Quantum Private Broadcasting

Christine Schuknecht

Thesis submitted to the Faculty of Science
in partial fulfillment of the requirements for the degree of
Master of Science Mathematics and Statistics[1]

Department of Mathematics and Statistics
Faculty of Science
University of Ottawa

[1]The M.Sc. program is a joint program with Carleton University, administered by the Ottawa-Carleton Institute of Mathematics and Statistics

Abstract

In *Private Broadcasting*, a single plaintext is *broadcast* to multiple recipients in an encrypted form, such that each recipient can decrypt locally. When the message is classical, a straightforward solution is to encrypt the plaintext with a single key shared among the parties, and to send each recipient a *copy* of the ciphertext. Surprisingly, the analogous method is insufficient in the case where the message is quantum (i.e. in *Quantum Private Broadcasting (QPB)*). In this work, we give three solutions to t-recipient QPB and compare them in terms of encryption key length. We examine *independent* encryption with the quantum one-time pad, unitary t-designs, and a new concept we define as *symmetric unitary t-designs*. Of these three, symmetric t-designs are the best choice when t is large, and these symmetric designs may be of independent interest beyond QPB.

Acknowledgement

I would like to thank my supervisor, Dr. Anne Broadbent, and my quasi-supervisor, Dr. Carlos González-Guillén from Universidad Politécnica de Madrid. These two have provided me with a graduate experience beyond anything I could have imagined, dedicating countless hours to this research work and helping me journey from mathematics to quantum cryptography.

I would like to thank the other members of our research group, who each deserve special mention. Sébastien, Supartha, Rabib, Martti, Raza, Eric, Peter and Sherry; thank you for answering my questions, providing insightful discussions, and keeping me sane throughout this degree. You all impacted my life, for which I will always be grateful.

Thank you to my friends and family for their constant love and support. In particular, thank you to my parents, my siblings, Angela, Trinity, Cindy and Ken, and my roommates who helped bring me out of my cave during this pandemic. I am extremely blessed to have all of you in my life.

Thank you to the University of Ottawa, the Government of Ontario, and the Natural Sciences and Engineering Research Council of Canada for their financial support of this research. Thank you also to the Department of Mathematics and to the Mathematics and Statistics Graduate Student Association for being welcoming and supportive.

Finally, I would like to thank Jesus, Mary and Joseph, who helped me see the light in the darkness, and who are the real reason I made it through this degree.

Contents

List of Figures

List of Tables

List of Symbols

$[d]$	$\{0, \ldots, d-1\}$ integers 17
$\langle \cdot \vert$	Dirac *bra* notation, represents a row vector 6
$\mathbb{C}^d$	Complex space of dimension d 7
$\mathcal{D}(\mathcal{H}_d)$	The set of $d \times d$ density operators in the Hilbert space $\mathcal{H}_d$ 13
$\mathcal{D}(\mathrm{Sym}(d^t))$	Density operators on $\mathrm{Sym}(d^t)$ 17
$\dagger$	Complex conjugate transpose 6
$\delta_{i,j}$	Kronecker delta function 50
$\mathcal{E}_{U_k}^{(t)}(\rho)$	$U_k^{\otimes t} \rho (U_k^\dagger)^{\otimes t}$ for $\rho \in \mathcal{D}(\mathcal{H}_{d^t})$ 42
$\mathcal{H}_d$	Hilbert space of dimension d 7
$\mathcal{H}_M$	Hilbert space of system M 13
$\mathrm{Hom}(\mathcal{U}(d), k, \ell)$	Homogeneous polynomials of degree k, ℓ in U, $U^\dagger$ 37
$\vert \cdot \rangle$	Dirac *ket* notation, represents a column vector 6
$\vert\psi\rangle^{\otimes t}$, $U^{\otimes t}$	t copies of a quantum state or unitary matrix 11
$\vert EPR_\lambda \rangle$	λ number of EPR pairs 15
$\langle \sigma \rangle$	State replacement channel 21
$\mathcal{L}(\mathcal{H}_d)$	The set of linear operators in the Hilbert space $\mathcal{H}_d$ 16
$\mathfrak{U} = (w, \{U_k\}_{k \in K})$	Unitary t-design 37
$\mathsf{dQOTP}_{a,b}$	Double QOTP encryption scheme 33
Enc_k, Dec_k	Encrypting and decrypting maps for key k 21
gQOTP_a	General QOTP encryption scheme for key $a \in [d^2]$ 30
$\mathsf{QOTP}_{a,b}$	QOTP encryption scheme for keys $a, b \in \{0,1\}$ 23
$\otimes$	Tensor product 10
$\mathcal{P} = \{\mathbb{1}, X, Y, Z\}$	Set of 2-dimensional Pauli matrices 8
Π_b	Projectors into subspaces orthogonal to $\mathrm{Sym}(d^t)$ 18
Π_{Sym}	Projector into $\mathrm{Sym}(d^t)$ 18
ρ	Density operator 12
ρ_{ME}	Density operator composed of two systems M and E 13
$\mathrm{Sym}(d^t)$	Symmetric subspace over $(\mathcal{H}_d)^{\otimes t}$ 17
τ_b	Normalized Π_b 18
τ_{Sym}	Normalized projector into $\mathrm{Sym}(d^t)$ 18
Tr	Trace of a matrix 12
$\mathcal{U}(\mathrm{Sym}(d^t))$	The set of $d_{\mathrm{Sym}} \times d_{\mathrm{Sym}}$ unitaries from $\mathrm{Sym}(d^t) \otimes \mathrm{Sym}(d^t)$ 17

