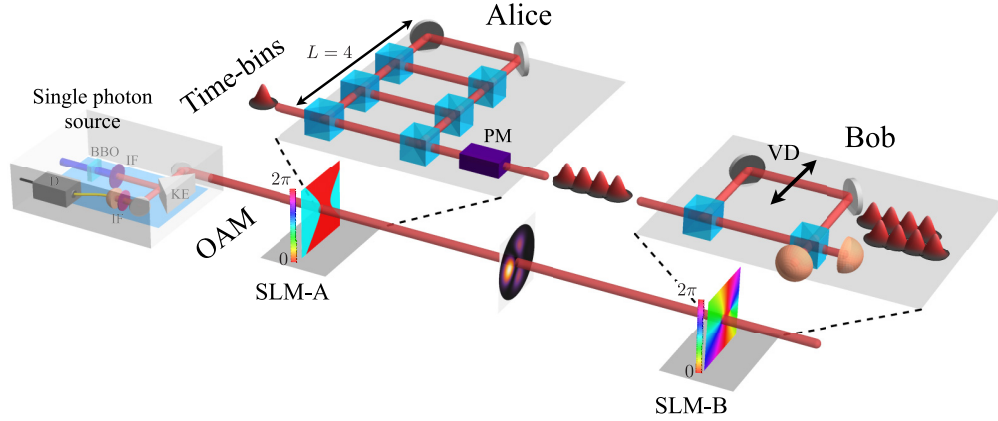


FIG. 1. Experimental setup: The original RRDPS scheme using the phase of time bins to encode information (depicted in the back) consisting of multiple interferometers for generation with a phase modulator (PM), and another interferometer with a variable delay (VD) for detection. By encoding using OAM instead, we can reduce the setups to be two phase holograms, displayed on spatial light modulators (SLMs), one for generation and one for detection of the states. An example of Alice's generation phase element for a state with $L = 4$, i.e., $s_\ell = (0, 0, 0, 0)$, is shown on her SLM-A. The intensity distribution of the generated state is shown in the channel, followed by Bob's measurement phase element (SLM-B) with a shift of $r = 1$ and a detected OAM value of $m = 2$ for a relative phase of 0. BBO: β -barium borate type I nonlinear crystal; IF: interference filter; KE: knife-edge mirror; D: detector.

the experimental setup for generation and detection with the ability to flexibly implement different dimensions, which we demonstrate for $L = 3$ – 8 , along with 16, 32, and 64.

The original proposal for implementation of the RRDPS QKD is based on state preparation in an L -pulse train single-photon state, and phase difference measurement using a switchable delayed interferometer with variable delays (see Fig. 1). Several experimental demonstrations of RRDPS QKD have used this encoding with active [16–18] or passive variable delays [15] using time-bin state dimensions of $L = 5$, 65, and 128, and even up to $L = 10^5$ with the passive configuration. The secret key rate, in the infinite-sized-key limit, is given by $R = 1 - h^{(2)}(e_b) - h[1/(L-1)]$ [14] and was recently improved to $R = 1 - h^{(2)}(e_b) - \max_{0 \leq x \leq 1} \varphi[(L-1)x, 1-x]/(L-1)$ [19], where $\varphi[x, y] = -x \log_2 x - y \log_2 y + (x+y) \log_2(x+y)$ and x is a variable to optimize over. Although these experiments highlight the described benefits in terms of error thresholds, they also demonstrate the expected challenges in implementing Bob's measurement unit that requires switchable delays and active stabilization of delayed interferometers. Given the practical implications of this scheme, it is desirable to explore encoding in other degrees of freedom of photons. Here, we investigate encoding on the OAM degree of freedom.

Photons carrying OAM are characterized by an $\exp(i\ell\phi)$ phase factor [20], where ℓ is an integer and ϕ is the transverse azimuthal angle, giving rise to ℓ intertwined helical wave fronts and a null of intensity along the propagation axis. The OAM of photons provides an unbounded Hilbert space [21], limited in practice by the numerical aperture of the system. OAM has provided a simplified way of realizing high-dimensional protocols. Only a single phase element is required for generation—typically a hologram displayed on a programmable spatial light modulator (SLM) [22,23]. For detection, a second SLM and single-mode fiber (SMF) [24,25] or OAM sorter [26,27] can be implemented to efficiently filter the different modes. High-dimensional QKD protocols using

OAM have been successfully demonstrated in the laboratory [28,29], studied and realized in realistic free-space conditions [30–32], and recently implemented in an underwater quantum channel [33]. Using these encryption techniques with OAM, we adapt previous RRDPS QKD schemes, which use many interferometers, to consist of two phase elements—one for state generation by Alice, and one for state measurement by Bob, shown in Fig. 1. In the original DPS proposal, Alice's generation is done by sending a single photon into an interferometer consisting of L arms. However, for practical considerations, a sequence of intensity modulators, phase modulators, and attenuator accomplishes the desired generation stage of Alice using weak coherent pulses. It is Bob's detection stage that presents the main technical challenges. Although using OAM modes of light is not as scalable as time bins, their generation and detection techniques do not require active stabilization.

Let us start with the preparation stage: Alice prepares an input state by encoding a random bit sequence of length L in the phases of different OAM states of a single photon,

$$|\psi^L\rangle = \frac{1}{\sqrt{L}} \sum_{\ell} (-1)^{s_\ell} |\ell\rangle, \quad (1)$$

where $s_\ell \in \{0, 1\}$, $|\ell\rangle$ are the OAM eigenstates that represent a single photon carrying $\ell\hbar$ units of OAM, analogous to the photon's time bin in the pulse train of the original RRDPS protocol, where $\hbar$ is the reduced Planck constant. For L even and odd, we respectively consider $\ell \in \{-L/2, \dots, L/2; \ell \neq 0\}$ and $\ell \in \{-(L-1)/2, \dots, (L-1)/2\}$ due to mode-symmetry reasons. Alice can generate this state with a single computer-generated hologram displayed on her SLM. One of the main advantages of using OAM states of photons is the inherent stability and interference visibility of superposition states. In spite of the fact that free-space propagation may alter the OAM superposition state due to Gouy phases [34], this effect is straightforward to control and compensate for. As one

considers larger values of L , the stability of the OAM state does not degrade as it might in the case of an interferometric configuration. However, the scalability is limited by the numerical aperture of the system.

Alice's photon is sent through the quantum channel and received at Bob's detection setup. In order to extract one qubit of information, following the original protocol, Bob sends the state into an interferometer and *shifts* one arm by a randomly chosen amount $r \in \{1, L-1\}$. For time-bin encoding, the shift corresponds to delaying each pulse in the train by rT , where T is the time between pulses. This *shift*-type interferometer may be achieved with OAM by inserting a phase element in one arm of a balanced interferometer. The phase element is given by $\exp(ir\phi)$, where this has the effect of shifting the OAM value analogously, i.e., $|\ell\rangle \rightarrow |\ell+r\rangle$. However, such configuration does not take full advantage of the OAM scheme. It can be seen that an interferometer with a phase-shift element in one arm and no phase element in the other arm is equivalent to a single phase element given by $[1 \pm \exp(ir\phi)]/\sqrt{2}$, where the relative phase ($\pm$) determines the "output port" of the interferometer. The last step in the RRDPS detection scheme is the time-resolved detection of the interfered pulse train. This is equivalent to any OAM detection scheme such as mode filtering [24] or OAM sorting [26]. Mode filtering is achieved using a phase element given by $\exp(-im\phi)$, which corresponds to a projection onto the state $|m\rangle$, followed by coupling into a SMF. A further simplification is done by combining the "measurement" phase element with the "shifting-interferometer" phase element, resulting in a phase of $\exp(-im\phi)[1 \pm \exp(ir\phi)]/\sqrt{2}$. This can be seen as a projection onto the state $|r, m\rangle = (|m\rangle \pm |m-r\rangle)/\sqrt{2}$, labeled by the random shift of r and a projection onto the state with OAM value of m , i.e., $|\langle\psi^L|r, m\rangle|^2$. Our simplified detection configuration corresponds to a filter-based scheme, resulting in a lower detection efficiency. However, by replacing the phase-flattening component with a sorter-type measurement device, the presifting detection efficiency can reach unity.

In the event of detecting a click from displaying $(|m\rangle - |m-r\rangle)/\sqrt{2}$ or $(|m\rangle + |m-r\rangle)/\sqrt{2}$, Bob records a 0 or 1, respectively. In order for Alice to have a shared corresponding bit, Bob publicly announces the random indices m and r . Alice obtains her sifted key bit by computing $s = s_m \oplus s_{m-r}$, where $\oplus$ corresponds to summation modulo 2. Moreover, Alice and Bob only keep the outcomes where $m \leq L$ with a sifting efficiency of $1/2$, as in the case of BB84.

Based on the proposed simplified scheme above, we perform a proof-of-principle experimental realization of the RRDPS protocol using OAM encoded on heralded single photons. We pump a 3 mm β -barium borate type I nonlinear crystal with a quasicontinuous wave UV laser at 355 nm to produce single-photon pairs (signal and idler) at 710 nm via spontaneous parametric down-conversion. The photons are spatially filtered to the fundamental Gaussian mode by coupling them to SMF with a measured single-photon heralding coincidence rate of 40 kHz within a coincidence window of 5 ns. Using a Hanbury-Brown and Twiss interferometer in a three-detector measurement configuration, the degree of

second-order coherence of our single-photon source is given by $g^{(2)}(0) = 0.015 \pm 0.004$. Alice prepares the signal photon into an equally weighted superposition of OAM states with a phase-only SLM (X10468-07; Hamamatsu), where a string of L bits is encoded in the phase (0 or π) of each OAM state using an intensity masking technique [35]. She subsequently distributes the photon to Bob through one meter of free-space in the laboratory. We note that when considering all 2^L possible bit sequences, the second half of the corresponding states are identical to the first half with an additional global phase of π . Hence, Alice randomly chooses one state out of the set of 2^{L-1} possible superposition states, $\{|\psi^L\rangle^i\}$, with distinct bit sequences. Bob projects the received state, using his own SLM (X10468-07; Hamamatsu) and SMF, onto a particular superposition of two OAM states from a choice of $L(L-1)/2$ possibilities, i.e., $|\eta\rangle = |r, m\rangle$. The idler photon is used to herald the presence of the signal photon for a coincidence event after Bob's measurement using single-photon detectors (ID120-500-800 nm; ID Quantique) with a dark count rate of less than 50 Hz. Due to the lossy nature of the above-mentioned intensity masking technique, the transmission of our experimental setup considering SLMs and coupling to SMF is approximately given by 5%.

The experiment is performed, under identical laboratory conditions, for values of L ranging from 3 to 8, 16, 32, and 64; the results for 3–8 are shown in Fig. 2. The measured probability-of-detection matrices shown represent the likelihood that Bob detects a click following the projection of the incoming photon's state onto $|\eta\rangle = (|m\rangle + |m-r\rangle)/\sqrt{2}$. Figure 2 also shows the experimentally extracted QBER with respect to dimension (L). Both the original [14] and improved [19] theoretical QBER thresholds of the RRDPS protocol security analyses are also shown along with the experimental QBER. For small dimensions, i.e., $L = 3-5$, the QBER exceeds the original error thresholds. In particular, for the case of $L = 3$, the original protocol cannot generate secret key bits. However, the improved theoretical bounds show that secure communication would still be feasible in all measured dimensions. Interestingly, above $L = 5$, the experimental QBERs are lower than the original thresholds, which appears to increase faster than our systematic errors do with dimension. The associated secret key rates, R , calculated from the improved RRDPS protocol, are given in Fig. 3 along with the theoretical secret key rates. Values of $e_b^{L=3} = 0.016$, $e_b^{L=4} = 0.019$, $e_b^{L=5} = 0.034$, $e_b^{L=6} = 0.039$, $e_b^{L=7} = 0.053$, $e_b^{L=8} = 0.056$, $e_b^{L=16} = 0.069$, $e_b^{L=32} = 0.139$, and $e_b^{L=64} = 0.315$ were obtained experimentally for the QBER. The corresponding secret key rates are $R^{L=3} = 0.188$, $R^{L=4} = 0.310$, $R^{L=5} = 0.322$, $R^{L=6} = 0.358$, $R^{L=7} = 0.339$, $R^{L=8} = 0.359$, $R^{L=16} = 0.440$, $R^{L=32} = 0.301$, and $R^{L=64} = 0.032$ bits per sifted photon, respectively.

The optimal dimension for our experimental implementation is found to be at $L = 16$. We may now compare our OAM-based implementation with an established RRDPS implementation based on time bins. With an overall transmission efficiency and QBER of 5% and 0.069, respectively, our scheme generates a secret key rate per photon that is on the same order as those reported in [17] using time bins and weak coherent pulses. However, in terms of secret key rate

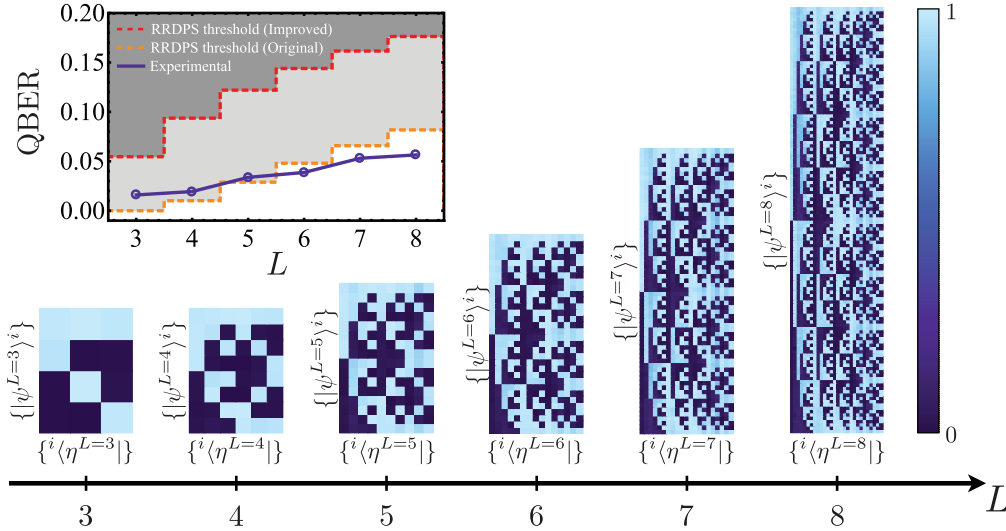


FIG. 2. Experimental results: Measured probability-of-detection matrices for RRDPS QKD scheme with OAM for dimensions $L = 3$ to $L = 8$. The rows consist of the 2^{L-1} states, $\{|\psi^i\rangle\}$, that Alice generates. The columns are the $L(L-1)/2$ measurements, $\{|\eta^j\rangle\}$, that Bob performs to determine the relative phase between two of the OAM states. Here, we are showing the results for when the two states are in-phase, i.e., relative phase of 0. The inset graph compares the quantum bit error rate (QBER) with increasing dimension between the theoretical original [14] and improved RRDPS [19] error thresholds and our experimentally measured QBER.

per second, our experimental implementation is limited in terms of repetition rate due to the restricted refresh rate of the SLMs.

For the cases of $L = 16, 32$, and 64 , in the interest of time, a subset of 1500 randomly selected generation and measurement settings is considered out of the $2^{L-1}L(L-1)/2$ possibilities. Interestingly, it is for the case of $L = 16$ that the largest secret key rate is achieved. We see an increased error rate (decrease in secret key rate) for higher dimensions most likely due to the limiting numerical aperture of our system and due to the SLM resolution. One potential way to circumvent this issue would be to extend our scheme to include radial modes

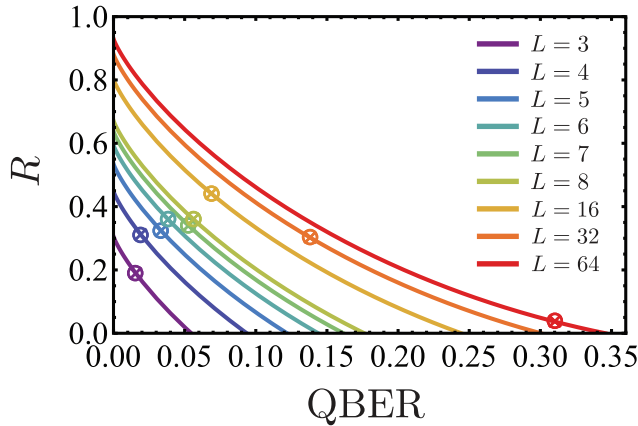


FIG. 3. Secret key rates: Calculated secret key rates (circles), R , for dimensions $L = 3-8, 16, 32$, and 64 from the experimentally measured QBERs with respect to the improved theoretical bounds (solid curves). As the dimension increases, the number of transmitted bits per sifted photon increases until we are limited by the numerical aperture of our system for higher dimensions.

[36,37] to make use of the full transverse spatial structure, i.e., optimize the best number of modes to fill the numerical aperture.

Finally, another advantage of our proposed scheme is the versatility of the experimental configuration. In the first place, the phase elements may be achieved using various techniques according to practical considerations, e.g., liquid-crystal devices [22,38], digital micromirror devices [39], refractive elements [40], metasurfaces [41–43], etc. However, SLM are limited in terms of repetition rate, leaving room for other approaches for faster spatial phase modulation of light. Moreover, the experimental configuration of our proposed scheme is compatible with many other prepare-and-measure high-dimensional QKD protocols such as BB84 [1], mutually unbiased bases-based protocols [28,44], Singapore [45], DPS [9], and Chau15 [10,11]. For fluctuating environmental conditions, Alice and Bob may adapt by selecting the most favorable QKD protocol. Hence, a single experimental configuration compatible with many protocols exhibits the versatility of QKD schemes based on OAM encoding [46]. The RRDPS scheme is one such example where the difficulty of monitoring signal disturbance is removed and may lead to improved performances in noisy environments. It will be important to see how this scheme performs in real-world conditions, in particular where there is atmospheric turbulence.

All authors would like to thank D. England for fruitful discussions. F.B. acknowledges the financial support of the Vanier graduate scholarship of the NSERC. R.F. acknowledges the financial support of the Banting postdoctoral fellowship of the NSERC. This work was supported by Canada Research Chairs (CRC), Canada Foundation for Innovation (CFI), Canada First Research Excellence Fund (CFREF), and Natural Sciences and Engineering Research Council of Canada (NSERC).