$\mathcal{U}(d)$	Unitary group of all $d \times d$ unitary matrices from $\mathcal{H}_d \otimes \mathcal{H}_d$ 8
$\{\|0\rangle, \|1\rangle\}$	Computational basis 7
$D(d, k, \ell)$	Dimension of $\mathrm{Hom}(\mathcal{U}(d), k, \ell)$ 43
d_{Sym}	Dimension of $\mathrm{Sym}(d^t)$ 17
F	SWAP operator 53
H	Hadamard matrix 8
M_m	Projective measurement operator for outcome m 9
$P_{\vee^2(2)}$	Projector into the antisymmetric subspace of $\mathcal{H}_{2^2}$ 53
$P_{\wedge^2(2)}$	Projector into the symmetric subspace of $\mathcal{H}_{2^2}$ 53
$S(\cdot)$	von Neuman entropy 65
S_t	Symmetric (permutation) group of t elements 17
t-PB	t-recipient Private Broadcasting 19
t-QPB	t-recipient Quantum Private Broadcasting 20
$T^{(t)}$	t-twirling channel, $\int_{\mathcal{U}(d)} U^{\otimes t} \rho (U^\dagger)^{\otimes t} dU$ for $\rho \in \mathcal{D}(\mathcal{H}_{d^t})$ 42
U	Unitary matrix of size $d \times d$ unless specified otherwise 8
$w : \{U_k\}_{k \in K} \to \mathbb{R}$	Positive weight function for unitaries U_k 37
OTP	One-Time Pad 19
QOTP	Quantum One-Time Pad 23

Chapter 1

Introduction

1.1 Encryption Schemes

For hundreds of years, there has been highly sensitive information that needs to be shared between two or more individuals in different locations. Common examples include attack strategies in active combat, information acquired by espionage agents, and locations for dealings of a highly lucrative nature. Such information is dangerous in the wrong hands, and therefore strategies to conceal information sent between parties are of extreme importance. These are otherwise known as encryption schemes, the strength of which varies depending on the underlying composition of these schemes. Encryption schemes are classified into *private key* or *public key* encryption schemes, where the encryption key is either kept hidden or is made publicly available. One common public key encryption scheme is RSA [RSA78], which relies on the difficulty of factoring the product of two large prime numbers. This scheme is widely used for the encryption of many web sites, including online banking and shopping sites. Therefore, if the factoring of the product of prime numbers can be solved quickly, this has disastrous results across the world wide web.

It has been shown that *quantum computers* are able to solve this factoring problem and are therefore able to break certain public key encryption schemes [Sho94]. The question now becomes: how can encryption schemes exist which are still secure in the presence of a quantum computer? There are two schools of thought with regards to this problem. The first is to use quantum computers within the encryption itself, and therefore create new schemes which are quantum-safe. This is called *quantum encryption*, which is a specific instance of *quantum cryptography*. In this thesis, quantum cryptography is defined to be where both the sender and the receiver have access to a quantum computer, and are therefore capable of performing cryptographic tasks that require quantum mechanics. The second option is to try and find other hard math problems which are not completely broken with the emergence of quantum computers. This is what is called *post-quantum encryption*. The National Institute

of Standard and Technology in the United States have been working on testing and approving proposed encryption schemes that meet their standards of security to both quantum and classical computers, a process that is currently in its third round of candidates [CSD].