- [1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
- [2] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
- [3] C. H. Bennett, *Phys. Rev. Lett.* **68**, 3121 (1992).
- [4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
- [5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2009).
- [6] H. Bechmann-Pasquinucci and A. Peres, *Phys. Rev. Lett.* **85**, 3313 (2000).
- [7] H. Bechmann-Pasquinucci and W. Tittel, *Phys. Rev. A* **61**, 062308 (2000).
- [8] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, *Phys. Rev. Lett.* **88**, 127902 (2002).
- [9] K. Inoue, E. Waks, and Y. Yamamoto, *Phys. Rev. Lett.* **89**, 037902 (2002).
- [10] H. F. Chau, *Phys. Rev. A* **92**, 062324 (2015).
- [11] H. F. Chau, Q. Wang, and C. Wong, *Phys. Rev. A* **95**, 022311 (2017).
- [12] S. Wang, Z.-Q. Yin, H. F. Chau, W. Chen, C. Wang, G.-C. Guo, and Z.-F. Han, *Quantum Sci. Technol.* **3**, 025006 (2018).
- [13] D. Bacco, J. B. Christensen, M. A. U. Castaneda, Y. Ding, S. Forchhammer, K. Rottwitz, and L. K. Oxenløwe, *Sci. Rep.* **6**, 36756 (2016).
- [14] T. Sasaki, Y. Yamamoto, and M. Koashi, *Nature (London)* **509**, 475 (2014).
- [15] J.-Y. Guan, Z. Cao, Y. Liu, G.-L. Shen-Tu, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Ma, Q. Zhang, and J.-W. Pan, *Phys. Rev. Lett.* **114**, 180502 (2015).
- [16] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, *Nat. Photonics* **9**, 827 (2015).
- [17] S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, *Nat. Photonics* **9**, 832 (2015).
- [18] Y.-H. Li, Y. Cao, H. Dai, J. Lin, Z. Zhang, W. Chen, Y. Xu, J.-Y. Guan, S.-K. Liao, J. Yin, Q. Zhang, X. Ma, C.-Z. Peng, and J.-W. Pan, *Phys. Rev. A* **93**, 030302 (2016).
- [19] Z.-Q. Yin, S. Wang, W. Chen, Y.-G. Han, R. Wang, G.-C. Guo, and Z.-Fu Han, *Nat. Commun.* **9**, 457 (2018).
- [20] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman, *Phys. Rev. A* **45**, 8185 (1992).
- [21] M. Erhard, R. Fickler, M. Krenn, and A. Zeilinger, *Light: Sci. Appl.* **7**, 17146 (2018).
- [22] N. Heckenberg, R. McDuff, C. Smith, and A. White, *Opt. Lett.* **17**, 221 (1992).
- [23] A. Forbes, A. Dudley, and M. McLaren, *Adv. Opt. Photonics* **8**, 200 (2016).
- [24] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, *Nature (London)* **412**, 313 (2001).
- [25] H. Qassim, F. M. Miatto, J. P. Torres, M. J. Padgett, E. Karimi, and R. W. Boyd, *J. Opt. Soc. Am. B* **31**, A20 (2014).
- [26] G. C. G. Berkhout, M. P. J. Lavery, J. Courtial, M. W. Beijersbergen, and M. J. Padgett, *Phys. Rev. Lett.* **105**, 153601 (2010).
- [27] H. Larocque, J. Gagnon-Bischoff, D. Mortimer, Y. Zhang, F. Bouchard, J. Upham, V. Grillo, R. W. Boyd, and E. Karimi, *Opt. Express* **25**, 19832 (2017).
- [28] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, *Phys. Rev. A* **88**, 032305 (2013).
- [29] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O’Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, *New J. Phys.* **17**, 033033 (2015).
- [30] G. Vallone, V. D’Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, *Phys. Rev. Lett.* **113**, 060503 (2014).
- [31] M. Krenn, J. Handsteiner, M. Fink, R. Fickler, and A. Zeilinger, *Proc. Natl. Acad. Sci. USA* **112**, 14197 (2015).
- [32] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, *Optica* **4**, 1006 (2017).
- [33] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, *arXiv:1801.10299*.
- [34] M. Born, E. Wolf, A. B. Bhatia, and P. C. Clemmow, *Principles of Optics: Electromagnetic Theory of Propagation, Interference and Diffraction of Light* (Pergamon Press, Oxford, 1970), Vol. 4.
- [35] E. Bolduc, N. Bent, E. Santamato, E. Karimi, and R. W. Boyd, *Opt. Lett.* **38**, 3546 (2013).
- [36] E. Karimi, D. Giovannini, E. Bolduc, N. Bent, F. M. Miatto, M. J. Padgett, and R. W. Boyd, *Phys. Rev. A* **89**, 013829 (2014).
- [37] E. Karimi, R. W. Boyd, P. de la Hoz, H. de Guise, J. Řeháček, Z. Hradil, A. Aiello, G. Leuchs, and L. L. Sánchez-Soto, *Phys. Rev. A* **89**, 063813 (2014).
- [38] L. Marrucci, C. Manzo, and D. Paparo, *Phys. Rev. Lett.* **96**, 163905 (2006).
- [39] M. Mirhosseini, O. S. Magaña-Loaiza, C. Chen, B. Rodenburg, M. Malik, and R. W. Boyd, *Opt. Express* **21**, 30196 (2013).
- [40] M. Beijersbergen, R. Coerwinkel, M. Kristensen, and J. Woerdman, *Opt. Commun.* **112**, 321 (1994).
- [41] N. Yu, P. Genevet, M. A. Kats, F. Aieta, J.-P. Tetienne, F. Capasso, and Z. Gaburro, *Science* **334**, 333 (2011).
- [42] E. Karimi, S. A. Schulz, I. D. Leon, H. Qassim, J. Upham, and R. W. Boyd, *Light: Sci. Appl.* **3**, e167 (2014).
- [43] F. Bouchard, I. D. Leon, S. A. Schulz, J. Upham, E. Karimi, and R. W. Boyd, *Appl. Phys. Lett.* **105**, 101905 (2014).
- [44] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, *Int. J. Quantum Inf.* **8**, 535 (2010).
- [45] B.-G. Englert, D. Kaszlikowski, H. K. Ng, W. K. Chua, J. Řeháček, and J. Anders, *arXiv:quant-ph/0412075*.
- [46] F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, and E. Karimi, *arXiv:1802.05773*.

Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons

Frédéric Bouchard¹, Khabat Heshami², Duncan England², Robert Fickler¹, Robert W. Boyd^{1 3 4}, Berthold-Georg Englert^{5 6 7}, Luis L. Sánchez-Soto^{3 8}, and Ebrahim Karimi^{1 3 9}

¹Department of physics, University of Ottawa, Advanced Research Complex, 25 Templeton, Ottawa ON Canada, K1N 6N5

²National Research Council of Canada, 100 Sussex Drive, Ottawa ON Canada, K1A 0R6

³Max-Planck-Institut für die Physik des Lichts, Staudtstraße 2, 91058 Erlangen, Germany

⁴Institute of Optics, University of Rochester, Rochester, NY 14627, USA

⁵Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore

⁶Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542, Singapore.

⁷MajuLab, CNRS-UNS-NUS-NTU International Joint Unit, UMI 3654, Singapore.

⁸Departamento de Óptica, Facultad de Física, Universidad Complutense, 28040 Madrid, Spain

⁹Department of Physics, Institute for Advanced Studies in Basic Sciences, 45137-66731 Zanjan, Iran.

November 30, 2018

Quantum key distribution is on the verge of real world applications, where perfectly secure information can be distributed among multiple parties. Several quantum cryptographic protocols have been theoretically proposed and independently realized in different experimental conditions. Here, we develop an experimental platform based on high-dimensional orbital angular momentum states of single photons that enables implementation of multiple quantum key distribution protocols with a single experimental apparatus. Our versatile approach allows us to experimentally survey different classes of quantum key distribution techniques, such as the 1984 Bennett & Brassard (BB84), tomographic protocols including the six-state and the Singapore protocol, and to investigate, for the first time, a recently introduced differential phase shift (Chau15) protocol using twisted photons. This enables us to experimentally compare the performance of these techniques and discuss their benefits and deficiencies in terms of noise tolerance in different dimensions.

1 Introduction

Quantum cryptography allows for the broadcasting of information between multiple parties in a perfectly secure manner under the sole assumption that the laws of quantum physics are valid [1]. Quantum Key Distribution (QKD) [2, 3] is arguably the most well-known and studied quantum cryptographic protocol to date. Other examples are quantum money [4] and quantum secret sharing [5]. In QKD schemes, two parties, conventionally referred to as *Alice* and *Bob*, exchange carriers of quantum information, typically photons, in an untrusted quantum channel. An adversary, known as *Eve*, is granted full access to the quantum channel in order to eavesdrop on Alice and Bob's shared information. It is also assumed that Eve is only limited by the laws of physics and has access to all potential future technologies to her advantage, including optimal cloning machines [6], quantum memories [7], quantum non-demolition measurement apparatus [8], and full control over the shared photons. In particular, the presence of Eve is revealed to Alice and Bob in the form of noises in the channel. It is the goal of QKD to design protocols for which secure information may be transmitted even in the presence of noises [9]. For quantum channels with high levels of noises, it has been rec-

ognized that high-dimensional states of photons constitute a promising avenue for QKD schemes, due to their potential increase in noise tolerance with larger encrypting alphabet [10, 11]. However, this improvement comes at the cost of generating and detecting complex high-dimensional superpositions of states, which may be a difficult task.

Orbital angular momentum (OAM) states are associated with helical phase fronts for which a quantized angular momentum value of $\ell\hbar$ along the photons propagation direction can be ascribed, where ℓ is an integer and $\hbar$ is the reduced Planck constant [12]. Any arbitrary superposition of OAM states can be straightforwardly realized by imprinting the appropriate transverse phase and intensity profile on an optical beam, which is typically done by displaying a hologram onto a spatial light modulator (SLM) [13, 14, 15]. OAM-carrying photons, also known as twisted photons, have been recognized to constitute useful carriers of high-dimensional quantum states for quantum cryptography [16, 17, 18], quantum communication [19, 20, 21, 22] and quantum information processing [23, 24, 25, 26, 27]. The flexibility in preparation and measurement of twisted-photon states enables us to create and use a single experimental setup for implementing several QKD protocols that offer different advantages, such as efficiency in secure bit rate per photon or noise tolerance for operation over noisy quantum channels. Here, we use OAM states of photons to perform and compare high-dimensional QKD protocols such as the 2-, 4- and 8-dimensional BB84 [2], tomographic protocols [28, 29, 30] using mutually unbiased bases (MUB) [31] and Symmetric Informationally Complete (SIC) Positive Operator-Valued Measures (POVMs) [32], and, for the first time, the 4- and 8-dimensional *Chau15* protocols using twisted photons. We finally demonstrate applications in full characterization of the quantum channel through quantum process tomography [33].

2 Theoretical background

Let us first start by briefly reviewing the BB84 protocol, which was introduced in 1984 by Bennett and Brassard [2]. In this protocol, Alice uses qubits to share a bit of information (0 or 1) with Bob, while using two different MUB [31]. This

QKD protocol relies on the *uncertainty principle*, since a measurement by Eve in the wrong basis will not yield any useful information for herself. However, this also means that half of the time, Alice and Bob will perform their generation/detection in the wrong basis. This is known as sifting: Alice and Bob will publicly declare their choices of bases for every photon sent and only when their bases match will they keep their shared key. On average, Alice and Bob will only use half of their bits in their shared *sifted key*. Nevertheless, in the infinite key limit, the sifting efficiency of several protocols, such as the BB84 and the six-state protocol, can approach 1, by making the basis choice extremely asymmetric [34]. In addition to sifting, Alice and Bob's shared key will be further reduced in size at the final stage of the protocol when performing error correction (EC) and privacy amplification (PA) [9]. In the case of BB84 in dimension 2, the number of bits of secret key established per sifted photon, defined here as the secret key rate R , is given by the following expression,

$$R = 1 - 2h(e_b), \quad (1)$$

where e_b is the quantum bit error rate (QBER) and $h(x) := -x \log_2(x) - (1-x) \log_2(1-x)$ is the Shannon entropy. From this equation, we find that the secret key rate becomes negative for $e_b > 0.11$. Hence, if Alice and Bob only have access to a quantum channel with a QBER larger than 0.11 to perform the BB84 protocol, they will not be able to establish a secure key regardless of sifting and losses. Due to this limitation, it has been the goal of many research efforts to come up with QKD protocols that are more error tolerant. One of the first proposed QKD protocols that was aimed at extending the 0.11-QBER threshold, is the so-called *six-state* protocol [28]. The six-state protocol is an extension of the BB84 in dimension 2, where all three MUB are used. Indeed, it is known that in dimension 2, there exists precisely 3 MUB. In the general case of a d -dimensional state space, the number of MUB is $(d+1)$, given that d is a power of a prime number [31]. Moreover, it is known that there exist at least three MUB for any dimension [31] such that these 3 MUB can be used to increase error thresholds in dimensions which are not a power of a prime number [35, 36]. Of course, this has the drawback of decreasing the efficiency of ob-

taining sifted data from $1/2$ to $1/3$. Nevertheless, by simply adding another basis to the encoding measurement scheme, the QBER threshold now increases to 0.126, as can be deduced from the secret key rate of the six-state protocol [28]

$$R = 1 - h\left(\frac{3}{2}e_b\right) - \frac{3}{2}e_b \log_2(3). \quad (2)$$

Another avenue to increase error tolerability in QKD is to use high-dimensional quantum states, also known as *qudits* [37]. This may be intuitively understood from the fact that the presence of an optimal cloning attack leads to larger signal disturbance in higher-dimensional QKD schemes [11, 38]. The BB84 protocol may be extended here by using qudits. The adoption of high-dimensional quantum systems has two distinct benefits: (i) an increase of the error-free key rate per sifted photons to a value of $R = \log_2(d)$; (ii) an increase in the maximum tolerable QBER, i.e. the error threshold for $R = 0$. For the simple case of a d -dimensional BB84 protocol, the secret key rate is given by [39],

$$R = \log_2(d) - 2h^{(d)}(e_b), \quad (3)$$

where $h^{(d)}(x) := -x \log_2(x/(d-1)) - (1-x) \log_2(1-x)$ is the d -dimensional Shannon entropy. Furthermore, it is also possible to extend the *six-state* protocol to higher dimensions by employing all $(d+1)$ MUB, assuming that d is a power of a prime number, where the secret key rate is given by,

$$R = \log_2(d) - h^{(d)}\left(\frac{d+1}{d}e_b\right) - \frac{d+1}{d}e_b \log_2(d+1). \quad (4)$$

This type of QKD scheme is also known as tomographic QKD [29, 30], where all measurements, including the sifted ones, are used to perform quantum state tomography (QST). In particular, MUB are closely related to the problem of quantum state tomography, where projections over all the states of every MUB, although redundant, yields a full reconstruction of the state's density matrix [40]. Following similar ideas, the *Singapore* protocol has been proposed using SIC-POVMs [30], as they are known to be the most efficient measurements to perform QST. The Singapore protocol may be equivalently performed in a prepare-and-measure or an entanglement-based scheme, similar to the analogy between BB84

and Ekert [41], respectively. Moreover, this QKD protocol may also be extended to higher dimensions [42] with the major advantage that the SIC-POVMs are believed to exist for all dimensions, including those that are not powers of prime numbers, contrary to MUB.

Another class of QKD protocols using qudits has recently been introduced, in which qudits are used to encode a single bit of information. Although, such protocols primarily benefits from one of the advantages mentioned earlier, i.e. an increase in the QBER threshold, they have proven to be interesting and advantageous due to a simplified generation and measurement of the states. Their main drawback is the fact that at a null QBER, the key rate per sifted photons is never larger than $R = 1$. An example of such a protocol is the *Differential Phase Shift* (DPS) QKD protocol [43]. The information is encoded by Alice in the relative phase of a superposition of all states then sent over the quantum channel. Bob may then measure the relative phase by detection of the different phases using an interferometric apparatus. In particular, the advantage of the 3-dimensional DPS scheme is in the higher sifting efficiency in comparison to BB84 in the finite key limit. An extension of the DPS protocol is the *Round-Robin Differential Phase Shift* (RRDPS) protocol [44] where Bob's interferometric apparatus is slightly modified. This modification results in a bound on Eve's leaked information removing the need to monitor signal disturbance (QBER) for performing privacy amplification. Nevertheless, the qudits employed in the RRDPS QKD protocol consist of a superposition of d states, which may pose some practical limitations in experimental implementations as d becomes larger. However, the RRDPS scheme has recently been demonstrated experimentally using twisted photons [45]. The recently introduced *Chau15* protocol [46, 47] addresses this problem as it uses "qubit-like" superpositions where only two states of the d -dimensional space are employed. More specifically, the information is encoded in the relative phase of a qubit-like state of the form $|\phi_{ij}^\pm\rangle = (|i\rangle \pm |j\rangle)/\sqrt{2}$ with states in a 2^n -dimensional Hilbert space with $n \geq 2$. This protocol will be explained in more details in the discussion section.

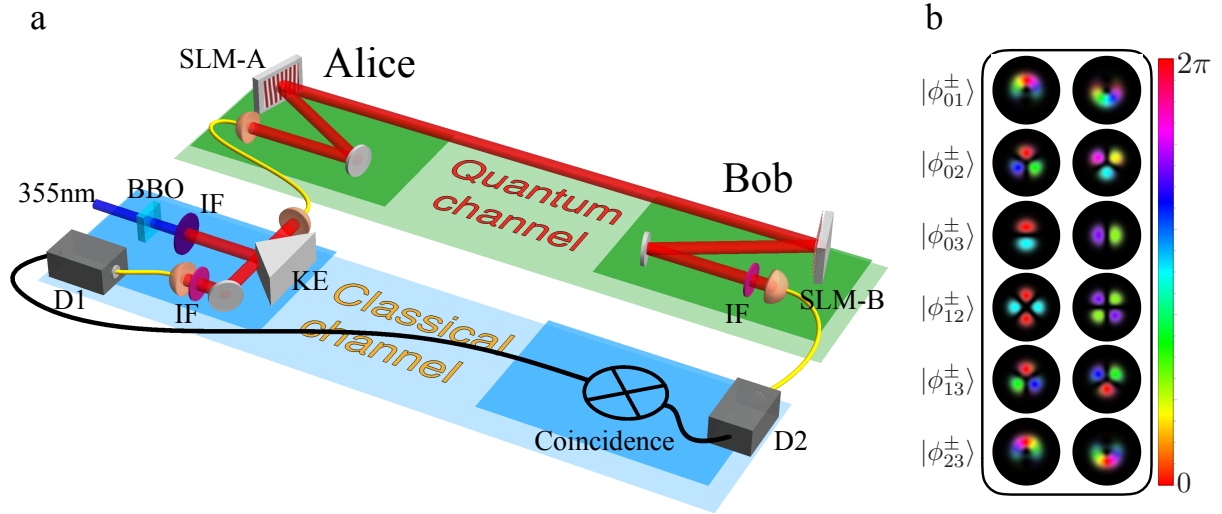


Figure 1: (a) Simplified experimental setup. Alice generates pairs of single photons using spontaneous parametric downconversion in a type-I β -barium borate (BBO) crystal. The pump wavelength (355 nm) is filtered using an interference filter (IF) and the photons are separated using a knife edge (KE) in the far-field of the crystal. The spatial modes of the photon pairs are filtered using single mode optical fibres making the photons completely separable. Alice imprints a state onto her signal photon using a holographic technique by means of a spatial light modulator (SLM-A). The photon is then sent to Bob through the quantum channel. Bob measures the photon's state using a phase flattening technique with his SLM-B followed by a single mode optical fibre. Moreover, Alice locally measures the idler photon and sends timing information to Bob via an electric signal over the classical channel. Our experimental configuration allows us to test different protocols by changing the holograms displayed on the SLMs using the same experimental apparatus without intermediate adjustments. Thus, we are able to compare the different strategies in a systematic manner. (b) States employed in the Chau15 ($N = 4$) protocol. The phase (Hue colour) is shown modulated by the intensity profile of the beam.

3 Experimental setup

We implement a prepare-and-measure QKD scheme at the single-photon level using the OAM degree of freedom of photons, see Fig. 1 (a). The single photon pairs, namely *signal* and *idler*, are generated by spontaneous parametric downconversion (SPDC) at a type I β -barium borate (BBO) crystal. The nonlinear crystal is pumped by a quasi-continuous wave ultraviolet laser operating at a wavelength of 355 nm. The generated photon pairs are coupled to single-mode optical fibres (SMF) in order to filter their spatial modes to the fundamental mode; i.e., Gaussian. Following the SMF, a coincidence rate of 30 kHz is measured within a coincidence time window of 2 ns. The heralded signal photon is sent onto SLM-A corresponding to Alice's generation stage. The SLM (X10468-07, Hamamatsu) are electronically controlled nematic liquid crystal devices with 792×600 pixels, a refresh rate of 60 Hz and a diffraction efficiency in excess

of 70 %. The OAM states are produced using a phase-only holography technique [14]. Due to the versatility of SLMs, any OAM superposition states of single photons may be produced, hence covering a large possibility of QKD schemes. Alice's heralded photon is subsequently sent over the untrusted quantum channel. Upon reception of the photon, Bob uses his SLM-B followed by a SMF to perform a projection over the appropriate states for a given protocol. In order to do so, Bob uses the phase-flattening technique to measure OAM states of light [48, 49]. If the incoming photon carried the OAM mode corresponding to Bob's projection, the phase of the mode is flattened and the photon will couple to the SMF. This verification-type measurements can further reduce the sifting rate, unless the protocols requires only a binary measurement and "no-click" events are included. Coincidences are recorded using single photon detectors (ID120-500-800nm, ID Quantique) with a dark count rate of less than 50 Hz and a measured deadtime of approximately

400 ns. For an integration time of 10 s and a coincidence time window of 2 ns, approximately 14,000 coincidences are recorded when both SLM-A and SLM-B are set to the same mode. This corresponds to a transmission of approximately 5 %. Finally, in order to evaluate the single photon nature of the SPDC source, we build a Hanbury-Brown and Twiss interferometer in order to measure the degree of second-order coherence $g^{(2)}(0)$ for our single photon source in a three-detector measurement configuration. The signal photon is sent to a beam splitter and subsequently measured at both output ports of the beam splitter, i.e. detectors A and B , while the idler photon is measured directly at detector C . The experimentally determined second-order coherence is given by $g^{(2)}(0) = (N_{ABC}N_C)/(N_{AC}N_{BC})$, where N_{ABC} is the three-fold coincidence rate among detectors A , B and C , N_C is the single count rate at detector C , N_{AC} is the coincidence rate between detector A and C and N_{BC} is the coincidence rate between B and C . We obtained an experimental value of $g^{(2)}(0) = 0.015 \pm 0.004$, where the experimental uncertainty is calculated assuming Poissonian statistics. For the case of BB84, the knowledge of the $g^{(2)}(0)$ and the efficiency of the source is sufficient to characterize the effect of multiphoton events on the secret key rate [50]. Following the analysis of [51], the secret key rate given in Eq. 1 becomes:

$$R = (1 - \Delta) \left(1 - h\left(\frac{e_b}{1 - \Delta}\right) \right) - h(e_b), \quad (5)$$

where $\Delta = P_m/Q$ is the multiphoton rate, $P_m = 1 - P_0 - P_1$ is the probability of having more than one photon in a pulse, $Q = \sum_{n=0}^{\infty} Y_n P_n$ is the gain, Y_n is the yield of an n -photon signal and P_n is the probability of having n photons in a pulse. The probability of creating a multiphoton state, P_m , is upper bounded by $g^{(2)}(0)$, i.e. $P_m \leq \mu^2 g^{(2)}(0)/2$, where μ is the mean photon number in a pulse. From the experimental parameters mentioned above, we obtain a gain, a mean photon number, and a multiphoton rate of $Q = 10^{-5}$, $\mu = 3 \times 10^{-4}$, and $\Delta = 4 \times 10^{-5}$, respectively, which will have a negligible effect on the secret key rate. For instance, in the case of BB84 in dimension 2, the secret key rate considering multiphoton events is reduced by an amount on the order of 10^{-5} bits per sifted photon.

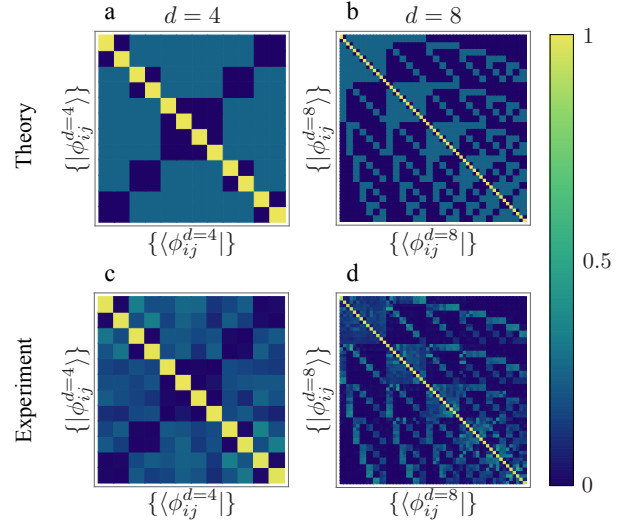


Figure 2: Results for the Chau15 protocol. (a)-(b) Theoretical probability-of-detection matrices for the Chau15 protocol in dimension $d = 4$ and $d = 8$, respectively. Rows are given by states $|\phi_{ij}^{\pm}\rangle \in \{|\phi_{1,2}^+\rangle, |\phi_{1,2}^-\rangle, |\phi_{1,3}^+\rangle, \dots, |\phi_{3,4}^-\rangle\}$ sent by Alice, whereas columns corresponds to state projections, $\langle\phi_{ij}^{\pm}|$, by Bob. (c)-(d) Experimentally measured probability-of-detection matrices for the Chau15 protocol in dimension $d = 4$ and $d = 8$. The sifted data corresponds to the on-diagonal 2×2 blocks. The remaining of the probability-of-detection matrix may be used to evaluate the dit error rate.

4 Results and Discussion

4.1 Chau15 protocol

At first, we perform the recently introduced Chau15 protocol, which is a qudit-based prepare-and-measure QKD scheme, where information is encoded in a qubit-like state of the form $|\phi_{ij}^{\pm}\rangle = (|i\rangle \pm |j\rangle)/\sqrt{2}$ with states in a 2^n -dimensional Hilbert space with $n \geq 2$; see [46, 47, 52]. The protocol starts with Alice randomly selecting i , j , and s , where $\{i, j\} \in \text{GF}(d = 2^n)$, $\text{GF}(d)$ being the Galois field, and $s = \pm 1$. Then, Alice prepares and sends the state $(|i\rangle + (-1)^s |j\rangle)/\sqrt{2}$ over an untrusted channel to Bob. Upon reception, Bob randomly selects i' , $j' \neq i' \in \text{GF}(d)$ and measures the state along $(|i'\rangle \pm |j'\rangle)/\sqrt{2}$. By announcing (i, j) and (i', j') through a classical channel, Alice and Bob can establish a raw bit sequence (key) from those events where $(i, j) = (i', j')$ and by keeping a record of s .

As discussed in [47], the performance of the scheme can be assessed through two sets of pa-

rameters. The first is the bit error rate of the sifted raw key (e_{raw}). The second is the average bit error rate and the average dit error rate associated with mismatch between preparation and measurement basis states. The average bit and dit error rates are estimated by averaging probabilities of the qudit states undergoing operations of $X_u Z_v$ in the insecure quantum channel, where $X_u|i\rangle = |i+u\rangle$, $Z_v|i\rangle = (-1)^{\text{Tr}(vi)}|i\rangle$, and $\text{Tr}(i) = i + i^2 + i^4 + \dots + i^{d/2}$; see [47] for more details. These parameters can be extracted from the experimental joint probability measurements. Alice and Bob respectively prepare and measure $|\phi_{ij}^\pm\rangle = (|i\rangle \pm |j\rangle)/\sqrt{2}$, where $|i\rangle$ and $|j\rangle$ ($i \neq j$) are pure OAM states in a Hilbert space of dimension $d = 4, 8$, see Fig. 1 (b). Using the OAM, Alice and Bob choose $i, j \in \{\ell = -2, -1, 1, 2\}$ for $d = 4$ and $i, j \in \{\ell = -4, -3, -2, -1, 1, 2, 3, 4\}$ for $d = 8$, where the $\ell = 0$ state has been omitted to make the states symmetric. In Fig. 2, we show theoretical and experimental probability-of-detection matrices obtained from a Chau15 QKD protocol for the cases of $d = 4$ and $d = 8$. After sifting, Alice and Bob are left with the on-diagonal 2×2 blocks of the presented probability-of-detection matrices.

In the case of $d = 4$, we obtained an average bit error rate of $e_b^{(d=4)} = 0.778\%$, and average dit error rate $e_d^{(d=4)} = 3.79\%$. This results in an asymptotic secure key rate of $R^{(d=4)} = 0.8170$ bit per sifted photon. For the case of $d = 8$, we obtained experimental values for the average bit error rate, average dit error rate and asymptotic secure key rate of $e_b^{(d=8)} = 3.11\%$, $e_d^{(d=8)} = 0.82\%$ and $R^{(d=8)} = 0.8172$, respectively. Note that the probability of obtaining sifted data in the Chau15 protocol is given by $2/(d^2 - d)$ compared to the fixed sifting rate of $1/2$ for the BB84 protocols in all dimensions. As we will see in the following sections, the Chau15 protocol does not perform well in the low-error case compared with other QKD protocols. Moreover, the unfavourable scaling of the sifting with dimensionality greatly affects the overall secure key rate (sifting included) in the finite key limit. Hence, the advantage of the Chau15 scheme is in the high-error scenario. In particular, given a small enough dit error rate, bit error rates of up to $e_b^{\text{max}} = 50\%$ may be tolerated. In the case of OAM states of light, this does not represent a clear advantage since bit and dit error rates will, in general, be the result of sim-

ilar error sources, e.g. misalignment, turbulence or optical aberration. However, for other kinds of high-dimensional states of light, such as time-bins, the distinction between bit and dit error rates is less ambiguous and the Chau15 may then be used to its full potential.

4.2 BB84 protocol

We now go on to compare the new Chau15 scheme to established protocols. The same experimental setup is used at first to perform the BB84 (2 MUB) protocol in dimension $d = 2, 4$ and 8 . In the BB84 protocols, the first basis is given by the logical pure OAM basis, i.e. $|\psi_i\rangle \in \{-d/2, \dots, d/2\}$ and the second basis is given by the Fourier basis where the states are obtained from the discrete Fourier transform, $|\phi_i\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega_d^{ij} |\psi_j\rangle$, with $\omega_d = \exp(i2\pi/d)$. The explicit form of the other MUB may be found elsewhere [31]. Although this works only for prime dimensions, it can be easily extended to composite dimensions. For the BB84 protocol, values of the QBER of $e_b^{d=2} = 0.628\%$, $e_b^{d=4} = 3.51\%$ and $e_b^{d=8} = 10.9\%$ were obtained in dimension 2, 4 and 8, respectively corresponding to secure key rates of $R^{d=2} = 0.8901$, $R^{d=4} = 1.4500$ and $R^{d=8} = 1.3942$. In the low-error case, the BB84 scheme performs very well. This is partly due to the fact that the sifting, i.e. $1/2$, is independent of dimensionality in the finite key limit. Interestingly, the BB84 protocol performs better in dimension 4 than it does in dimension 8. Hence, although in the error-free case, larger dimensions result in larger secure key rates, this is not necessarily the case in experimental implementations, due to more complex generations and detections of the high-dimensional OAM states. The nature of the quantum channel may also dictate the optimal dimensionality of the protocol [53].

4.3 Tomographic protocols

4.3.1 MUB-based protocol

The six-state protocol in dimension $d = 2$ is an extension of the BB84 protocol where all existing MUB are considered. The protocol can be extended to higher dimensions (powers of prime numbers) where all $(d+1)$ MUB are considered. In dimension 2 and 4, we obtained a QBER of $e_b^{d=2, m=3} = 0.923\%$ and $e_b^{d=4, m=5} = 3.87\%$

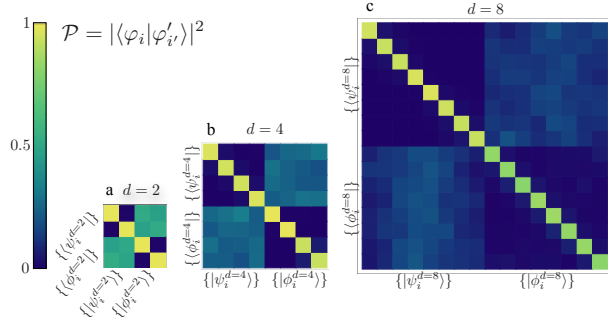


Figure 3: BB84 protocol. (a)-(c) Experimentally measured probability-of-detection matrices for the BB84 protocol in dimension $d = 2, 4$ and 8 , respectively. The rows and columns of the matrices correspond to the states sent and measured by Alice and Bob, respectively. The sifted data corresponds to the on-diagonal $d \times d$ blocks.

for the 3-MUB and the 5-MUB protocols, see Fig. 4 (a) and (c), corresponding to key rates of $R^{d=2,m=3} = 0.8727$ and $R^{d=4,m=5} = 1.5316$ bits per sifted photon. In comparison to the BB84 protocol, the $(d+1)$ -MUB protocol has a sifting efficiency of $1/(d+1)$, which scales poorly with dimensions. Nevertheless, in the infinite key limit, the $(d+1)$ -MUB approach could exceed the performance of the BB84 protocol by considering an efficient asymmetric basis choice. Furthermore, this scheme only applies to dimensions that are powers of prime numbers. However, the $(d+1)$ -MUB approach consists of a tomographic protocol and in the case of large errors, it will outperform the BB84 scheme. In practical implementations, one could consider an intermediate scenario where the number of MUB considered is between 2 and $(d+1)$ in order to optimize the secure key rate.

4.3.2 Singapore protocol

Finally, we perform another tomographic QKD protocol based on SIC-POVMs, known as the Singapore protocol. In particular, we use the Weyl-Heisenberg covariant SIC-POVMs elements. Reference vectors $|f\rangle$ have been conjectured to exist in arbitrary dimensions [32, 54] such that SIC-POVMs can be obtained by considering a displacement operator $\hat{D}_{jk}$ acting on the reference vector $|f\rangle$, where

$$\hat{D}_{jk} = \omega_d^{jk/2} \sum_{m=0}^{d-1} \omega_d^{jm} |k+m\rangle \langle m|, \quad (6)$$

and $\omega_d = e^{2\pi i/d}$. The fiducial vectors $|f\rangle$ have been derived numerically and analytically for different dimensions [32]. The fiducial vector is found such that $|\psi_{jk}\rangle = \{\hat{D}_{jk}|f\rangle, j, k = 0 \dots d-1\}$ are normalized states satisfying $|\langle \psi_{jk} | \psi_{j'k'} \rangle|^2 = 1/(d+1)$ for $j \neq j'$ and $k \neq k'$. This set of d^2 states are then used by Alice and Bob in the prepare-and-measure Singapore protocol. In dimension 2, the SIC POVMs are explicitly given by

$$\begin{aligned} |\psi_{0,0}\rangle &= (0.888|0\rangle + 0.325(1-i)|1\rangle), \\ |\psi_{0,1}\rangle &= (0.325(1-i)|0\rangle + 0.888|1\rangle), \\ |\psi_{1,0}\rangle &= (0.888|0\rangle - 0.325(1-i)|1\rangle), \\ |\psi_{1,1}\rangle &= (0.325(1+i)|0\rangle - 0.888i|1\rangle). \end{aligned}$$

Using the same experimental apparatus, we perform the Singapore protocol in dimension $d = 2$, where a QBER of $e_b = 1.23\%$ was measured, see Fig. 4 (a).

Inspired by the Singapore protocol [30] an iterative key extraction method can be applied to extract a sifted secret key surpassing the $1/3$ limit of the six-state protocol. The asymptotic efficiency of the iterative approach have been shown to reach 0.4 which is slightly smaller than the theoretical maximum of 0.415 under ideal conditions [30]. Here, we use the experimental joint probability matrix to find the experimental mutual information as an upper bound for the key extraction rate. For this purpose, we parametrize $|\psi_m^{A,B}(x)\rangle$ vectors (as Alice's and Bob's experimental preparation and measurement states). We then numerically minimize a maximum likelihood relation of the form $f(x) = \sum_{m,n=1}^{d^2} \left| |\langle \psi_m^A(x) | \psi_n^B(x) \rangle|^2 - |\langle \psi_m | \psi_n \rangle|^2 \right|^2$ to find deviations (errors) in the experimental SIC states of Alice and Bob. These deviations can also be interpreted as errors in the quantum channel.

The Singapore protocol relies on an anti-correlation between Alice and Bob. In the entanglement-based version of this protocol, this can be achieved by sharing a singlet entangled state. Assuming a singlet state of $|\Psi^{(-)}\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} (-1)^{d-m} |m\rangle |d-m-1\rangle$, we can extract the joint anti-correlated prepare-and-measure probabilities. In dimension $d = 2$, this takes the form of $p_{kl} = \text{Tr}[\hat{\rho}_{AB}(1 + \vec{t}_k \cdot \vec{\sigma}_A)(1 + \vec{t}_l \cdot \vec{\sigma}_B)]$, where $\vec{t}_k$ s are unit vectors denoting SIC states and $\hat{\sigma}_i$ s are Pauli matrices. This typically deviates from

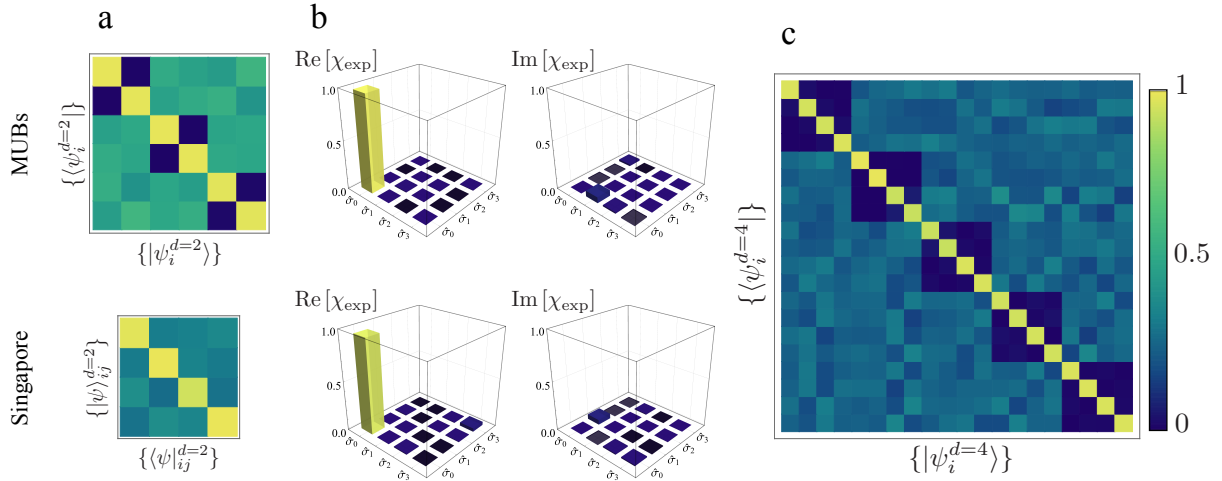


Figure 4: Results for the $(d+1)$ -MUB and Singapore protocols. (a) Experimentally measured probability-of-detection matrices for the $(d+1)$ -MUB and Singapore protocols in dimension $d = 2$. The rows and columns of the matrices correspond to the states sent and measured by Alice and Bob, respectively. For the case $(d+1)$ -MUB protocols, the sifted data corresponds to the on-diagonal $d \times d$ blocks. (b) Reconstructed process matrix for the six-state (upper) and the Singapore (lower) protocols. (c) Experimentally measured probability-of-detection matrices for the $(d+1)$ -MUB protocol in dimension $d = 4$.

the ideal case with prepare-and-measure probabilities of $p_{kl} = (1 - \delta_{kl})/12$. Keep in mind that the Singapore protocol relies on completely symmetric prepare-and-measure probabilities. This symmetrization can be achieved by twirling the calculated probability matrix leading to

$$p_{kl}^{\text{exp}} = \frac{4 - \epsilon}{48} (1 - \delta_{kl}) + \frac{\epsilon}{16} \delta_{kl}, \quad (7)$$

where $\epsilon = 0.0137$. The mutual information between Alice and Bob is given by

$$I_{AB} = \sum_{k,l=1}^{d^2} p_{kl} \log_2 \left(\frac{p_{kl}}{p_k p_l} \right), \quad (8)$$

where $p_k = \sum_{l=1}^{d^2} p_{kl}$ and $p_l = \sum_{k=1}^{d^2} p_{kl}$. Our approach results in mutual information of $I_{AB}^{d=2} = 0.388$ compared to the theoretical maximum of 0.415; surpassing the maximum attainable rate in the six-state scheme. Moreover, protocols analogous to the Singapore protocol have a poor yield for higher-dimensional systems. The mutual information for qubit, qutrit and ququart pairs are respectively given by 0.415, 0.170 and 0.093 bits.

4.3.3 Quantum process tomography of the QKD channel

In this subsection we considered the two QKD protocols that offer full tomography capabilities [33, 55]. Quantum state preparation and

measurements in all possible MUB states provide an overcomplete set of results that can be used to perform quantum process tomography on the channel. In the Singapore protocol, the SIC POVMs are optimal set of preparation and measurements for process tomography of the channel. Both of these protocols allow one to go beyond a coarse-grained qubit error rate estimation and fully characterize the quantum channel. We use the experimental results for the six-state and Singapore protocols to characterize the quantum channel.