1.2 Private Broadcasting

This thesis focuses on quantum encryption, and specifically the problem where multiple copies of an encrypted message (called the ciphertext) are sent to different individuals. To contextualize such a problem, consider the following fictional scenario.

> You are on your way home from work when you witness a crime being committed in one of the back alleys between your office and the subway. You recognize the culprit and you see them murder another man in cold blood. Moving as quietly as a mouse, you slip away and head to the police to report what you saw. The police are able to capture the guilty party, whom you positively identify. You head home, exhausted now that the rollercoaster of adrenaline has worn off. A few days later, you get called back to the police station, where they tell you that they need you to testify at the murder trial. It turns out there is not enough physical evidence to link the murderer to the crime, and you have now become the key witness in this trial. Unfortunately for you, the guilty man is related to the leader of one of the rival gangs in your city. They do not take kindly to snitches, which you discover when you get home and see this note slipped under your door:
>
> ```
> If you testify, you will find yourself looking at the bottom of
> a 6 foot hole sooner than you expect.
> ```
>
> To keep you safe, you and your family are put into witness protection and are relocated to another part of the country. When it is time for you to testify, the prosecutor's office will send the same message to the authorities both in your old city and your new city, as well as the members of your protection detail, giving them all the same message. To keep this message secure, it is encrypted and sent to the above parties. Since the intended recipients are in different parts of the country, it must be possible for each of them to independently decrypt the message once it is received.

This is the problem examined in this thesis, where there is a message (known as the plaintext) being sent to t different people, possibly in different parts of the world, who all need to decrypt this message on their own. This is what we call the *t-recipient private broadcasting problem*.

This problem causes no issues with classical encryption, as one can use the same encryption key for each copy of the plaintext message, and each ciphertext remains independent of the original plaintext. This implies that an adversary who intercepts the ciphertext receives no information about the plaintext. If this plaintext is instead a pure quantum state $|\varphi\rangle\langle\varphi|$ and is encrypted using a unitary matrix U, it is no longer true in general that encrypting multiple copies with the same key outputs ciphertexts which are independent of the original plaintext. The encryption key in this case is a sequence of classical bits that specifies which unitary is used for the encryption from a finite subset of possible unitaries. The problem where one desires to securely encrypt t copies of a pure quantum state is what we call the *t-recipient quantum private broadcasting problem (t-QPB)*, and we examine this problem through the lens of the encryption key, which is described by classical bits. The longer the encryption key, the more storage space is needed for the key, and generating a truly random key is expensive. Therefore, a small encryption key is desirable, and we consider three possible solutions to this t-QPB problem in terms of their key length.

The first is the quantum one-time pad (QOTP), which is a perfectly secure quantum encryption scheme when used once. We show that this scheme is no longer perfectly secure when the same encryption key is used to encrypt two copies of the same quantum state. This is the quantum encryption scheme mentioned in the previous paragraph, and since it is not secure for two copies, one is unable to claim security for general t. This setback is resolved instead by using independent keys for each copy of the plaintext that is to be sent. This results in a key length that increases linearly with respect to t, the number of copies. The question then becomes whether we can improve this key length so as to accomplish t-QPB with the same level of security as the QOTP but with less classical bits. This leads us to examining unitary t-designs, resulting in two other solutions to this t-QPB problem.

The second solution uses unitary t-designs as encryption schemes. Unitary t-designs are composed of a finite set of unitary matrices, along with a probability distribution that specifies the probability each matrix is chosen from this set. These unitary t-designs have the property that applying a matrix from this finite set, up to t times to a quantum state, appears the same as applying a Haar-random unitary matrix. A Haar-random unitary can be thought of as a uniformly random matrix from the whole group of unitaries, but it is inefficient to generate these matrices as the amount of resources (i.e. quantum gates) increases exponentially with the number of quantum states [DCEL09]. These unitary t-designs are useful because with only a finite number of matrices, one is able to obtain a matrix that appears randomly chosen from infinitely many unitary matrices. Using the upper bounds on the number of unitaries needed for a unitary t-design, the key length for these design encryption schemes increases logarithmically with respect to t.