The channel can be characterized as a positive trace-preserving map $\mathcal{E}$ such that $\hat{\rho}_{\text{out}} = \mathcal{E}(\hat{\rho}_{\text{in}})$. This can then be described by the $d^2 \times d^2$ process matrix, χ , where $\mathcal{E}(\hat{\rho}) = \sum_{ij} \chi_{ij} \hat{\sigma}_i \hat{\rho} \hat{\sigma}_j^\dagger$. In $d = 2$, $\hat{\sigma}_i$ are identity and Pauli matrices. This approach can be extended to higher dimensions using Gell-Mann matrices as they also offer an orthogonal basis, $\text{Tr}(\hat{\sigma}_i \hat{\sigma}_j) = 2\delta_{ij}$, spanning the vector space of complex matrices. Moreover, the trace-preserving assumption may be eliminated while using a similar computational approach to reconstruct the process matrix [56]. By doing so, we may take into consideration mode-dependent losses coming from our measurement scheme or the quantum channel itself. Mode-dependent loss is insignificant in our laboratory-scale quantum channel, but may become an issue on longer dis-

Protocol	d	$e_b^{\max}$	e_b^{exp}	$R(0)$	R^{exp}	Sifting	$R^{\text{exp}} \times \text{Sifting}$
Chau15	4	50 %	0.778 %	1	0.8170	1/6	0.1362
	8	50 %	3.11 %	1	0.8172	1/28	0.0292
BB84	2	11.00 %	0.628 %	1	0.8901	1/2 - 1*	0.4451 - 0.8901
	4	18.93 %	3.51 %	2	1.4500	1/2 - 1*	0.7250 - 1.4500
	8	24.70 %	10.9 %	3	1.3942	1/2 - 1*	0.6971 - 1.3942
MUB	2	12.62 %	0.923 %	1	0.8727	1/3 - 1*	0.2909 - 0.8727
	4	23.17 %	3.87 %	2	1.5316	1/5 - 1*	0.3063 - 1.5316
Singapore	2	38.93 %	1.23 %	0.4	0.374**	1	0.374**

Table 1: Quantum bit error rates and key rates are presented for various quantum key distribution protocols. Four protocols, in various dimensions d , were investigated. The theoretical values of the error-free secret key rate, i.e. $R(0)$, and the maximum QBER, i.e. $e_b^{\max}$ for which $R = 0$, are presented for the different protocols alongside the experimentally measured QBER, e_b^{exp} , and secret key rates, R^{exp} . Finally, the sifting rate, defined as the probability of obtaining sifted data, is also shown for each protocols. *Depending on the size of the key, the choice of basis can be biased to get a larger sifting efficiency than 1/2 and 1/(d+1) for BB84 and MUB, respectively [58]. In the infinite key limit, the sifting efficiency can be made to approach 1. **Experimental rate for the Singapore protocol is deduced based on the point that a rate of 0.4 per 0.415 value of mutual information can be achieved.

tance links [22].

Given the experimental preparation and measurement results, we parametrize the process matrix and minimize a maximum likelihood function of

$$f(\vec{t}) = \sum_{a,b} \frac{[N_{ab}/N - \langle \psi_b | (\sum_{i,j} \chi_{ij}(\vec{t}) \hat{\sigma}_i | \psi_a \rangle \langle \psi_a | \hat{\sigma}_j | \psi_b \rangle)]^2}{2 \langle \psi_b | (\sum_{i,j} \chi_{ij}(\vec{t}) \hat{\sigma}_i | \psi_a \rangle \langle \psi_a | \hat{\sigma}_j | \psi_b \rangle)},$$

to find the process matrix. Here N_{ab}/N are normalized prepare-and-measure results, and $|\psi_a\rangle$ ($|\psi_b\rangle$) are prepared states (measurement projection settings). Using numerical minimization, we find the process matrix for both the six-state and Singapore protocols that are depicted in Fig. 4b. The quality of the channel may be described using the process fidelity, which is defined as $F = \text{Tr}[\chi_{\text{exp}} \tilde{\chi}]$, where χ_{exp} is the experimentally reconstructed process matrix and $\tilde{\chi}$ is the ideal process matrix, i.e. $\tilde{\chi}_{ij} = \delta_{i,0} \delta_{j,0}$, where $\delta_{i,j}$ is the Kronecker delta. The process fidelity obtained from the process tomography using MUB and SIC-POVMs are given by $F_{\text{MUB}} = 98.7\%$ and $F_{\text{SIC-POVM}} = 95.8\%$, respectively. Although SIC-POVMs offer a more efficient tomography of the channel, measurements of modes belonging to OAM MUB are of higher quality, leading to a larger process fidelity. This capability in tomographic protocols can potentially be used to identify attacks, and pre- or post-compensate for non-dynamical errors in the channel [57].

5 Conclusion

Application of quantum physics in public key cryptography first emerged in the seminal work of Bennet and Brassard in 1984; leading to several other protocols that benefit from different properties of quantum states for secure quantum communications. Many experimental efforts have been dedicated to physical implementation of these protocols using mostly polarization and temporal degrees of freedom of photons. Despite significant progress in experimental realization of QKD protocols, each demonstration is practically limited to implement a single protocol in a specific dimension. Structured light, on the other hand, have been shown to offer flexibility in quantum state preparation and measurement in a theoretically unbounded Hilbert space. Here, we employed the versatility offered by the OAM states of photons to perform an experimental laboratory survey of four classes of QKD protocols in different dimensions. Table 1 summarizes the main results of the several QKD schemes. This included the Chau15 scheme (in $d = 4$, and 8) based on differential phases, the BB84 protocol in dimensions 2, 4, and 8, and tomographic protocols based on $(d+1)$ -MUB in $d = 2$ (six-state), and 4, and SIC-POVMs in $d = 2$. We observed experimental secure bit rates that ranges from 0.03 to 0.72 bit per sifted photon with schemes that have error tolerances from 11 % up to 50 %. In particular, for the case of 2-dimensional to-

mographic protocols, for similar noise levels, the Singapore protocol can outperform the six-state protocol after sifting. For higher dimensions, the cross-talk among the different OAM modes limits the performance of several protocols. For example, the 8-dimensional BB84 fails to offer any advantage except for higher error tolerance compared to its 4-dimensional counterpart. However, there is a clear benefit in using the 4-dimensional BB84 rather than the 2-dimensional BB84 protocol, both in terms of key rate and noise tolerance given our experimental configuration. Moreover, in the case of the Chau15 scheme, the sifting rate scales unfavourably with dimensions. Thus, it is likely that under most conditions the 4-dimensional Chau15 scheme will be optimal. Our experimental setup allows one to easily switch between protocols and dimensions to benefit from advantages of different protocols under varying channel conditions. This included using tomographic protocols for a more elaborate characterization of the errors in the quantum channel.

Acknowledgments All authors would like to thank Gerd Leuchs, Markus Grassl and Imran Khan for helpful discussions. F.B. acknowledges the financial support of the Vanier graduate scholarship of the NSERC. R.F. acknowledges the financial support of the Banting postdoctoral fellowship of the NSERC. This work was supported by Canada Research Chairs; Canada Foundation for Innovation (CFI); Canada Excellence Research Chairs, Government of Canada (CERC); Canada First Research Excellence Fund (CFREF); Natural Sciences and Engineering Research Council of Canada (NSERC); Singapore Ministry of Education (partly through the Academic Research Fund Tier 3 MOE2012-T3-1-009) and the National Research Foundation of Singapore; and Spanish Ministerio de Economía y Competitividad (MINECO).

References

- [1] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H., Quantum cryptography, *Rev. Mod. Phys.* **74**, 145 (2002).
- [2] Bennett, C. H. & Brassard, G., Quantum cryptography: Public key distribution and coin tossing, Proceedings of the IEEE international conference on computers, systems, and signal processing, bangalore, india, 1984 (1984).
- [3] Scarani, V. *et al.*, The security of practical quantum key distribution, *Rev. Mod. Phys.* **81**, 1301 (2009).
- [4] Wiesner, S. Conjugate coding, *ACM Sigact News* **15**, 78–88 (1983).
- [5] Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing, *Phys. Rev. A* **59**, 1829 (1999).
- [6] Scarani, V., Iblisdir, S., Gisin, N. & Acin, A. Quantum cloning, *Rev. Mod. Phys.* **77**, 1225 (2005).
- [7] Simon, C. *et al.* Quantum memories, *Eur. Phys. J. D* **58**, 1–22 (2010).
- [8] Werner, M. & Milburn, G. Eavesdropping using quantum-nondemolition measurements, *Phys. Rev. A* **47**, 639 (1993).
- [9] Bennett, C. H., Brassard, G., Crépeau, C. & Maurer, U. M. Generalized privacy amplification, *IEEE T. Inform. Theory* **41**, 1915–1923 (1995).
- [10] Bechmann-Pasquinucci, H. & Tittel, W. Quantum cryptography using larger alphabets, *Phys. Rev. A* **61**, 062308 (2000).
- [11] Cerf, N. J., Bourennane, M., Karlsson, A. & Gisin, N. Security of quantum key distribution using d-level systems, *Phys. Rev. Lett.* **88**, 127902 (2002).
- [12] Allen, L., Beijersbergen, M. W., Spreeuw, R. & Woerdman, J. Orbital angular momentum of light and the transformation of laguerre-gaussian laser modes, *Phys. Rev. A* **45**, 8185 (1992).
- [13] Heckenberg, N., McDuff, R., Smith, C. & White, A. Generation of optical phase singularities by computer-generated holograms, *Opt. Lett.* **17**, 221–223 (1992).
- [14] Bolduc, E., Bent, N., Santamato, E., Karimi, E. & Boyd, R. W. Exact solution to simultaneous intensity and phase encryption with a single phase-only hologram, *Opt. Lett.* **38**, 3546–3549 (2013).
- [15] Forbes, A., Dudley, A. & McLaren, M. Creation and detection of optical modes with spatial light modulators, *Advances in Optics and Photonics* **8**, 200–227 (2016).

- [16] Gröblacher, S., Jennewein, T., Vaziri, A., Weihs, G. & Zeilinger, A. Experimental quantum cryptography with qutrits, *New J. Phys.* **8**, 75 (2006).
- [17] Mafu, M. *et al.* Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases, *Phys. Rev. A* **88**, 032305 (2013).
- [18] Mirhosseini, M. *et al.* High-dimensional quantum cryptography with twisted light, *New J. Phys.* **17**, 033033 (2015).
- [19] D’ambrosio, V. *et al.* Complete experimental toolbox for alignment-free quantum communication, *Nat. Commun.* **3**, 961 (2012).
- [20] Vallone, G. *et al.* Free-space quantum key distribution by rotation-invariant twisted photons, *Phys. Rev. Lett.* **113**, 060503 (2014).
- [21] Krenn, M., Handsteiner, J., Fink, M., Fickler, R. & Zeilinger, A. Twisted photon entanglement through turbulent air across Vienna, *PNAS* **112**, 14197–14201 (2015).
- [22] Sit, A. *et al.* High-dimensional intracity quantum cryptography with structured photons, *Optica* **4**, 1006–1010 (2017).
- [23] Cardano, F. *et al.* Quantum walks and wavepacket dynamics on a lattice with twisted photons, *Science Adv.* **1**, e1500087 (2015).
- [24] Cardano, F. *et al.* Statistical moments of quantum-walk dynamics reveal topological quantum transitions, *Nat. Commun.* **7**, 11439 (2016).
- [25] Cardano, F. *et al.* Detection of zak phases and topological invariants in a chiral quantum walk of twisted photons, *Nature Commun.* **8**, 15516 (2017).
- [26] Babazadeh, A. *et al.* High-dimensional single-photon quantum gates: concepts and experiments, *Phys. Rev. Lett.* **119**, 180510 (2017).
- [27] Erhard, M., Fickler, R., Krenn, M. & Zeilinger, A. Twisted photons: New quantum perspectives in high dimensions, *Light Sci. Appl.* (2018).
- [28] Bruß, D. Optimal eavesdropping in quantum cryptography with six states, *Phys. Rev. Lett.* **81**, 3018 (1998).
- [29] Liang, Y. C., Kaszlikowski, D., Englert, B.-G., Kwek, L. C. & Oh, C. H. Tomographic quantum cryptography, *Phys. Rev. A* **68**, 022324 (2003).
- [30] Englert, B.-G. *et al.* Efficient and robust quantum key distribution with minimal state tomography, *arXiv preprint quant-ph/0412075* (2008).
- [31] Durt, T., Englert, B.-G., Bengtsson, I. & Życzkowski, K. On mutually unbiased bases, *Int. J. Quantum Inf.* **8**, 535–640 (2010).
- [32] Renes, J. M., Blume-Kohout, R., Scott, A. J. & Caves, C. M. Symmetric informationally complete quantum measurements, *J. Math. Phys.* **45**, 2171–2180 (2004).
- [33] Chuang, I. L. & Nielsen, M. A. Prescription for experimental determination of the dynamics of a quantum black box, *J. Mod. Opt.* **44**, 2455–2467 (1997).
- [34] Lo, H.-K., Chau, H. F., & Ardehali, M. Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security, *Journal of Cryptology* **18**, 133–165 (2005).
- [35] Brádler, K., Mirhosseini, M., Fickler, R., Broadbent, A. & Boyd, R. Finite-key security analysis for multilevel quantum key distribution, *New Journal of Physics* **18**, 073030 (2016).
- [36] Ding, Y. *et al.* High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits, *npj Quantum Information* **3**, 25 (2017).
- [37] Genovese, M. & Traina, P. Review on qudits production and their application to quantum communication and studies on local realism, *Advanced Science Letters* **1**, 153–160 (2008).
- [38] Bouchard, F., Fickler, R., Boyd, R. W. & Karimi, E. High-dimensional quantum cloning and applications to quantum hacking, *Science Adv.* **3**, e1601915 (2017).
- [39] Sheridan, L. & Scarani, V. Security proof for quantum key distribution using qudit systems, *Phys. Rev. A* **82**, 030301 (2010).
- [40] D’ambrosio, V. *et al.* Test of mutually unbiased bases for six-dimensional photonic quantum systems, *Sci. Rep.* **3**, 2726 (2013).

- [41] Ekert, A. K. Quantum cryptography based on bell's theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [42] Bent, N. *et al.* Experimental realization of quantum tomography of photonic qudits via symmetric informationally complete positive operator-valued measures, *Phys. Rev. X* **5**, 041006 (2015).
- [43] Inoue, K., Waks, E. & Yamamoto, Y. Differential phase shift quantum key distribution, *Phys. Rev. Lett.* **89**, 037902 (2002).
- [44] Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance, *Nature* **509**, 475 (2014).
- [45] Bouchard F., Sit A., Heshami K., Fickler R. & Karimi E. Round-robin differential phase-shift quantum key distribution with twisted photons, *Phys. Rev. A* **98**, 010301(R) (2018).
- [46] Chau, H. Quantum key distribution using qudits that each encode one bit of raw key, *Phys. Rev. A* **92**, 062324 (2015).
- [47] Chau, H., Wang, Q. & Wong, C. Experimentally feasible quantum-key-distribution scheme using qubit-like qudits and its comparison with existing qubit-and qudit-based protocols, *Phys. Rev. A* **95**, 022311 (2017).
- [48] Mair, A., Vaziri, A., Weihs, G. & Zeilinger, A. Entanglement of the orbital angular momentum states of photons, *Nature* **412**, 313–316 (2001).
- [49] Qassim, H. *et al.* Limitations to the determination of a laguerre–gauss spectrum via projective, phase-flattening measurement, *J. Opt. Soc. Am. B* **31**, A20–A23 (2014).
- [50] Waks, E. *et al.* Security aspects of quantum key distribution with sub-Poisson light, *Phys. Rev. A* **66**, 042315 (2002).
- [51] Schiavon, M. *et al.* Heralded single-photon sources for quantum-key-distribution applications, *Phys. Rev. A* **93**, 012331 (2016).
- [52] Wang, S. *et al.* Proof-of-principle experimental realization of a qubit-like qudit-based quantum key distribution scheme, *Quantum Sci. Technol.* **3**, 025006 (2018).
- [53] Bouchard, F., Sit, A., Hufnagel, F., Abbas, A., Zhang, Y., Heshami, K., Fickler, R., Marquardt, C., Leuchs, G., Boyd, R. W. & Karimi, E. Quantum cryptography with twisted photons through an outdoor underwater channel, *Opt. Express* **26**, 22563–22573 (2018).
- [54] Scott, A. J. & Grassl, M. Symmetric informationally complete positive-operator-valued measures: A new computer study, *J. Math. Phys.* **51**, 042203 (2010).
- [55] Ndagano, B. *et al.* Characterizing quantum channels with non-separable states of classical light, *Nat. Phys.* **13**, 397 (2017).
- [56] Bongioanni, I., Sansoni, L., Sciarrino, F., Vallone, G., & Mataloni, P., Experimental quantum process tomography of non-trace-preserving maps, *Phys. Rev. A* **82**, 042307 (2010).
- [57] Bouchard, F., Hufnagel, F., Koutný, D., Abbas, A., Sit, A., Heshami, K., Fickler, R. & Karimi, E., Full characterization of a high-dimensional quantum communication channel, *arXiv preprint arXiv:1806.08018* (2018).
- [58] Tomamichel, M. *et al.* Tight finite-key analysis for quantum cryptography, *Nat. Commun.* **3**, 634 (2012).

Chapter 6

Conclusions

In conclusion, we have carried out eight independent projects studying high-dimensional quantum cryptography.

In chapter 2, we explored the fundamental implications of encoding larger alphabets onto single photons. In particular, we experimentally demonstrated that high-dimensional quantum cloning results in lower cloning fidelities, thus meaning that in the context of quantum cryptography, an eavesdropper would have a harder time obtaining information from the channel without revealing herself. In a second experiment, we showed that using high-dimensional encoding schemes can greatly simplify experimental implementations for tasks in quantum metrology, showing the wide-reaching applications of quantum information tasks using high-dimensional quantum states.

In chapter 3, we reviewed the different techniques available to experimentalists to measure spatial modes of light. Moreover, we present a novel technique that allows one to characterize with high mode fidelity any arbitrary spatial modes, at the cost of a non-optimal detection efficiency. We then use this technique to experimentally investigate several quantum information tasks such as quantum key distribution and quantum state tomography. Going beyond quantum state tomography, we introduce the formalism of a technique called quantum process tomography, which allows one to fully characterize quantum processes. We then experimentally show that quantum process tomography can be used to drastically improve secret key rates in high-dimensional quantum key distribution.

In chapter 4, we perform out-of-the-laboratory demonstrations of quantum key distribution in realistic conditions. In particular, we established two different types

of quantum cryptographic links, namely an intra-city 300 m long free-space link and an outdoor 3 m underwater link. In both cases, we use high-dimensional encoding schemes based on spatial modes to establish a secure quantum link. In both experiments, a main challenge is the effect of atmospheric and water turbulence, respectively, on spatial modes. In both cases, we operated our link at conditions that were favourable enough to successfully establish the secure links. Nevertheless, in order to extend the distance of free-space and underwater links, active adaptive optics systems will be required.

In addition to the effect of turbulence, channel losses due to absorption and scattering in the atmosphere is another challenge limiting the distance of quantum links. To circumvent this limitation, the development of quantum repeaters and quantum satellites will be necessary. In particular, for the case of quantum repeaters, high-dimensional quantum memories supporting multi-mode states of single photons and high-dimensional Bell state measurement still need to be investigated experimentally to employ them in a high-dimensional quantum communication channel. For quantum satellites, the main challenge of using spatial modes in a high-dimensional quantum channel is the fact that higher-order modes diverge more rapidly for larger dimensions resulting in a lower detection efficiency at the receiving aperture. Nevertheless, higher-dimensional time-bin states encoded in the fundamental Gaussian spatial mode should be compatible with quantum satellites as an avenue to increase information capacity and noise resilience in long-distance quantum communication.