Lastly, we propose a new concept of *symmetric unitary t-designs*, which are a relaxation of unitary t-designs acting on the symmetric subspace. In contrast to unitary

t-designs, the input quantum state must be an element of the symmetric subspace. We use these symmetric unitary t-designs as encryption schemes, and the unitary bounds are now with respect to the dimension of the symmetric subspace, which we denote as d_{Sym}. The key length increases logarithmically with respect to d_{Sym}, which corresponds to increasing logarithmically with respect to t. Figure 1.1 compares the key lengths of the quantum one-time pad, unitary t-designs, and symmetric unitary t-designs when the dimension is fixed at 2 and t is increased. As t increases, this key length is smallest with symmetric unitary t-designs as opposed to regular unitary t-designs or to the quantum one-time pad.

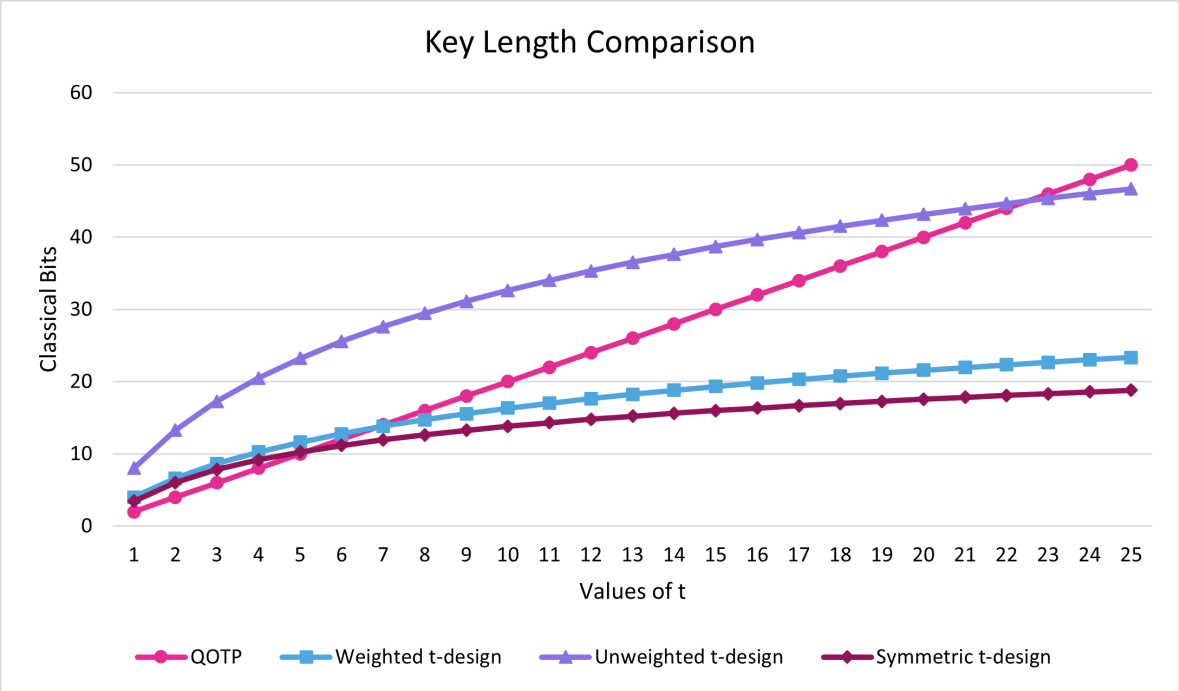

Figure 1.1: QOTP, Weighted t-design, Symmetric t-design, $t \leq 25$, $d = 2$

1.3 Structure

The rest of this thesis is organized as follows. Chapter 2 covers background information regarding quantum computing that is needed for the subsequent chapters. Chapter 3 formally defines this t-QPB problem along with its corresponding security properties. Chapter 4 introduces the quantum one-time pad and examines the key length bounds when used for t-QPB. Chapter 5 defines unitary t-designs, their bounds, and how they can be used as encryption schemes for t-QPB. Chapter 6 presents symmetric unitary t-designs and their corresponding bounds, how they are

used as encryption schemes, and ending with a comparison of all three solutions to the t-QPB problem. Chapter 7 discusses open problems and further work. Appendix A contains the Python code used for the trace distance calculations throughout this thesis, and Appendix B contains the data for each of the figures. We note that the main results of this thesis have been posted as a pre-print [BGGS21]. In particular, Section 4.3, Section 5.4, Chapter 6, and the open problems presented in Chapter 7 closely follow [BGGS21].

Chapter 2

Preliminaries

In this chapter we present background information in quantum computing, providing the reader with sufficient knowledge in order to understand the mathematical notation and concepts used throughout this thesis. In particular, we explain the four postulates of quantum mechanics, providing examples throughout to illustrate these phenomena. Next, we explain density operators, entanglement and Schmidt decomposition, before discussing concepts specific to our t-recipient quantum private broadcasting. These include the Haar measure, the specific norms we use, a brief introduction to the symmetric subspace and results from representation theory and convex analysis. Section 2.8, Section 2.9 and Section 2.10 closely follow the preliminary section of [BGGS21].

2.1 Bits and Qubits

In classical computing, the behaviour of the computing systems is described by bits, 0 and 1, and strings of bits $\{0,1\}^n$. In quantum computing, these bits are no longer sufficient, and instead quantum systems are needed. Quantum bits, or *qubits*, are *two*-dimensional quantum systems while *qudits* are d-dimensional quantum systems. These quantum systems can be characterized as *pure* or *mixed* systems, where a pure qubit is written as a two dimensional complex vector. Mixed qubits are written as matrices, specifically density matrices, which are explained later. The common notation used for quantum systems is the Dirac (bra-ket) notation, which we use in this thesis. This notation is comprised of 'kets' and 'bras', where a ket is written as $|\cdot\rangle$ and represents a column vector. A row vector is represented by a bra, written as $\langle\cdot|$. Kets and bras are complex conjugate transposes of each other, i.e. $|\psi\rangle^\dagger = \langle\psi|$ where the conjugate transpose is denoted as $\dagger$. For example, one common qubit is $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$, and $\langle 0| = [1\ 0]$. These kets and bras can be combined as $\langle\phi|\psi\rangle$ and $|\psi\rangle\langle\phi|$, called the *inner product* and *outer product*, respectively. The inner product results in a scalar,

while the outer product results in a matrix. If two vectors $|\phi\rangle$ and $|\psi\rangle$ are orthogonal, this means their inner product is zero, which is equivalent to saying $\langle\phi|\psi\rangle = 0$. The *norm* of a vector $|\phi\rangle$ is $|| \, |\phi\rangle \, || = \sqrt{\langle\phi|\phi\rangle}$, which means $|| \, |\phi\rangle \, ||^2 = \langle\phi|\phi\rangle$ and $|\phi\rangle$ is a unit vector if $\langle\phi|\phi\rangle = 1$.

There are certain conditions that need to hold for a vector to be a valid qubit, along with other rules about how quantum systems can be described, how they evolve, are measured, and are combined with other quantum systems. To explain this phenomena, we follow the postulates of quantum mechanics as described by Nielsen and Chuang in [NC10].

2.2 Postulates of Quantum Mechanics

Postulate 1. Associated to any isolated physical system is a complex vector space with inner product (that is, a *Hilbert* space known as the *state space* of the system). The system is completely described by its *state vector*, which is a unit vector in the system's state space.

As previously mentioned, a qubit is a 2-dimensional system. Its state space is therefore $\mathbb{C}^2$ with inner product and is described by unit vectors in this Hilbert space. We denote $\mathcal{H}_d$ as the Hilbert space of dimension d throughout this thesis, and the unit vectors in this Hilbert space are called quantum states. We are only concerned with d being finite, and therefore use $\mathbb{C}^d$ and $\mathcal{H}_d$ interchangeably. Examples of two quantum states in $\mathcal{H}_2$ are $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ and $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$, which are also orthogonal and therefore form a basis for $\mathcal{H}_2$. This basis $\{|0\rangle, |1\rangle\}$ is called the *computational basis*, and any arbitrary qubit can be written as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, i.e. as a linear combination of the basis states. Since $|\psi\rangle$ is a unit vector, this means that it must be true that

$$\begin{aligned} \langle\psi|\psi\rangle &= \Big(\alpha^* \langle 0| + \beta^* \langle 1|\Big)\Big(\alpha|0\rangle + \beta|1\rangle\Big) \\ 1 &= \alpha^*\alpha \langle 0|0\rangle \, \alpha^*\beta \langle 0|1\rangle + \beta^*\alpha \langle 1|0\rangle + \beta^*\beta \langle 1|1\rangle \\ &= |\alpha|^2 + |\beta|^2, \end{aligned} \tag{2.2.1}$$

where α^* and β^* are the complex conjugates of α and β.