Finally, in chapter 5, we explored novel high-dimensional quantum key distribution protocols and experimentally compared them with established schemes. In particular, we performed proof-of-principle experimental demonstrations of the round-robin differential phase shift protocol and the Chau15 protocol using OAM modes of light, achieving a record dimension of 64 for OAM-based high-dimensional QKD demonstrations. Our experimental platform allows one to change protocol depending on the channel conditions in order to achieve the largest secret key rates.

APPENDICES

Appendix A

Supplementary materials:

High-dimensional quantum cloning
and applications to quantum
hacking

Supplementary Materials for **High-dimensional quantum cloning and applications to quantum hacking**

Frédéric Bouchard, Robert Fickler, Robert W. Boyd, Ebrahim Karimi

Published 3 February 2017, *Sci. Adv.* **3**, e1601915 (2017)

DOI: 10.1126/sciadv.1601915

This PDF file includes:

- Supplementary Text
- fig. S1. Detailed experimental setup.
- fig. S2. Experimental cloning fidelities for every element of each MUB in dimension 7.
- fig. S3. Projective measurements of the input and cloned Gaussian state.

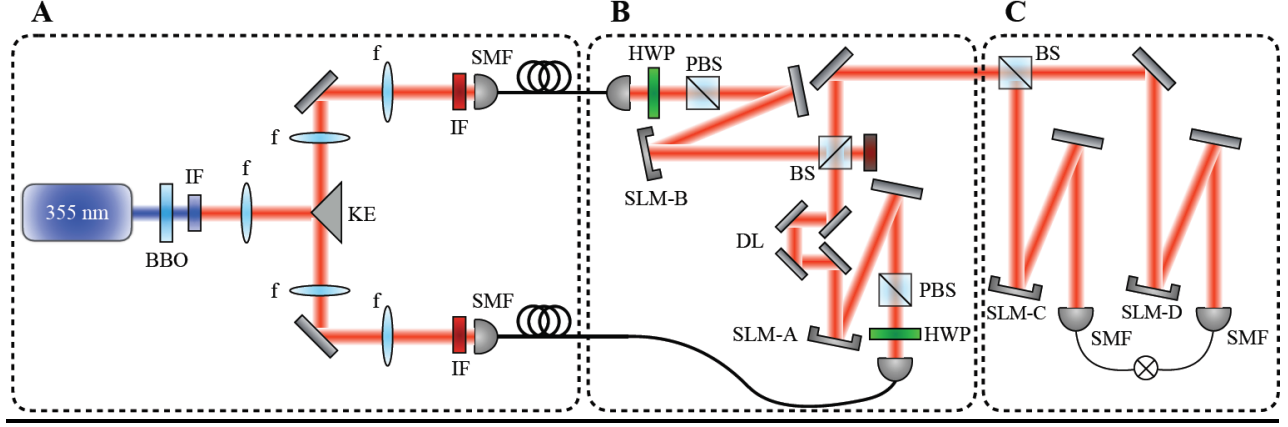


fig. S1. Detailed experimental setup.

Cloning fidelities for various mutually unbiased bases:

In quantum information, mutually unbiased bases (MUBs) are orthogonal bases such that two elements, $|\psi_i\rangle$ and $|\phi_j\rangle$, belonging to different MUBs obeys the following inner product relation

$$|\langle\psi_i|\phi_j\rangle|^2 = \frac{1}{d}$$

An important result in quantum information is the existence of a number of MUBs for a specific dimension. In the particular case of dimensions that are powers of prime numbers, the number of MUBs is given by $d + 1$. Let us now give explicit expressions for each elements of every MUBs, $|\psi_n^{(\alpha)}\rangle$, where $n \in [1, d]$ and $\alpha \in [1, d + 1]$. The first MUB is given by the logical basis, i.e. $|\psi_n^{(1)}\rangle = |n\rangle$. Further, the elements of each MUBs with $\alpha \geq 2$ are given by the following expressions

$$|\psi_n^{(\alpha)}\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^d \exp \left[\frac{2\pi i}{d} \left((n-1)(d-j+1) - (\alpha-2) \left(\sum_{m=j-2}^{d+1} m \right) \right) \right] |i\rangle$$

In order to test the universality of our cloner, we perform cloning fidelity measurements for each element of every MUBs, see fig. S2.

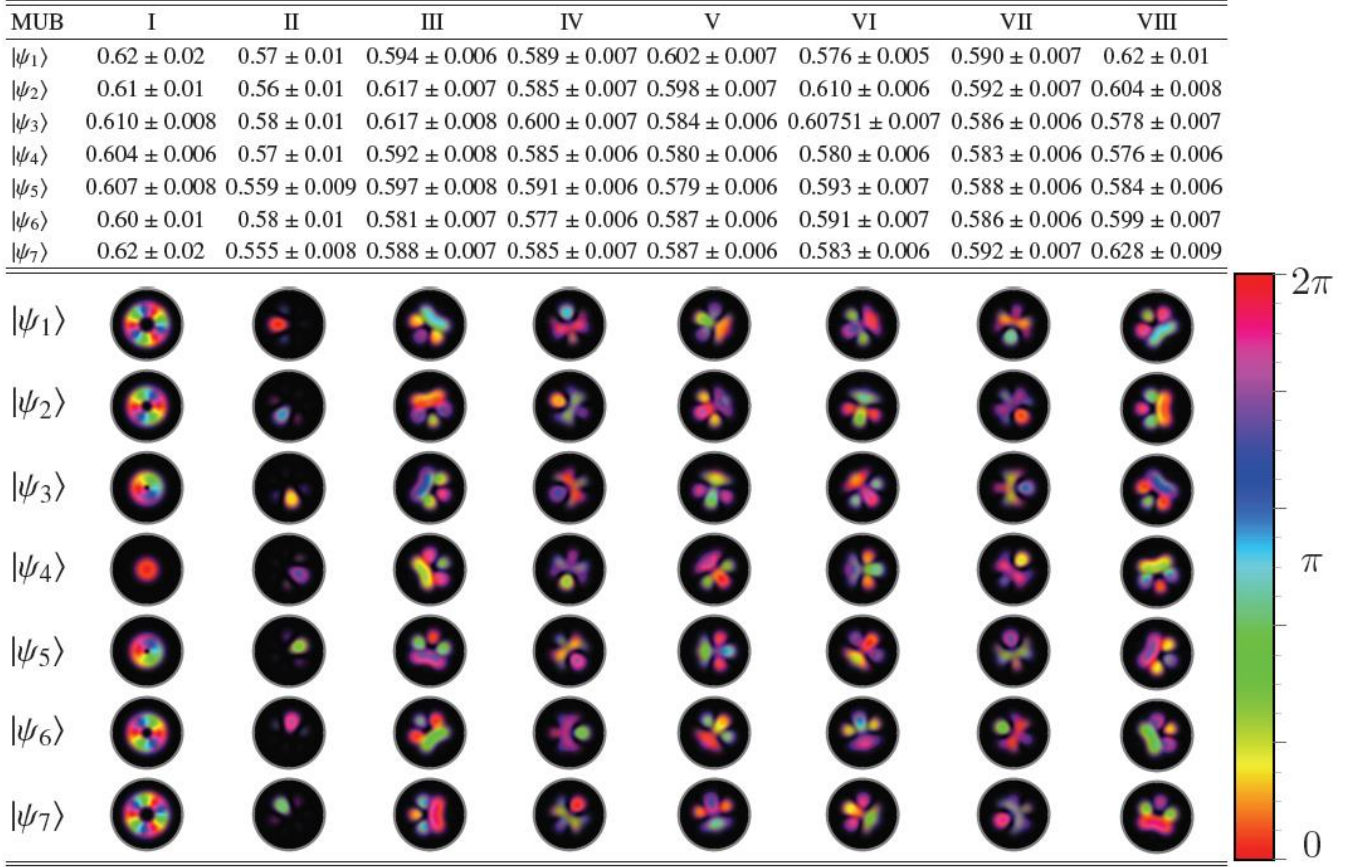


fig. S2. Experimental cloning fidelities for every element of each MUB in dimension 7. The elements $|\psi_i\rangle$ corresponds to the input state that is to be cloned. Experimental data are shown for all $d + 1$ MUBs (I)-(VIII). In the bottom, the transverse profile of each element are shown for every MUBs. The transverse profile is illustrated by plotting the transverse phase modulated by the intensity profile, allowing one to visualize both the phase and intensity pattern at the same time.

High-dimensional quantum state tomography:

In order to reconstruct the density matrix of an arbitrary state, we can perform quantum state tomography. For a given dimension d , where d is a power of a prime number, it is possible to reconstruct the density matrix of a given state by projecting it over each d elements of every $d + 1$ MUBs. In our case, this corresponds to a total of 56 projective measurements. Such projective measurements are expressed as $P_n^{(\alpha)}$, where n labels the states with ($n = 1, \dots, d$) and α labels the MUB with ($\alpha = 1, \dots, d + 1$). These measurements are formally connected to projection operators given by $\Pi_n^{(\alpha)} = |\psi_n^{(\alpha)}\rangle\langle\psi_n^{(\alpha)}|$. Experimentally recorded projective measurements may now be expressed in terms of their associated projection operators, i.e. $P_n^{(\alpha)} = \text{Tr}[\hat{\rho} \Pi_n^{(\alpha)}]$, where $\text{Tr}[\cdot]$ is the trace operator. Finally, the reconstructed density matrix may be expressed in terms of the projective measurements

$$\hat{\rho} = \sum_{\alpha=1}^{d+1} \sum_{n=1}^d P_n^{(\alpha)} \Pi_n^{(\alpha)} - \hat{I}$$

where $\hat{I}$ is the d -dimensional identity matrix. For the case of a *Gaussian* state given earlier by, $|\psi_{\text{Gauss}}\rangle = \mathcal{N} \sum_{\ell=-3}^{\ell=3} \exp[-(\ell/2)^2] |\ell\rangle$, one may perform sequence of projective measurements to tomographically reconstruct its density matrix. Those projective measurements for the input and cloned states are shown in fig. S3. Furthermore, the cloning fidelity of the cloned state can be directly calculated by considering, $\mathcal{F} = \langle \psi_{\text{Gauss}} | \hat{\rho}_{\text{cl}} | \psi_{\text{Gauss}} \rangle$. From the set of measurements presented in fig. S3, one can readily see how a slight misalignment in one MUB can lead to larger misalignment in a different MUB. Moreover, all 56 measurements are in some sense *added* up to reconstruct the density matrix, hence leading to a degraded state fidelity, i.e. 0.80 ± 0.03 for the cloned state.

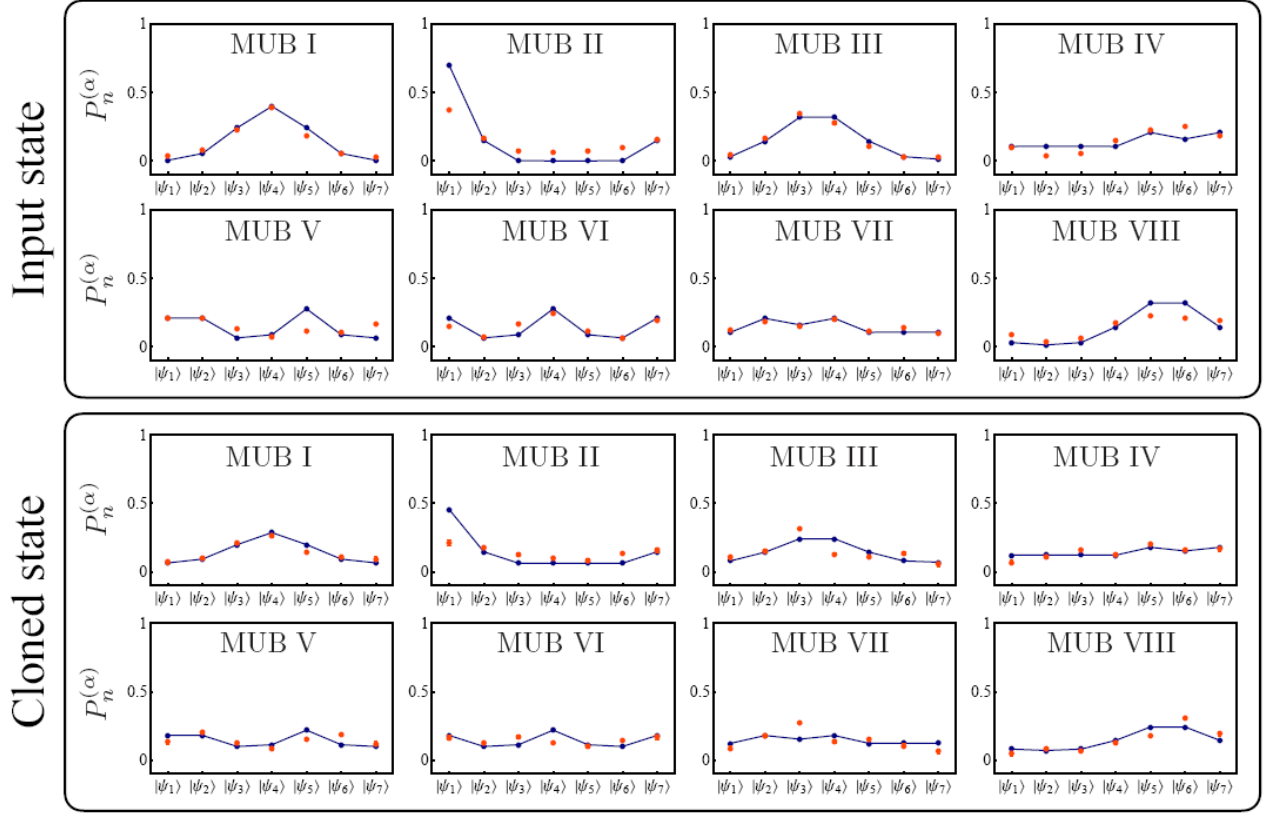


fig. S3. Projective measurements of the input and cloned Gaussian state. Projective measurements $P_n^{(\alpha)}$ are shown for $n = 1, \dots, d$ and $\alpha = 1, \dots, d + 1$. The red points correspond to experimental results and the joined blue points correspond to theoretical values.

Appendix B

Supplementary materials:
Quantum metrology at the limit
with extremal Majorana
constellations

Quantum metrology at the limit with extremal Majorana constellations: supplemental material

F. BOUCHARD¹, P. DE LA HOZ², G. BJÖRK³, R. W. BOYD^{1,4}, M. GRASSL⁵,
Z. HRADIL⁶, E. KARIMI^{1,7}, A. B. KLIMOV⁸, G. LEUCHS^{5,1}, J. ŘEHÁČEK⁶, AND
L. L. SÁNCHEZ-SOTO^{2,5,*}

¹Department of Physics, University of Ottawa, 150 Louis Pasteur, Ottawa, Ontario, K1N 6N5 Canada

²Department of Optics, Faculty of Physics, Universidad Complutense, 28040 Madrid, Spain

³Department of Applied Physics, Royal Institute of Technology (KTH), AlbaNova, SE-106 91 Stockholm, Sweden

⁴Institute of Optics, University of Rochester, Rochester, New York, 14627, USA

⁵Max Planck Institute for the Science of Light, Staudtstraße 2, 91058 Erlangen, Germany

⁶Department of Optics, Palacký University, 17. listopadu 12, 771 46 Olomouc, Czech Republic

⁷Departamento de Óptica, Facultad de Física, Universidad Complutense, 28040 Madrid, Spain

⁸Department of Physics, Institute for Advanced Studies in Basic Sciences, 45137-66731 Zanjan, Iran

⁸Department of Physics, Universidad de Guadalajara, 44420 Guadalajara, Jalisco, Mexico

*Corresponding author: lsanchez@fis.ucm.es

Published 17 November 2017

This document provides supplementary information to “Quantum metrology at the limit with extremal Majorana constellations,” <https://doi.org/10.1364/OPTICA.4.001429>.

<https://doi.org/10.6084/m9.figshare.5533669>

1. MULTIPOLES AND EXTREMAL STATES

We consider a state represented by a density matrix $\hat{\rho}$ living in the $(2S + 1)$ -dimensional Hilbert space $\mathcal{H}_S$ of spin S . The state multipoles can be defined in terms of the Husimi Q function as

$$q_{Kq} = C_K \int_{S_2} d^2\mathbf{n} Y_{Kq}(\mathbf{n}) Q(\mathbf{n}), \quad (1)$$

where the normalization constant is

$$C_K = \sqrt{\frac{4\pi}{2S+1}} \frac{1}{C_{SS,K0}^{SS}}, \quad (2)$$

and $C_{SS,K0}^{SS}$ is a Clebsch-Gordan coefficient [1].

When expressed in the Cartesian basis they appear in a very transparent way. For example, the three dipole (q_{1q}) and the five quadrupole (q_{2q}) terms can be given, respectively, as

$$\wp_i = \langle n_i \rangle, \quad Q_{ij} = \langle 3n_i n_j - \delta_{ij} \rangle, \quad (3)$$

where $\langle f(\mathbf{n}) \rangle = \int_{S_2} d^2\mathbf{n} f(\mathbf{n}) Q(\mathbf{n}) / \int_{S_2} d^2\mathbf{n} Q(\mathbf{n})$ and the index i runs x, y , and z . These multipoles appear then as the standard ones in electrostatics, but replacing the charge density by $Q(\mathbf{n})$ and distances by directions [2]. It is also clear that they are the

K th directional moments of the state constellation and, therefore, these terms resolve progressively finer angular features.

We look at the cumulative distribution

$$\mathcal{A}_M = \sum_{K=1}^M \sum_{q=-K}^K |q_{Kq}|^2, \quad (4)$$

which sums polarization information up to order M ($1 \leq M \leq 2S$). The distribution $\mathcal{A}_M$ can be regarded as a nonlinear functional of the density matrix $\hat{\rho}$. On that account, one can try to ascertain the states that maximize $\mathcal{A}_M$ for each order M . As with any cumulative distribution, $\mathcal{A}_M$ is a monotonically non-decreasing function of the multipole order. We shall be considering only pure states, which we expand in the Dicke basis as $|\Psi\rangle = \sum_{m=-S}^S \Psi_m |S, m\rangle$, with coefficients $\Psi_m = \langle S, m | \Psi \rangle$. We easily get

$$\mathcal{A}_M = \sum_{K=1}^M \sum_{q=-K}^K \frac{2K+1}{2S+1} \left| \sum_{m,m'=-S}^S C_{Sm,Kq}^{Sm'} \Psi_{m'} \Psi_m^* \right|^2. \quad (5)$$

As it has been proven in Ref. [3], spin coherent states $|\mathbf{n}\rangle$ maximize $\mathcal{A}_M$ for all orders M .

We concentrate on the opposite case of states minimizing $\mathcal{A}_M$. Obviously, the maximally mixed state

$$\hat{\rho} = \frac{1}{2S+1} \hat{1}_{2S+1} \quad (6)$$

kills all the multipoles and so indeed causes Eq. (4) to vanish for all M , being fully unpolarized [4, 5]. Nonetheless, we are interested in pure M th-order unpolarized states. The strategy we adopt is thus very simple to state: starting from a set of unknown normalized state amplitudes in Eq. (5), which we write as $\Psi_m = a_m + ib_m$ ($a_m, b_m \in \mathbb{R}$), we try to get $\mathcal{A}_M = 0$ for the highest possible M . This yields a system of polynomial equations of degree two for a_m and b_m , which we solve using Gröbner bases implemented in the computer algebra system MAGMA. In this way, we get exact algebraic expressions and we can detect when there is no feasible solution.

The detailed list of resulting minimal states, which are the Kings of Quantumness, can be found in [6], where the reader can also see the associated Majorana constellations. In this paper, we have considered the cases of $S = 3, 5, 6$ and 10: the Kings have the following nonzero Ψ_m components:

$$\begin{array}{l|l} S=3 & \Psi_{\pm 2} = \mp \frac{1}{\sqrt{2}} \\ S=5 & \Psi_{\pm 5} = \frac{1}{\sqrt{5}} \quad \Psi_0 = \sqrt{\frac{3}{5}} \\ S=6 & \Psi_{\pm 5} = \mp \frac{\sqrt{7}}{5} \quad \Psi_0 = \frac{\sqrt{11}}{5} \\ S=10 & \Psi_{\pm 10} = \frac{\sqrt{561}}{75} \quad \Psi_{\pm 5} = \mp \frac{3\sqrt{209}}{75} \quad \Psi_0 = \frac{\sqrt{741}}{75} \end{array} \quad (7)$$

Intuitively, these constellations seem to have the points as symmetrically placed on the unit sphere as possible. We have explored the connection with spherical t -designs [7], which are patterns of N points on a sphere such that every polynomial of degree at most t has the same average over the N points as over the sphere. Thus, the N points mimic a flat distribution up to order t , which obviously implies a fairly symmetric distribution.

For a given S , the maximal order of M for which we can cancel out $\mathcal{A}_M$ does not follow a clear pattern. However, the numerical evidence suggests that $M_{\max}$ coincides with $t_{\max}$ in the corresponding spherical design. Further work is needed, however, to support this conjecture.

2. ROTATIONAL SENSITIVITY

The goal of our work is the estimation of a rotation $\hat{R}(\omega, \mathbf{u})$ of angle ω around an axis $\mathbf{u}$ of spherical angles (Θ, Φ) ; i.e.,

$$\hat{R}(\omega, \mathbf{u}) = \exp(-i\omega \hat{S} \cdot \mathbf{u}), \quad (8)$$

which is generated precisely by $\hat{S} \cdot \mathbf{u}$. Our measurement was a projection onto the original state; i.e., $\hat{P} = |\Psi\rangle\langle\Psi|$. The sensitivity of the state $|\Psi\rangle$ to this measurement can be retrieved from a simple error propagation [8]

$$\Delta\omega = \frac{\Delta\hat{P}}{|\partial\langle\hat{P}\rangle/\partial\omega|}, \quad (9)$$

where the variance is $\Delta\hat{P} = [\langle\hat{P}^2\rangle - \langle\hat{P}\rangle^2]^{1/2}$. Note that for projective measurements, we have the simplification $\Delta\hat{P} = [\langle\hat{P}\rangle - \langle\hat{P}\rangle^2]^{1/2}$, and so the knowledge of $\langle\hat{P}\rangle$ is enough to assess $\Delta\omega$.

We consider only small rotations, which means that the angle ω is small enough to expand $\hat{R}(\omega, \mathbf{u})$ up to second order. Obviously, $\langle\hat{P}\rangle = |\langle\Psi|\hat{R}|\Psi\rangle|^2$ and then, after a direct computation, we get

$$\langle\hat{P}\rangle = \left| 1 - i\omega \langle\hat{S}\rangle \cdot \mathbf{u} - \frac{1}{2}\omega^2 \langle(\hat{S} \cdot \mathbf{u})^2\rangle \right|^2. \quad (10)$$

The last term is a little messy, but can be evaluated; the result reads (after expanding up to ω^2 and using spherical coordinates)

$$\langle\hat{P}_{\text{Kings}}\rangle = 1 - \frac{1}{3}\omega^2 S(S+1), \quad (11)$$

$$\langle\hat{P}_{\text{NOON}}\rangle = 1 - \frac{1}{2}\omega^2 S \left(\sin^2 \Theta + 2S \cos^2 \Theta \right). \quad (12)$$

From here we can finally get the sensitivity

$$\Delta\omega_{\text{Kings}} = \frac{\sqrt{3}}{2} \frac{1}{\sqrt{S(S+1)}}, \quad (13)$$

$$\Delta\omega_{\text{NOON}} = \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2S^2 \cos^2 \Theta + S \sin^2 \Theta}}, \quad (14)$$

as quoted in the Letter.

3. NOON STATES ROTATION

We experimentally generate our states using the OAM of single photons. In consequence, the index m in the Dicke basis is identified with the OAM eigenvalue ℓ of a single photon along its propagation direction. In this representation, only the azimuthal modes; i.e., $\exp(i\ell\phi)$, are relevant. In general, there exist many families of optical modes carrying OAM. Here, we choose the Laguerre-Gauss basis $\text{LG}_{\ell,p}$. As the radial profile is irrelevant to the experimental realization of the Kings states using OAM, for the sake of simplicity, we set the radial index to its fundamental value; i.e., $p = 0$.

The energy of modes with different azimuthal mode index ℓ varies slightly with the absolute value of the index. Thus a transformation of a state with predominant contribution of modes with large $|\ell|$ to one with a predominant contribution of modes with vanishing ℓ will result in a red-shift due to the rotational Doppler effect. However, for two reasons this effect will be miniscule. The first is that the wave-vector along the axis of propagation is much larger than the azimuthal wave vector. Secondly, the King state per definition comprises of points spread rather evenly on the Bloch sphere, thus involving modes with both small and large $|\ell|$. After a transformation, the points will still be rather evenly spread over the Bloch sphere (the constellation rotates rigidly), so while some of the constituent modes will get red-shifted, other will be blue-shifted. This will further act to hide any rotational Doppler shift.

In Fig. 1, we experimentally confirm the superiority of the Kings over the NOON states. For this purpose, we have used the case of $S = 3, 6$ and 10, as well. To compare the performances of the NOON states with that of the Kings, we perform the same set of projective measurements by rotating the NOON states over the same axes discussed in previously for the Kings. However, due to their lack of rotation sensitivity, the NOON states are studied under a full rotation of π . As it was expected, the NOON states possess the largest sensitivity to rotation for a single axis (z), thus overcoming the Kings for this case. Nonetheless, it is clearly evident that the Kings are distinctly superior with respect to any other rotation axes.

4. TOMOGRAPHIC RECONSTRUCTION

To verify the generated states two different sets of projections were utilized: (i) projections onto coherent states and (ii) projections onto rotated Kings with the axes of rotations defined

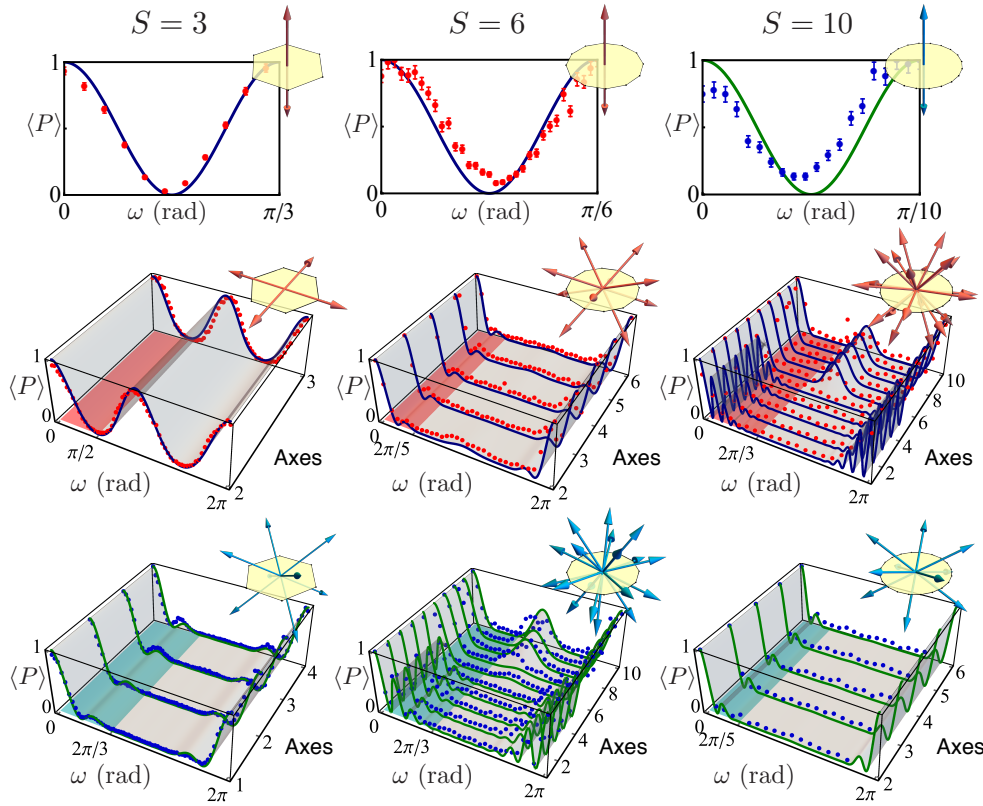


Fig. 1. Kings superiority over NOON states. Experimental results of projecting NOON states corresponding to $S = 3, 6$ and 10 onto themselves after a rotation along the various axes sketched in Fig. 3 of the main text. In the first row, the NOON states are rotated around their optimal z axis. For a comparison of the NOON versus the Kings, we show rotations of the NOON states along the axes of rotation defined by the Majorana points (second row) and the normal to the facets (third row) of the constellations of the Kings with corresponding S . The axes are presented graphically along with the associated constellations on the top-right corner of each plot. The coloured region (red for Majorana points rotations and blue for facets rotation) shows the region for which the Kings are mapped back onto themselves, as shown in Fig. 3 of the main text.

by the Majorana points. Such a D -dimensional channel can be described by an overcomplete positive operator-valued measurement (POVM) $\hat{\Pi}_j \geq 0, j = 1, \dots, D$. The probabilities p_j of observed relative frequencies f_j , as given by the Born rule $p_j = \text{Tr}(\hat{\rho} \hat{\Pi}_j)$ can be inverted by maximizing the Fermi extended likelihood [9]

$$\mathcal{L} = \sum_j f_j \log \left(\frac{p_j}{\sum_{j'} p_{j'}} \right) \quad (15)$$

to yield the Kings estimates. This amounts to solving the extremal equation

$$\hat{R} \hat{Q} = \hat{G} \hat{Q}, \quad (16)$$

where we have defined

$$\hat{R} = \sum_j \frac{f_j}{p_j(\rho)} \hat{\Pi}_j, \quad \hat{G} = \frac{\sum_j f_j}{\sum_j p_j(\rho)} \sum_j \hat{\Pi}_j. \quad (17)$$

This can be solved in an iterative way

$$\hat{Q}^{(k+1)} = \hat{G}^{-1} \hat{R} \hat{Q}^{(k)} \hat{R} \hat{G}^{-1}, \quad (18)$$

starting from the $(2S + 1)$ -dimensional maximally mixed state (6). A few thousand of iterations are typically needed to observe a convergence to the stationary point of the map Eq. (16).

In the experiment, several hundred of projections were recorded for each King and the fidelities of the estimated states

with respect to the target states were found to be close to or in excess of 90% in all cases. See Table 1 for details.

The conventional description of the quantum world involves a key mathematical object—the quantum state—that conveys complete information about the system under study: once it is known, the probabilities of the outcomes of any measurement can be predicted. This statistical description entails many counterintuitive effects that have prompted several notions of quantumness, yet no single one captures the whole breadth of the physics.

S	dim	D	fidelity
3	7	288	0.94
5	11	572	0.87
6	13	544	0.91
10	21	1054	0.93

Table 1. Measurement sizes D and resulting fidelities obtained with quantum state tomography of experimentally generated King states.

REFERENCES

1. D. A. Varshalovich, A. N. Moskalev, and V. K. Khersonskii, *Quantum Theory of Angular Momentum* (World Scientific, Singapore, 1988).
2. J. D. Jackson, *Classical Electrodynamics* (John Wiley, New York, 1999), 3rd ed.
3. G. Björk, A. B. Klimov, P. de la Hoz, M. Grassl, G. Leuchs, and L. L. Sánchez-Soto, "Extremal quantum states and their Majorana constellations," *Phys. Rev. A* **92**, 031801 (2015).
4. H. Prakash and N. Chandra, "Density operator of unpolarized radiation," *Phys. Rev. A* **4**, 796–799 (1971).
5. G. S. Agarwal, "On the state of unpolarized radiation," *Lett. Nuovo Cimento* **1**, 53–56 (1971).
6. "<http://polarization.markus-grassl.de/>," .
7. P. Delsarte, J. M. Goethals, and J. J. Seidel, "Spherical codes and designs," *Geom. Dedicata* **6**, 363–388 (1977).
8. A. K. Jha, G. S. Agarwal, and R. W. Boyd, "Supersensitive measurement of angular displacements using entangled photons," *Phys. Rev. A* **83**, 053829 (2011).
9. M. G. A. Paris and J. Řeháček, eds., *Quantum State Estimation*, vol. 649 of *Lect. Not. Phys.* (Springer, Berlin, 2004).

Appendix C

Supplementary materials:
High-dimensional intracity
quantum cryptography with
structured photons

High-dimensional intracity quantum cryptography with structured photons: supplementary material

**ALICIA SIT¹, FRÉDÉRIC BOUCHARD¹, ROBERT FICKLER¹, JÉRÉMIE GAGNON-BISCHOFF¹,
HUGO LAROCQUE¹, KHABAT HESHAMI², DOMINIQUE ELSE^{3,4}, CHRISTIAN PEUNTINGER^{3,4},
KEVIN GÜNTHER^{3,4}, BETTINA HEIM^{3,4}, CHRISTOPH MARQUARDT^{3,4}, Gerd LEUCHS^{1,3,4},
ROBERT W. BOYD^{1,5}, AND EBRAHIM KARIMI^{1,6,*}**

¹Physics Department, Centre for Research in Photonics, University of Ottawa, Advanced Research Complex, 25 Templeton, Ottawa ON K1N 6N5, Canada

²National Research Council of Canada, 100 Sussex Drive, Ottawa ON K1A 0R6, Canada

³Max-Planck-Institut für die Physik des Lichts, Staudtstraße 2, 91058 Erlangen, Germany

⁴Institut für Optik, Information und Photonik, Universität Erlangen-Nürnberg, Staudtstraße 7/B2, 91058 Erlangen, Germany

⁵Institute of Optics, University of Rochester, Rochester, New York, 14627, USA

⁶Department of Physics, Institute for Advanced Studies in Basic Sciences, 45137-66731 Zanjan, Iran

*Corresponding author: ekarimi@uottawa.ca

Published 24 August 2017

This document provides supplementary information to “High-dimensional intracity quantum cryptography with structured photons,” <https://doi.org/10.1364/optica.4.001006>. © 2017 Optical Society of America

<https://doi.org/10.6084/m9.figshare.5248189>

1. MUTUALLY UNBIASED BASIS

Given a set of bases $\alpha_0, \dots, \alpha_n$ of dimension d , they are said to be mutually unbiased with respect to one another if they satisfy the following condition,

$$|\langle \alpha_i | \alpha_{i'} \rangle|^2 = \begin{cases} \delta_{j,j'} & \forall i = i' \\ \frac{1}{d} & \forall i \neq i' \end{cases}; \quad i \in \{0, 1, \dots, n\}, \quad j \in \{1, 2, \dots, d\}. \quad (\text{S1})$$

For dimensions where d is a power of a prime, $d + 1$ mutually unbiased bases (MUBs) can be found. For 2-dimensional quantum key distribution (QKD) protocols, photons can be encoded using polarization and orbital angular momentum (OAM). We represent states of light that have a particular polarization and OAM value using a compound ket notation. In this way, if a photon has a certain polarization Π and carries ℓ units of OAM, it is written as $|\Pi, \ell\rangle$.

The two MUBs of dimension 2 are given by,

$$\begin{aligned} \{|\xi\rangle^i\} &= \left\{ \frac{1}{\sqrt{2}} (|L, -\ell\rangle + |R, +\ell\rangle), \frac{1}{\sqrt{2}} (|L, -\ell\rangle - |R, +\ell\rangle) \right\}, \\ \{|\xi\rangle^j\} &= \left\{ \frac{1}{\sqrt{2}} (|L, -\ell\rangle + i|R, +\ell\rangle), \frac{1}{\sqrt{2}} (|L, -\ell\rangle - i|R, +\ell\rangle) \right\}. \end{aligned} \quad (\text{S2})$$

In dimension 4, the natural basis is $|k\rangle \in$

$\{|H, \ell\rangle, |H, -\ell\rangle, |V, \ell\rangle, |V, -\ell\rangle\}$, and the two sets of MUBs $\{|\psi\rangle^i\}$ and $\{|\varphi\rangle^j\}$ were generated by the following matrices,

$$\begin{aligned} \mathcal{M}_0^{ik} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \\ \mathcal{M}_1^{jk} &= \frac{1}{2} \begin{pmatrix} 1 & i & 1 & -i \\ 1 & i & -1 & i \\ 1 & -i & 1 & i \\ -1 & i & 1 & i \end{pmatrix}, \end{aligned} \quad (\text{S3})$$

such that $|\psi\rangle^i = \mathcal{M}_0^{ik} |k\rangle$ and $|\varphi\rangle^j = \mathcal{M}_1^{jk} |k\rangle$. This results in the following states:

$$\{|\psi\rangle^i\} = \{|H, +\ell\rangle, |H, -\ell\rangle, |V, +\ell\rangle, |V, -\ell\rangle\}, \quad (\text{S4})$$

$$\begin{aligned} \{|\varphi\rangle^j\} &= \left\{ \frac{1}{\sqrt{2}} (|L, \ell\rangle + |R, -\ell\rangle), \frac{1}{\sqrt{2}} (|L, \ell\rangle - |R, -\ell\rangle), \right. \\ &\quad \left. \frac{1}{\sqrt{2}} (|L, -\ell\rangle + |R, \ell\rangle), \frac{1}{\sqrt{2}} (|L, -\ell\rangle - |R, \ell\rangle) \right\}. \end{aligned} \quad (\text{S5})$$

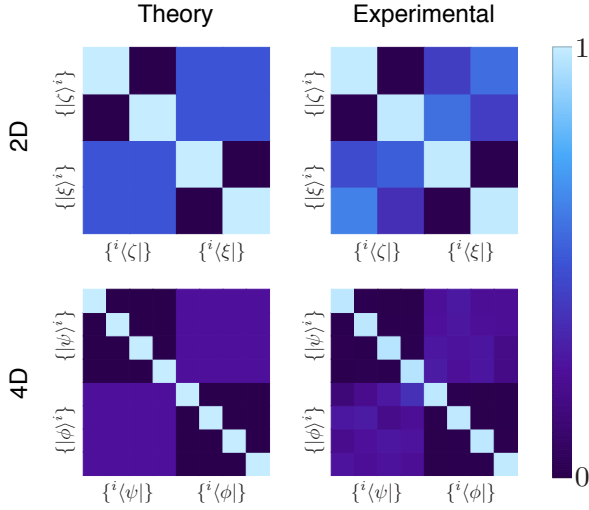


Fig. S1. Visualization of MUBs in $d=2$ and $d=4$ Theoretical probability-of-detection matrices (left column) for dimensions 2 and 4 using Eq. (S2) and Eqs. (S4–S5) by applying Eq. (S1). The probability-of-detection matrices as measured in the laboratory (right column) give bit error rates of 0.83% and 1.83% in dimensions 2 ($\ell = 2$) and 4 ($\ell = 2$), respectively.

Figure S1 shows a visual representation of the 2D (top row) and 4D (bottom row) MUBs using Eq. (S1), comparing the theoretical probability-of-detection matrix to the experimental one as measured in the laboratory, i.e. without the intra-city link. The quantum bit error rate is calculated as one minus the average of the on-diagonal elements. The calculated quantum bit error rates from the experimentally measured matrices are 0.83% and 1.83% in dimensions 2 ($\ell = 2$) and 4 ($\ell = 2$), respectively.

2. GENERATION OF IMPLEMENTED MUBS IN $D = 2$ AND 4

In order to create structured photons possessing both polarization and OAM, we utilize patterned liquid crystal devices known as q -plates. Q -plates coherently couple spin (i.e. polarization) to orbital angular momentum such that $\ell = \pm 2q$, where q is the topological charge of the liquid crystal distribution. The action of a q -plate is as follows:

$$|L, 0\rangle \xrightarrow{q\text{-plate}} |R, +2q\rangle, \quad (\text{S6})$$

$$|R, 0\rangle \xrightarrow{q\text{-plate}} |L, -2q\rangle. \quad (\text{S7})$$

Since q -plates are linear devices, a photon in a superposition of $|L, 0\rangle$ and $|R, 0\rangle$ will be mapped to a state in a superposition of $|R, +2q\rangle$ and $|L, -2q\rangle$. Thus, just as waveplates are used to transform polarization states on the Poincaré sphere, waveplates in combination with a q -plate perform the same transformations on a hybrid OAM-Poincaré sphere.