Postulate 2. The evolution of a closed quantum system is described by a *unitary transformation*. That is, the state $|\psi\rangle$ of the system t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle. \tag{2.2.2}$$

This means that to transform one quantum state to another, this is done by a unitary operator. A unitary operator (i.e. a unitary matrix) is a square matrix such that $UU^\dagger = \mathbb{1}$. The group of all $d \times d$ unitary matrices is the *unitary group*, which we denote as $\mathcal{U}(d)$. Four common unitary operators in $\mathcal{U}(2)$ are the identity and the Pauli X, Y and Z:

$$\mathbb{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.2.3}$$

The identity operator naturally changes nothing when applied to any qubit. The Pauli X, also called the NOT operator, acts as $X(\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha\,|1\rangle + \beta\,|0\rangle$. The Pauli Z changes the sign of β when applied to $\alpha\,|0\rangle + \beta\,|1\rangle$, and $Y = -iXZ$. A *Hermitian* matrix is a square matrix M such that $M = M^\dagger$. It is easy to see that $U = U^\dagger$ for $U \in \mathcal{P} = \{\mathbb{1}, X, Y, Z\}$, which implies that the Pauli operators are also Hermitian matrices.

Another unitary operator is the *Hadamard*,

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{2.2.4}$$

When the Hadamard is applied to the computational basis states, this gives two other orthogonal quantum states, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Postulate 3. Quantum measurements are described by a collection $\{M_m\}$ of *measurement operators*. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement, then the probability that result m occurs is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle\,, \tag{2.2.5}$$

and the state of the system after the measurement is

$$\frac{M_m\,|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}. \tag{2.2.6}$$

The measurement operators satisfy the *completeness equation*,

$$\sum_m M_m^\dagger M_m = \mathbb{1}. \tag{2.2.7}$$

The completeness equation expresses the fact that the probabilities sum to one:

$$1 = \sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle\,. \tag{2.2.8}$$

This postulate says that when a measurement is performed to a quantum state, the outcome is a purely classical result, this index m, where each classical result occurs with a certain probability. The quantum state 'collapses' to this classical result, along with a post-measurement quantum state, and it is not possible to go back and reconstruct the original quantum state once it has been measured. For this reason, quantum states are measured at the end of any manipulations that are performed.

Example 2.2.1. One example of a collection of measurement operators are $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$, which are operators on $\mathcal{H}_2$ and satisfy the completeness equation. Applying each of these operators to an arbitrary qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ gives

$$\begin{aligned} M_0|\psi\rangle &= |0\rangle\langle 0|\Big(\alpha|0\rangle + \beta|1\rangle\Big) \\ &= \alpha|0\rangle\langle 0|0\rangle + \beta|0\rangle\langle 0|1\rangle \\ &= \alpha|0\rangle, \end{aligned} \tag{2.2.9}$$

$$\begin{aligned} M_1|\psi\rangle &= \alpha|1\rangle\langle 1|0\rangle + \beta|1\rangle\langle 1|1\rangle \\ &= \beta|1\rangle, \end{aligned}$$

since $\langle 0|0\rangle = \langle 1|1\rangle = 1$ and $\langle 0|1\rangle = \langle 1|0\rangle = 0$.

Now measuring $|\psi\rangle$ gives

$$\begin{aligned} p(0) &= \langle\psi|M_0^\dagger M_0|\psi\rangle \\ &= \langle 0|\alpha^*\alpha|0\rangle \\ &= |\alpha|^2\langle 0|0\rangle \\ &= |\alpha|^2, \end{aligned} \tag{2.2.10}$$

$$\begin{aligned} p(1) &= \langle\psi|M_1^\dagger M_1|\psi\rangle \\ &= |\beta|^2, \end{aligned}$$

with the post-measurement states being

$$\begin{aligned} \frac{M_0|\psi\rangle}{\sqrt{\langle\psi|M_0^\dagger M_0|\psi\rangle}} &= \frac{\alpha}{|\alpha|}|0\rangle \\ \frac{M_1|\psi\rangle}{\sqrt{\langle\psi|M_1^\dagger M_1|\psi\rangle}} &= \frac{\beta}{|\beta|}|1\rangle. \end{aligned} \tag{2.2.11}$$

This is known as the computational basis measurement, where 0 occurs with probability $|\alpha|^2$ and 1 occurs with probability $|\beta|^2$. As seen in the post-measurement

states, they have each collapsed to either $\frac{\alpha}{|\alpha|}|0\rangle$ or $\frac{\beta}{|\beta|}|1\rangle$, and there is no indication that the original state was $\alpha|0\rangle + \beta|1\rangle$. Therefore, this original quantum state is lost after measuring and cannot be reconstructed.