The MUBs in dimension 2, $\{|\zeta\rangle^i\}$ and $\{|\xi\rangle^i\}$ are generated using the sequence of a half-wave plate (HWP) followed by a q -plate. The

waveplate angles are given in (S8).

state	HWP
$ \zeta\rangle^1$	0°
$ \zeta\rangle^2$	$+45^\circ$
$ \xi\rangle^1$	$+22.5^\circ$
$ \xi\rangle^2$	-22.5°

(S8)

The MUBs in dimension 4, $\{|\psi\rangle^i\}$ and $\{|\varphi\rangle^i\}$ are generated by sandwiching a q -plate between either HWPs or QWPs. If photons pass left to right through the following optical elements, the waveplate angles that Alice uses to generate $\{|\psi\rangle^i\}$ are given in the (S9), and $\{|\varphi\rangle^i\}$ in (S10).

state	QWP before QP	QWP after QP
$ \psi\rangle^1$	-45°	-45°
$ \psi\rangle^2$	$+45^\circ$	$+45^\circ$
$ \psi\rangle^3$	-45°	$+45^\circ$
$ \psi\rangle^4$	$+45^\circ$	-45°

(S9)

state	HWP before QP	HWP after QP
$ \varphi\rangle^1$	0°	0°
$ \varphi\rangle^2$	$+45^\circ$	0°
$ \varphi\rangle^3$	0°	–
$ \varphi\rangle^4$	$+45^\circ$	–

(S10)

Bob uses the same waveplate angles, but mirrors the sequence of waveplates as Alice has in order to project his received photons onto a particular state.

3. EXPERIMENTAL DATA

Coincidence counts are accumulated per 200 ms. For each of Bob's measurements, he records fifty data points. Bob obtains a probability-of-detection matrix by averaging the data points for each measurement and then normalizing over each state that Alice sends. The states that Alice sends and the states that Bob projects onto are labelled on the left and top, respectively, of each matrix below.

Normalized raw data for probability-of-detection matrix in dimension 2 as measured across the intra-city link using a $q=1/2$ -plate, as shown in Fig. 3a of the main text (top row):

$$\begin{array}{c}
 \begin{array}{cc} {}^1\langle\zeta| & {}^2\langle\zeta| \\ {}^1\langle\xi| & {}^2\langle\xi| \end{array} \\
 \begin{array}{c} |\zeta\rangle^1 \\ |\zeta\rangle^2 \\ |\xi\rangle^1 \\ |\xi\rangle^2 \end{array}
 \end{array}
 \begin{pmatrix}
 0.971 & 0.029 & 0.421 & 0.579 \\
 0.062 & 0.938 & 0.677 & 0.323 \\
 0.731 & 0.269 & 0.959 & 0.041 \\
 0.459 & 0.541 & 0.068 & 0.932
 \end{pmatrix}
 \quad (\text{S11})$$

Target corrected data from (S11):

$$\begin{array}{c}
 \begin{array}{cc} {}^1\langle\zeta| & {}^2\langle\zeta| \\ {}^1\langle\xi| & {}^2\langle\xi| \end{array} \\
 \begin{array}{c} |\zeta\rangle^1 \\ |\zeta\rangle^2 \\ |\xi\rangle^1 \\ |\xi\rangle^2 \end{array}
 \end{array}
 \begin{pmatrix}
 0.972 & 0.028 & 0.351 & 0.649 \\
 0.050 & 0.950 & 0.653 & 0.347 \\
 0.725 & 0.275 & 0.961 & 0.039 \\
 0.463 & 0.537 & 0.069 & 0.931
 \end{pmatrix}
 \quad (\text{S12})$$

Normalized raw data for probability-of-detection matrix in dimension 4 as measured across the intra-city link:

$$\begin{array}{c}
 \begin{array}{c} |\psi\rangle^1 \\ |\psi\rangle^3 \\ |\psi\rangle^2 \\ |\psi\rangle^4 \\ |\varphi\rangle^1 \\ |\varphi\rangle^2 \\ |\varphi\rangle^3 \\ |\varphi\rangle^4 \end{array}
 \begin{array}{c}
 \begin{array}{c} {}^1\langle\psi| \quad {}^3\langle\psi| \quad {}^2\langle\psi| \quad {}^4\langle\psi| \end{array}
 \left| \begin{array}{c} {}^1\langle\varphi| \quad {}^2\langle\varphi| \quad {}^3\langle\varphi|^3 \quad {}^4\langle\varphi| \end{array} \right. \\
 \begin{pmatrix}
 0.918 & 0.019 & 0.051 & 0.012 & 0.252 & 0.245 & 0.275 & 0.228 \\
 0.020 & 0.937 & 0.038 & 0.005 & 0.190 & 0.192 & 0.312 & 0.306 \\
 0.012 & 0.156 & 0.816 & 0.012 & 0.279 & 0.277 & 0.289 & 0.155 \\
 0.149 & 0.009 & 0.018 & 0.824 & 0.152 & 0.195 & 0.384 & 0.269 \\
 0.319 & 0.125 & 0.325 & 0.231 & 0.869 & 0.039 & 0.064 & 0.029 \\
 0.252 & 0.217 & 0.239 & 0.292 & 0.038 & 0.822 & 0.042 & 0.098 \\
 0.185 & 0.177 & 0.447 & 0.191 & 0.065 & 0.027 & 0.872 & 0.037 \\
 0.207 & 0.205 & 0.381 & 0.208 & 0.030 & 0.134 & 0.036 & 0.800
 \end{pmatrix}
 \end{array}
 \end{array} \quad (S13)$$

Target corrected data from (S13), as shown in Fig. 3a of the main text (bottom row):

$$\begin{array}{c}
 \begin{array}{c} |\psi\rangle^1 \\ |\psi\rangle^3 \\ |\psi\rangle^2 \\ |\psi\rangle^4 \\ |\varphi\rangle^1 \\ |\varphi\rangle^2 \\ |\varphi\rangle^3 \\ |\varphi\rangle^4 \end{array}
 \begin{array}{c}
 \begin{array}{c} {}^1\langle\psi| \quad {}^3\langle\psi| \quad {}^2\langle\psi| \quad {}^4\langle\psi| \end{array}
 \left| \begin{array}{c} {}^1\langle\varphi| \quad {}^2\langle\varphi| \quad {}^3\langle\varphi|^3 \quad {}^4\langle\varphi| \end{array} \right. \\
 \begin{pmatrix}
 0.924 & 0.035 & 0.011 & 0.031 & 0.272 & 0.232 & 0.254 & 0.243 \\
 0.024 & 0.960 & 0.012 & 0.004 & 0.197 & 0.213 & 0.260 & 0.330 \\
 0.005 & 0.052 & 0.930 & 0.013 & 0.239 & 0.301 & 0.301 & 0.159 \\
 0.049 & 0.004 & 0.029 & 0.918 & 0.094 & 0.242 & 0.433 & 0.232 \\
 0.376 & 0.108 & 0.321 & 0.195 & 0.874 & 0.033 & 0.065 & 0.028 \\
 0.273 & 0.197 & 0.255 & 0.275 & 0.035 & 0.825 & 0.045 & 0.096 \\
 0.200 & 0.132 & 0.511 & 0.157 & 0.060 & 0.016 & 0.889 & 0.035 \\
 0.186 & 0.163 & 0.365 & 0.287 & 0.026 & 0.129 & 0.043 & 0.803
 \end{pmatrix}
 \end{array}
 \end{array} \quad (S14)$$

Normalized raw data for probability-of-detection matrix in dimension 4 on a turbulent night:

$$\begin{array}{c}
 \begin{array}{c} |\psi\rangle^1 \\ |\psi\rangle^3 \\ |\psi\rangle^2 \\ |\psi\rangle^4 \\ |\varphi\rangle^1 \\ |\varphi\rangle^2 \\ |\varphi\rangle^3 \\ |\varphi\rangle^4 \end{array}
 \begin{array}{c}
 \begin{array}{c} {}^1\langle\psi| \quad {}^3\langle\psi| \quad {}^2\langle\psi| \quad {}^4\langle\psi| \end{array}
 \left| \begin{array}{c} {}^1\langle\varphi| \quad {}^2\langle\varphi| \quad {}^3\langle\varphi|^3 \quad {}^4\langle\varphi| \end{array} \right. \\
 \begin{pmatrix}
 0.741 & 0.032 & 0.043 & 0.184 & 0.370 & 0.168 & 0.364 & 0.098 \\
 0.096 & 0.722 & 0.138 & 0.044 & 0.120 & 0.432 & 0.221 & 0.228 \\
 0.043 & 0.177 & 0.755 & 0.025 & 0.276 & 0.247 & 0.197 & 0.281 \\
 0.101 & 0.041 & 0.047 & 0.811 & 0.122 & 0.433 & 0.332 & 0.113 \\
 0.126 & 0.471 & 0.197 & 0.206 & 0.707 & 0.051 & 0.144 & 0.098 \\
 0.211 & 0.234 & 0.352 & 0.203 & 0.110 & 0.694 & 0.079 & 0.117 \\
 0.265 & 0.285 & 0.259 & 0.191 & 0.195 & 0.056 & 0.632 & 0.117 \\
 0.478 & 0.146 & 0.185 & 0.191 & 0.048 & 0.103 & 0.075 & 0.775
 \end{pmatrix}
 \end{array}
 \end{array} \quad (S15)$$

4. NUMERICAL APPROACH FOR THE SECRET KEY RATE CALCULATION

Here we use a numerical approach to calculate the secret key rate for the MUBs in the current experiment that are shown in Eqs. (S3–S5). The secret key rate calculation below relies on the dual optimization problem that has recently been introduced as an efficient numerical approach for unstructured quantum key distribution [1]. The main result in [1] indicates that the achievable secure key rate is lower bounded by the following maximization problem,

$$K \geq \frac{\Theta}{\ln 2} - H(Z_A|Z_B), \quad (S15)$$

where

$$\Theta := \max_{\vec{\lambda}} \left(- \left\| \sum_j Z_A^j R(\vec{\lambda}) Z_A^j \right\| - \vec{\lambda} \cdot \vec{\gamma} \right), \quad (S16)$$

and

$$R(\vec{\lambda}) := \exp(-\mathbb{1} - \vec{\lambda} \cdot \vec{\Gamma}). \quad (S17)$$

Here Z_A (Z_B) denotes the measurement performed by Alice (Bob) to derive the raw key, and $\vec{\gamma} = \{\gamma_i := \text{Tr}(\rho_{AB} \Gamma_i)\}$ are determined through average value of experimental measurements.

For the generalized BB84 in dimension $d = 4$ with two MUBs, the experimental constraints can be summarized to

$$\text{Key-map POVM: } Z_A = \{|\psi\rangle^i \langle\psi|, \text{ for } i = 1 \cdots d = 4\} \quad (S18)$$

$$\text{Constraints: } \langle \mathbb{1} \rangle = 1 \quad (S19)$$

$$\langle \mathbf{E}_X \rangle = Q \quad (S20)$$

$$\langle \mathbf{E}_Z \rangle = Q \quad (S21)$$

where $\mathbf{E}_{Z(X)}$ are coarse-grained error operators in $\mathcal{M}_{0(1)}$ MUBs and defined as

$$\mathbf{E}_X = \mathbb{1} - \sum_i^{d=4} |\psi\rangle^i \langle\psi| \otimes |\psi\rangle^i \langle\psi| \quad (S22)$$

$$\mathbf{E}_Z = \mathbb{1} - \sum_i^{d=4} |\varphi\rangle^i \langle\varphi| \otimes |\varphi\rangle^i \langle\varphi|. \quad (S23)$$

Eqs. (S4) and (S5) show the definition for $|\psi\rangle^i$ and $|\varphi\rangle^i$ basis states.

Figure S2 shows the numerical result of the optimization problem in Eq. (S15) with MUBs in Eqs. (S4,S5) in comparison with the theoretical key rates in [2, 3]. This numerical approach may be extended to find secret key rate per signal with two-way classical communications to tolerate higher qubit error rates [4].

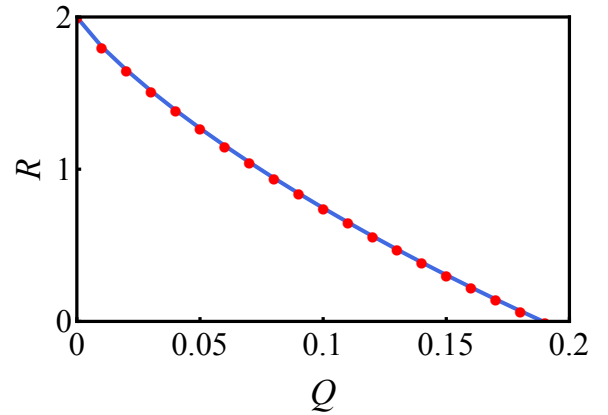


Fig. S2. Secret key rate per signal for BB84 in $d=4$ with 2 MUBs. Solution to the numerical optimization problem in Eq. (S15) are shown for different values of average error rates (red dots). As it can be seen, the numerical optimization saturates the bound and shows a good agreement with the theory from [2, 3]. For more details on the numerical approach see [1].

REFERENCES

1. P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, “Numerical approach for unstructured quantum key distribution,” *Nature Communications* **7**, 11712 (2016).
2. A. Ferenczi, and N. Lütkenhaus, “Symmetries in quantum key distribution and the connection between optical attacks and optimal cloning,” *Physical Review A* **85**, 052310 (2012).
3. L. Sheridan, and V. Scarani, “Security proof for quantum key distribution using qudit systems,” *Physical Review A* **82**, 030301 (2010).

4. G. M. Nikolopoulos, K. S. Ranade, and G. Alber, “Error tolerance of two-basis quantum-key-distribution protocols using qudits and two-way classical communication,” *Physical Review A* **73**, 032325 (2006).

Bibliography

- [1] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777, 1935.
- [2] N. Bohr. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 48(8):696, 1935.
- [3] J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.
- [4] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Physical Review Letters*, 28(14):938, 1972.
- [5] E. S. Fry and R. C. Thompson. Experimental test of local hidden-variable theories. *Physical Review Letters*, 37(8):465, 1976.
- [6] A. Aspect, J. Dalibard, and G. Roger. Experimental test of bell's inequalities using time-varying analyzers. *Physical Review Letters*, 49(25):1804, 1982.
- [7] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661, 1991.
- [8] J. P. Dowling and G. J. Milburn. Quantum technology: the second quantum revolution. *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 361(1809):1655–1674, 2003.
- [9] M. A Nielsen and I. Chuang. Quantum computation and quantum information. *AAPT*, 2002.
- [10] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces.*, 1984.

- [11] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145, 2002.
- [12] C. L. Degen, F. Reinhard, and P. Cappellaro. Quantum sensing. *Reviews of Modern Physics*, 89(3):035002, 2017.
- [13] W. Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik*, 43:172–198, 1927.
- [14] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802, 1982.
- [15] S. Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.
- [16] M. Hillery, V. Bužek, and A. Berthiaume. Quantum secret sharing. *Physical Review A*, 59(3):1829, 1999.
- [17] V. Scarani, H. Bechmann-Pasquinucci, N. J Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301, 2009.
- [18] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28, 1992.
- [19] A. Muller, J. Breguet, and N. Gisin. Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km. *EPL (Europhysics Letters)*, 23(6):383, 1993.
- [20] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons. Practical free-space quantum key distribution over 1 km. *Physical Review Letters*, 81(15):3283, 1998.
- [21] H. Bechmann-Pasquinucci and W. Tittel. Quantum cryptography using larger alphabets. *Physical Review A*, 61(6):062308, 2000.
- [22] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin. Security of quantum key distribution using d-level systems. *Physical Review Letters*, 88(12):127902, 2002.
- [23] T. Sasaki, Y. Yamamoto, and M. Koashi. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature*, 509(7501):475, 2014.

- [24] H. Larocque, J. Gagnon-Bischoff, D. Mortimer, Y. Zhang, F. Bouchard, J. Upham, V. Grillo, R. W. Boyd, and E. Karimi. Generalized optical angular momentum sorter and its application to high-dimensional quantum cryptography. *Optics Express*, 25(17):19832–19843, 2017.
- [25] A. Sit, R. Fickler, F. Alsaiani, F. Bouchard, H. Larocque, P. Gregg, L. Yan, R. W. Boyd, S. Ramachandran, and E. Karimi. Quantum cryptography with structured photons through a vortex fiber. *Optics Letters*, 43(17):4108–4111, 2018.
- [26] F. Bouchard, D. Koutný, F. Hufnagel, Z. Hradil, J. Řeháček, Y.-S. Teo, D. Ahn, H. Jeong, L. L. Sánchez-Soto, G. Leuchs, and E. Karimi. Compressed sensing of twisted photons. *Opt. Express*, 27(13):17426–17434, Jun 2019.
- [27] Y. Zhang, A. Sit, F. Bouchard, H. Larocque, F. Grenapin, E. Cohen, A. C. Elitzur, J. L. Harden, R. W. Boyd, and E. Karimi. Interaction-free ghost-imaging of structured objects. *Optics Express*, 27(3):2212–2224, 2019.
- [28] F. Nejdassattari, Y. Zhang, F. Bouchard, H. Larocque, A. Sit, E. Cohen, R. Fickler, and E. Karimi. Experimental realization of wave-packet dynamics in cyclic quantum walks. *Optica*, 6(2):174–180, 2019.
- [29] D. Ahn, Y.-S. Teo, H. Jeong, F. Bouchard, F. Hufnagel, E. Karimi, D. Koutný, J. Řeháček, Z. Hradil, G. Leuchs, and L. L. Sanchez-Soto. Adaptive compressive tomography with no a priori information. *Physical Review Letters*, 122(10):100404, 2019.
- [30] S. Ecker, F. Bouchard, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, and M. Huber. Entanglement distribution beyond qubits or: How i stopped worrying and learned to love the noise. *arXiv preprint arXiv:1904.01552*, 2019.
- [31] P. Woźniak, P. Banzer, F. Bouchard, E. Karimi, G. Leuchs, and R. W. Boyd. Tighter spots of light with superposed orbital-angular-momentum beams. *Physical Review A*, 94(2):021803, 2016.
- [32] H. Larocque, J. Gagnon-Bischoff, F. Bouchard, R. Fickler, J. Upham, R. W. Boyd, and E. Karimi. Arbitrary optical wavefront shaping via spin-to-orbit coupling. *Journal of Optics*, 18(12):124002, 2016.

- [33] F. Tamburini, B. Thidé, I. Licata, F. Bouchard, and E. Karimi. Majorana states for subluminal structured photons. *arXiv preprint arXiv:1707.07160*, 2017.
- [34] M. G. Rahimian, F. Bouchard, H. Al-Khazraji, E. Karimi, P. B. Corkum, and V. R. Bhardwaj. Polarization dependent nanostructuring of silicon with femtosecond vortex pulse. *APL Photonics*, 2(8):086104, 2017.
- [35] T. Bauer, P. Banzer, F. Bouchard, S. Orlov, L. Marrucci, E. Santamato, R. W. Boyd, E. Karimi, and G. Leuchs. Multi-twist polarization ribbon topologies in highly-confined optical fields. *New Journal of Physics*, 21(5):053020, may 2019.
- [36] F. Bouchard, H. Larocque, A. M. Yao, C. Travis, I. De Leon, Andrea Rubano, Ebrahim Karimi, Gian-Luca Oppo, and R. W. Boyd. Polarization shaping for control of nonlinear propagation. *Physical review letters*, 117(23):233903, 2016.
- [37] F. Kong, C. Zhang, F. Bouchard, Z. Li, G. G. Brown, D. H. Ko, T. J. Hammond, L. Arissian, R. W. Boyd, E. Karimi, and P. B. Corkum. Controlling the orbital angular momentum of high harmonic vortices. *Nature Communications*, 8:14970, 2017.
- [38] F. Kong, C. Zhang, H. Larocque, F. Bouchard, Z. Li, M. Taucer, G. Brown, T. J. Hammond, E. Karimi, and P. B. Corkum. Spin constrained orbital angular momentum control in high-harmonic generation. *arXiv preprint arXiv:1810.05894*, 2018.
- [39] F. Kong, C. Zhang, H. Larocque, Z. Li, F. Bouchard, D. H. Ko, G. G. Brown, A. Korobenko, T. J. Hammond, R. W. Boyd, E. Karimi, and P. B. Corkum. Vectorizing the spatial structure of high-harmonic radiation from gas. *Nature Communications*, 10(1):2020, 2019.
- [40] H. Larocque, F. Bouchard, V. Grillo, A. Sit, S. Frabboni, R. E. Dunin-Borkowski, M. J. Padgett, R. W. Boyd, and E. Karimi. Nondestructive measurement of orbital angular momentum for an electron beam. *Physical Review Letters*, 117(15):154801, 2016.
- [41] V. Grillo, A. H. Tavabi, F. Venturi, H. Larocque, R. Balboni, G. C. Gazzadi, S. Frabboni, P.-H. Lu, E. Mafakheri, F. Bouchard, R. E. Dunin-Borkowski, R. W. Boyd, M. P. J. Lavery, M. J. Padgett, and E. Karimi. Measuring the orbital angular momentum spectrum of an electron beam. *Nature Communications*, 8:15536, 2017.

- [42] V. Grillo, T. R. Harvey, F. Venturi, J. S. Pierce, R. Balboni, F. Bouchard, G. C. Gazzadi, S. Frabboni, A. H. Tavabi, Z.-A. Li, R. E. Dunin-Borkowski, R. W. Boyd, B. McMorran, and E. Karimi. Observation of nanoscale magnetic fields using twisted electron beams. *Nature Communications*, 8(1):689, 2017.
- [43] Hugo Larocque, Ido Kaminer, Vincenzo Grillo, Gerd Leuchs, Miles J Padgett, Robert W Boyd, Mordechai Segev, and Ebrahim Karimi. ‘twisted’electrons. *Contemporary Physics*, 59(2):126–144, 2018.
- [44] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman. Orbital angular momentum of light and the transformation of laguerre-gaussian laser modes. *Physical Review A*, 45(11):8185, 1992.
- [45] S. Franke-Arnold, L. Allen, and M. J. Padgett. Advances in optical angular momentum. *Laser & Photonics Reviews*, 2(4):299–313, 2008.
- [46] S. W. Hell. Far-field optical nanoscopy. *science*, 316(5828):1153–1158, 2007.
- [47] L. Paterson, M. P. MacDonald, J. Arlt, W. Sibbett, P. E. Bryant, and K. Dholakia. Controlled rotation of optically trapped microscopic particles. *Science*, 292(5518):912–914, 2001.
- [48] H He, NR Heckenberg, and H Rubinsztein-Dunlop. Optical particle trapping with higher-order doughnut beams produced using high efficiency computer generated holograms. *Journal of Modern Optics*, 42(1):217–223, 1995.
- [49] NR Heckenberg, R McDuff, CP Smith, and AG White. Generation of optical phase singularities by computer-generated holograms. *Optics letters*, 17(3):221–223, 1992.
- [50] A. Forbes, A. Dudley, and M. McLaren. Creation and detection of optical modes with spatial light modulators. *Advances in Optics and Photonics*, 8(2):200–227, 2016.
- [51] L. Marrucci, C. Manzo, and D. Paparo. Optical spin-to-orbital angular momentum conversion in inhomogeneous anisotropic media. *Physical Review Letters*, 96(16):163905, 2006.
- [52] S. Slussarenko, A. Murauski, T. Du, V. Chigrinov, L. Marrucci, and E. Santamato. Tunable liquid crystal q-plates with arbitrary topological charge. *Optics Express*, 19(5):4085–4090, 2011.

- [53] F. Cardano, E. Karimi, S. Slussarenko, L. Marrucci, C. de Lisio, and E. Santamato. Polarization pattern of vector vortex beams generated by q-plates with different topological charges. *Applied Optics*, 51(10):C1–C6, 2012.
- [54] H. Rubinsztein-Dunlop, A. Forbes, M. V. Berry, M. R. Dennis, D. L. Andrews, M. Mansuripur, C. Denz, C. Alpmann, P. Banzer, T. Bauer, E. Karimi, L. Marrucci, M. Padgett, M. Ritsch-Marte, N. M. Litchinitser, N. P. Bigelow, C. Rosales-Guzmán, A. Belmonte, J. P. Torres, T. W. Neely, M. Baker, R. Gordon, A. B. Stilgoe, J. Romero, A. G. White, R. Fickler, A. E. Willner, G. Xie, B. McMorran, and A. M. Weiner. Roadmap on structured light. *Journal of Optics*, 19(1):013001, 2016.
- [55] D. Lin, P. Fan, E. Hasman, and M. L. Brongersma. Dielectric gradient metasurface optical elements. *Science*, 345(6194):298–302, 2014.
- [56] E. Karimi, S. A. Schulz, I. De Leon, H. Qassim, J. Upham, and R. W. Boyd. Generating optical orbital angular momentum at visible wavelengths using a plasmonic metasurface. *Light: Science & Applications*, 3(5):e167, 2014.
- [57] F. Bouchard, I. De Leon, S. A. Schulz, J. Upham, E. Karimi, and R. W. Boyd. Optical spin-to-orbital angular momentum conversion in ultra-thin metasurfaces with arbitrary topological charges. *Applied Physics Letters*, 105(10):101905, 2014.
- [58] F. Bouchard, H. Mand, M. Mirhosseini, E. Karimi, and R. W. Boyd. Achromatic orbital angular momentum generator. *New Journal of Physics*, 16(12):123006, 2014.
- [59] V. Scarani, S. Iblisdir, N. Gisin, and A. Acin. Quantum cloning. *Reviews of Modern Physics*, 77(4):1225, 2005.
- [60] James L Park. The concept of transition in quantum mechanics. *Foundations of Physics*, 1(1):23–33, 1970.
- [61] N. Herbert. Flash—a superluminal communicator based upon a new kind of quantum measurement. *Foundations of Physics*, 12(12):1171–1179, 1982.
- [62] G. C. Ghirardi and T. Weber. Quantum mechanics and faster-than-light communication: methodological considerations. *Il Nuovo Cimento B (1971-1996)*, 78(1):9–20, 1983.

- [63] V. Bužek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Physical Review A*, 54(3):1844, 1996.
- [64] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin. Optimal universal and state-dependent quantum cloning. *Physical Review A*, 57(4):2368, 1998.
- [65] P. Navez and N. J. Cerf. Cloning a real d-dimensional quantum state on the edge of the no-signaling condition. *Physical Review A*, 68(3):032313, 2003.
- [66] F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi. High-dimensional quantum cloning and applications to quantum hacking. *Science Advances*, 3(2):e1601915, Feb 2017.
- [67] V. Giovannetti, S. Lloyd, and L. Maccone. Advances in quantum metrology. *Nature photonics*, 5(4):222, 2011.
- [68] F. Bouchard, P. de la Hoz, G. Björk, R. W. Boyd, M. Grassl, Z. Hradil, E. Karimi, A. B. Klimov, G. Leuchs, J. Řeháček, and et al. Quantum metrology at the limit with extremal majorana constellations. *Optica*, 4(11):1429, Nov 2017.
- [69] J. P. Kirk and A. L. Jones. Phase-only complex-valued spatial filter. *Journal of the Optical Society of America A*, 61(8):1023–1028, 1971.
- [70] E. Bolduc, N. Bent, E. Santamato, E. Karimi, and R. W. Boyd. Exact solution to simultaneous intensity and phase encryption with a single phase-only hologram. *Optics letters*, 38(18):3546–3549, 2013.
- [71] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger. Entanglement of the orbital angular momentum states of photons. *Nature*, 412(6844):313–316, 2001.
- [72] H. Qassim, F. M. Miatto, J. P. Torres, M. J. Padgett, E. Karimi, and R. W. Boyd. Limitations to the determination of a laguerre–gauss spectrum via projective, phase-flattening measurement. *Journal of the Optical Society of America B*, 31(6):A20–A23, 2014.
- [73] J. Leach, M. J. Padgett, S. M. Barnett, S. Franke-Arnold, and J. Courtial. Measuring the orbital angular momentum of a single photon. *Physical Review Letters*, 88(25):257901, 2002.

- [74] G. C. G. Berkhout, M. P. J. Lavery, J. Courtial, M. W. Beijersbergen, and M. J. Padgett. Efficient sorting of orbital angular momentum states of light. *Physical Review Letters*, 105(15):153601, 2010.
- [75] M. P. J. Lavery, D. J. Robertson, G. C. G. Berkhout, G. D. Love, M. J. Padgett, and J. Courtial. Refractive elements for the measurement of the orbital angular momentum of a single photon. *Optics Express*, 20(3):2110–2115, 2012.
- [76] M. Mirhosseini, M. Malik, Z. Shi, and R. W. Boyd. Efficient separation of the orbital angular momentum eigenstates of light. *Nature Communications*, 4:2781, 2013.
- [77] E. Karimi and E. Santamato. Radial coherent and intelligent states of paraxial wave equation. *Optics Letters*, 37(13):2484, Jun 2012.
- [78] E. Karimi, R. W. Boyd, P. de la Hoz, H. de Guise, J. Řeháček, Z. Hradil, A. Aiello, G. Leuchs, and L. L. Sánchez-Soto. Radial quantum number of laguerre-gauss modes. *Physical Review A*, 89(6), 2014.
- [79] E. Karimi, D. Giovannini, E. Bolduc, N. Bent, F. M. Miatto, M. J. Padgett, and R. W. Boyd. Exploring the quantum nature of the radial degree of freedom of a photon via hong-ou-mandel interference. *Physical Review A*, 89(1), 2014.
- [80] R. Fickler, M. Ginoya, and R. W. Boyd. Custom-tailored spatial mode sorting by controlled random scattering. *Physical Review B*, 95(16), 2017.
- [81] Y. Zhou, M. Mirhosseini, D. Fu, J. Zhao, S. M. Hashemi Rafsanjani, A. E. Willner, and R. W. Boyd. Sorting photons by radial quantum number. *Physical Review Letters*, 119(26):263602, 2017.
- [82] X. Gu, M. Krenn, M. Erhard, and A. Zeilinger. Gouy phase radial mode sorter for light: Concepts and experiments. *Physical Review Letters*, 120(10):103601, 2018.
- [83] J. A. Carpenter, N. K. Fontaine, R. Ryf, H. Chen, D. T. Neilson, and K. Kim. Laguerre-gaussian mode sorter. *Complex Light and Optical Forces XIII*, Mar 2019.
- [84] R. Fickler, F. Bouchard, E. Giese, V. Grillo, G. Leuchs, and E. Karimi. Full-field mode sorter using two optimized phase transformations for high-dimensional quantum cryptography. *arXiv preprint arXiv:1905.01175*, 2019.

- [85] F. Bouchard, N. Herrera Valencia, F. Brandt, R. Fickler, M. Huber, and M. Malik. Measuring azimuthal and radial modes of photons. *Optics Express*, 26(24):31925, Nov 2018.
- [86] Z. Hradil. Quantum-state estimation. *Physical Review A*, 55(3):R1561–R1564, 1997.
- [87] C. Schwemmer, L. Knips, D. Richart, H. Weinfurter, T. Moroder, M. Kleinmann, and O. Gühne. Systematic errors in current quantum state tomography tools. *Physical Review Letters*, 114(8):080403, 2015.
- [88] I. L. Chuang and M. A. Nielsen. Prescription for experimental determination of the dynamics of a quantum black box. *Journal of Modern Optics*, 44(11-12):2455–2467, 1997.
- [89] F. Bouchard, F. Hufnagel, D. Koutný, A. Abbas, A. Sit, K. Heshami, R. Fickler, and E. Karimi. Quantum process tomography of a high-dimensional quantum communication channel. *Quantum*, 3:138, 2019.
- [90] H. Bechmann-Pasquinucci and A. Peres. Quantum cryptography with 3-state systems. *Physical Review Letters*, 85(15):3313–3316, 2000.
- [91] M. Bourennane, A. Karlsson, and G. Björk. Quantum key distribution using multilevel encoding. *Physical Review A*, 64(1):012306, 2001.
- [92] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. S. Ribeiro. Quantum key distribution with higher-order alphabets using spatially encoded qudits. *Physical Review Letters*, 96(9), 2006.
- [93] S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger. Experimental quantum cryptography with qutrits. *New Journal of Physics*, 8(5):75–75, 2006.
- [94] I. Ali-Khan, C. J. Broadbent, and J. C. Howell. Large-alphabet quantum key distribution using energy-time entangled bipartite states. *Physical Review Letters*, 98(6):060503, 2007.
- [95] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes. Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Physical Review A*, 88(3):032305, 2013.

- [96] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O’Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd. High-dimensional quantum cryptography with twisted light. *New Journal of Physics*, 17(3):033033, 2015.
- [97] F. Bouchard, A. Sit, K. Heshami, R. Fickler, and E. Karimi. Round-robin differential-phase-shift quantum key distribution with twisted photons. *Physical Review A*, 98(1):010301, 2018.
- [98] F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, and E. Karimi. Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons. *Quantum*, 2:111, 2018.
- [99] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier. Provably secure and high-rate quantum key distribution with time-bin qudits. *Science Advances*, 3(11):e1701491, Nov 2017.
- [100] G. Gibson, J. Courtial, M. J. Padgett, M. Vasnetsov, V. Pas’ko, S. M. Barnett, and S. Franke-Arnold. Free-space information transfer using light beams carrying orbital angular momentum. *Optics Express*, 12(22):5448, 2004.
- [101] Jian Wang, Jeng-Yuan Yang, Irfan M. Fazal, Nisar Ahmed, Yan Yan, Hao Huang, Yongxiong Ren, Yang Yue, Samuel Dolinar, Moshe Tur, and A. E. Willner. Terabit free-space data transmission employing orbital angular momentum multiplexing. *Nature Photonics*, 6(7):488–496, Jun 2012.
- [102] F. Tamburini, E. Mari, A. Sponselli, B. Thidé, A. Bianchini, and F. Romanato. Encoding many channels on the same frequency through radio vorticity: first experimental test. *New Journal of Physics*, 14(3):033001, 2012.
- [103] M. Krenn, R. Fickler, M. Fink, J. Handsteiner, M. Malik, T. Scheidl, R. Ursin, and A. Zeilinger. Communication with spatially modulated light through turbulent air across vienna. *New Journal of Physics*, 16(11):113028, 2014.
- [104] M. Krenn, J. Handsteiner, M. Fink, R. Fickler, R. Ursin, M. Malik, and A. Zeilinger. Twisted light transmission over 143 km. *Proceedings of the National Academy of Sciences*, 113(48):13648–13653, 2016.

- [105] M. P. J. Lavery, C. Peuntinger, K. Günthner, P. Banzer, D. Elser, R. W. Boyd, M. J. Padgett, C. Marquardt, and G. Leuchs. Free-space propagation of high-dimensional structured optical fields in an urban environment. *Science Advances*, 3(10):e1700552, 2017.
- [106] G. Vallone, V. D’Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi. Free-space quantum key distribution by rotation-invariant twisted photons. *Physical Review Letters*, 113(6):060503, 2014.
- [107] M. Krenn, J. Handsteiner, M. Fink, R. Fickler, and A. Zeilinger. Twisted photon entanglement through turbulent air across vienna. *Proceedings of the National Academy of Sciences*, 112(46):14197–14201, 2015.
- [108] P. Shi, S.-C. Zhao, Y.-J. Gu, and W.-D. Li. Channel analysis for single photon underwater free space quantum key distribution. *Journal of the Optical Society of America A*, 32(3):349–356, 2015.
- [109] L. Ji, J. Gao, A.-L. Yang, Z. Feng, X.-F. Lin, Z.-G. Li, and X.-M. Jin. Towards quantum communications in free-space seawater. *Optics Express*, 25(17):19795–19806, 2017.
- [110] C.-Q. Hu, Z.-Q. Yan, J. Gao, Z.-Q. Jiao, Z.-M. Li, W.-G. Shen, Y. Chen, R.-J. Ren, L.-F. Qiao, A.-L. Yang, H. Tang, and X.-M. Jin. Transmission of photonic polarization states through 55-meter water: Towards air-to-sea quantum communication. *arXiv:1811.11176*, 2018.
- [111] S. Zhao, W. Li, Y. Shen, Y. H. Yu, X. H. Han, H. Zeng, M. Cai, T. Qian, S. Wang, Z. Wang, Y. Xiao, and Y. Gu. Experimental investigation of quantum key distribution over water channel. *arXiv:1903.01171*, 2019.
- [112] Y. Chen, W.-G. Shen, Z.-M. Li, C.-Q. Hu, Z.-Q. Yan, Z.-Q. Jiao, J. Gao, M.-M. Cao, K. Sun, and X.-M. Jin. Underwater transmission of high-dimensional twisted photons over 55 meters. *arXiv:1902.01392*, 2019.
- [113] S. Tarantino, D. Cozzolino, K. Rottwitt, and D. Bacco. Feasibility of quantum communications in aquatic scenario. In *2018 IEEE Photonics Conference (IPC)*, pages 1–2. IEEE, 2018.
- [114] B. Guo, G. Yuan, J. Yu, H. Liu, W. Xu, and R. Hou. Simulations and measurements of polarization states changing in underwater laser transmission. In

- Ocean Optics and Information Technology*, volume 10850, page 108500U. International Society for Optics and Photonics, 2018.
- [115] J. Gariano and I. B. Djordjevic. Theoretical study of a submarine to submarine quantum key distribution systems. *Optics Express*, 27(3):3055–3064, 2019.
- [116] P. W. Shor and J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441, 2000.
- [117] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121, 1992.
- [118] L.-M. Duan and G.-C. Guo. Probabilistic cloning and identification of linearly independent quantum states. *Physical Review Letters*, 80(22):4999, 1998.
- [119] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14):3018, 1998.
- [120] B.-G. Englert, D. Kaszlikowski, H. K. Ng, W. K. Chua, J. Řeháček, and J. Anders. Efficient and robust quantum key distribution with minimal state tomography. *arXiv preprint quant-ph/0412075*, 2004.
- [121] V. Scarani, A. Acin, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92(5):057901, 2004.
- [122] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders. Limitations on practical quantum cryptography. *Physical Review Letters*, 85(6):1330, 2000.
- [123] H.-K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94(23):230504, 2005.
- [124] K. Inoue, E. Waks, and Y. Yamamoto. Differential phase shift quantum key distribution. *Physical Review Letters*, 89(3):037902, 2002.
- [125] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden. Fast and simple one-way quantum key distribution. *Applied Physics Letters*, 87(19):194108, 2005.
- [126] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi. Experimental quantum key distribution without monitoring signal disturbance. *Nature Photonics*, 9(12):827, 2015.

- [127] S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han. Experimental demonstration of a quantum key distribution without signal disturbance monitoring. *Nature Photonics*, 9(12):832, 2015.
- [128] Y.-H. Li, Y. Cao, H. Dai, J. Lin, Z. Zhang, W. Chen, Y. Xu, J.-Y. Guan, S.-K. Liao, J. Yin, Q. Zhang, X. Ma, C.-Z. Peng, and J.-W. Pan. Experimental round-robin differential phase-shift quantum key distribution. *Physical Review A*, 93(3):030302, 2016.
- [129] J.-Y. Guan, Z. Cao, Y. Liu, G.-L. Shen-Tu, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Ma, Q. Zhang, and J.-W. Pan. Experimental passive round-robin differential phase-shift quantum key distribution. *Physical Review Letters*, 114(18):180502, 2015.
- [130] H. F. Chau. Quantum key distribution using qudits that each encode one bit of raw key. *Physical Review A*, 92(6):062324, 2015.
- [131] H. F. Chau, Q. Wang, and C. Wong. Experimentally feasible quantum-key-distribution scheme using qubit-like qudits and its comparison with existing qubit-and qudit-based protocols. *Physical Review A*, 95(2):022311, 2017.
- [132] S. Wang, Z.-Q. Yin, H. F. Chau, W. Chen, C. Wang, G.-C. Guo, and Z.-F. Han. Proof-of-principle experimental realization of a qubit-like qudit-based quantum key distribution scheme. *Quantum Science and Technology*, 3(2):025006, 2018.