Another type of measurements as described in [NC10] are *projective measurements*. These are defined exactly the same as in Postulate 3, now with the added restriction that the measurement operators M_m are Hermitian operators and orthogonal to each other. This means that when multiplied together, the matrix product $M_m M_n$ yields the zero matrix except when $m = n$. Therefore, for a measurement $\{M_m\}$ to be classified as a projective measurement, it must be true that $M_m^\dagger = M_m$ and $M_m M_n = 0$ when $m \neq n$. These conditions hold for $\{M_0, M_1\}$ in Example 2.2.1, which implies that $\{M_0, M_1\}$ is a projective measurement.

Recalling that $\langle\psi|\psi\rangle = ||\,|\psi\rangle\,||^2$ and assuming $\{M_m\}$ is a projective measurement, the probability that result m occurs can be simplified in the following manner,

$$\begin{aligned} p(m) &= \langle\psi|M_m^\dagger M_m|\psi\rangle \\ &= \langle\psi|M_m M_m|\psi\rangle \\ &= ||M_m\,|\psi\rangle\,||^2. \end{aligned} \tag{2.2.12}$$

This simplification is precisely what is used in the probability calculations in Example 2.2.1.

Postulate 4. The state space of a composite physical system is the *tensor product* of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

In order to understand this postulate, we must first understand what is meant by the tensor product, denoted as $\otimes$. We use the explanations of Nielsen and Chuang in [NC10] to explicitly define the tensor product, which is interchangeably called the *Kronecker product*, along with what it means to have tensor products of Hilbert spaces and quantum states, and the basic properties of the tensor product.

Definition 2.2.2 (Kronecker Product)**.** Suppose A is an $m \times n$ matrix and B is

a $p \times q$ matrix. The Kronecker product between A and B is defined as

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{bmatrix}$$

$$= \begin{bmatrix} A_{11}B_{11} & \cdots & A_{11}B_{1q} & A_{12}B_{11} & \cdots & A_{12}B_{1q} & \cdots & A_{1n}B_{11} & \cdots & A_{1n}B_{1q} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \dots & \vdots & \ddots & \vdots \\ A_{11}B_{p1} & \cdots & A_{11}B_{pq} & A_{12}B_{p1} & \cdots & A_{12}B_{pq} & \cdots & A_{1n}B_{p1} & \cdots & A_{1n}B_{pq} \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ A_{m1}B_{11} & \cdots & A_{m1}B_{1q} & A_{m2}B_{11} & \cdots & A_{m2}B_{1q} & \cdots & A_{mn}B_{11} & \cdots & A_{mn}B_{1q} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \dots & \vdots & \ddots & \vdots \\ A_{m1}B_{p1} & \cdots & A_{m1}B_{pq} & A_{m2}B_{p1} & \cdots & A_{m2}B_{pq} & \cdots & A_{mn}B_{p1} & \cdots & A_{mn}B_{pq} \end{bmatrix} \tag{2.2.13}$$

where $A \otimes B$ is an $nq \times mp$ matrix. To illustrate this further, a simple example is the tensor product of $|0\rangle$ and $|1\rangle$:

$$|0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \cdot 0 \\ 1 \cdot 1 \\ 0 \cdot 0 \\ 0 \cdot 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}. \tag{2.2.14}$$

When considering Hilbert spaces V and W of dimension m and n respectively, these Hilbert spaces can be combined with linear combinations of such tensor product to obtain $W' = V \otimes W$, which has dimension mn. The elements of W' are of the form $|v\rangle \otimes |w\rangle$, where $|v\rangle \in V$ and $|w\rangle \in W$. Furthermore, if $\{|i_1\rangle, \dots, |i_m\rangle\}$ and $\{|j_1\rangle, \dots, |j_n\rangle\}$ are bases for V and W respectively, then $\{|i_k\rangle \otimes |j_\ell\rangle\}$ for $k \in [1, m]$, $\ell \in [1, n]$ is a basis for W'. If A is a linear operator on V and B is a linear operator on W, then $A \otimes B$ is a linear operator on W'. The tensor product of quantum states is written interchangeably in this thesis as $|\phi\rangle \otimes |\psi\rangle = |\phi\psi\rangle = |\phi\rangle |\psi\rangle$. The notation $|\psi\rangle^{\otimes t}$ represents $\underbrace{|\psi\rangle \otimes |\psi\rangle \cdots \otimes |\psi\rangle}_{t \text{ times}}$.

The basic properties of tensor products are the following:

1. For an arbitrary scalar z and elements $|v\rangle$ of V and $|w\rangle$ of W,

$$z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle). \tag{2.2.15}$$

2. For arbitrary $|v_1\rangle$ and $|v_2\rangle$ in V and $|w\rangle$ in W,

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle. \tag{2.2.16}$$

3. For arbitrary $|v\rangle$ in V and $|w_1\rangle$ and $|w_2\rangle$ in W,

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle . \tag{2.2.17}$$

2.3 Density Operators

Pure quantum states are written as unit complex vectors, or equivalently, a quantum state is pure if it can be written as a $|\psi\rangle$ whose norm is 1. Are all quantum states pure? No. There are also mixed states that are written using density operators, which we explain along the same lines as [NC10]. It is possible that a quantum system is an ensemble of quantum states, each with a certain probability. For example, if one were to toss a coin and have $|0\rangle$ and $|1\rangle$ represent heads and tails, respectively, the quantum system describing the outcome of this coin toss is $|0\rangle$ with probability $1/2$ and $|1\rangle$ with probability $1/2$. This is an example of a mixed state because the resulting quantum system is either $|0\rangle$ or $|1\rangle$. Formally, let $|\psi_i\rangle$ be quantum states with probability p_i for index i, and suppose a quantum system is in one of these states with the associated probability. The *density operator* of this system is defined as

$$\rho = \sum_i p_i \, |\psi_i\rangle\langle\psi_i| . \tag{2.3.1}$$

Density operators (also called density matrices) must satisfy two conditions; they must have trace equal to 1, and they must be positive operators. The *trace* of a matrix is the sum of the diagonal entries. For example,

$$\mathrm{Tr}\left(\begin{bmatrix} 1 & 3 & 4 \\ 0 & 2 & 7 \\ 6 & 9 & 5 \end{bmatrix}\right) = 1 + 2 + 5 = 8. \tag{2.3.2}$$

The trace is a valid linear operation, and by its cyclic property, it is true that $\langle\psi|A|\psi\rangle = \mathrm{Tr}(A\,|\psi\rangle\langle\psi|)$ for linear operator A and quantum state $|\psi\rangle$. An operator ρ is considered *positive* if for an arbitrary quantum state $|\phi\rangle$, it is true that $\langle\phi|\rho|\phi\rangle \geq 0$.

To transform one quantum state into another, this is done by applying a unitary matrix U, as explained in Postulate 2. For density operators, this becomes

$$\sum_i p_i U \, |\psi_i\rangle\langle\psi_i| \, U^\dagger = U\rho U^\dagger. \tag{2.3.3}$$

Measurements of quantum states written with density operators are similar to as explained in Postulate 3. Using the fact that $\langle\psi|A|\psi\rangle = \mathrm{Tr}(A\,|\psi\rangle\langle\psi|)$, the probability of outcome m is

$$p(m) = \mathrm{Tr}\big(M_m^\dagger M_m \rho\big). \tag{2.3.4}$$

With regards to notation, in this thesis we use both kets and density operators to represent quantum states. The set of $d \times d$ density operators in the Hilbert space $\mathcal{H}_d$ is denoted as $\mathcal{D}(\mathcal{H}_d)$.

From Postulate 4, a total state space can be composed of other state spaces through the tensor product. One such example is a quantum state ρ that is an element of $\mathcal{H}_2 \otimes \mathcal{H}_2$, where we denote the first Hilbert space as system M and the second Hilbert space as system E. Such a ρ is written as ρ_{ME} to illustrate that the total state space is composed of two distinct systems. It is possible to look at just one of these two systems, and to do so is called taking the *partial trace* of ρ_{ME}. Tracing out the system M is denoted as $\mathrm{Tr}_M(\rho_{ME}) = \rho_E$, and this operation is equivalent to applying the trace to the part of ρ from system M and applying the identity to the part from system E. To make this concept concrete, consider the following example.

Example 2.3.1. Suppose we have the quantum state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, which corresponds to the following density operator

$$\begin{aligned}\rho_{ME} &= \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)\left(\frac{1}{\sqrt{2}}(\langle 00| + \langle 11|)\right) \\ &= \frac{1}{2}\Big(\,|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|\,\Big),\end{aligned} \tag{2.3.5}$$

where the first qubit is from system M and the second qubit is from system E. Tracing out system M gives

$$\begin{aligned}\mathrm{Tr}_M(\rho_{ME}) &= (\mathrm{Tr} \otimes \mathbb{1})\frac{1}{2}\Big(\,|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|\,\Big) \\ &= \frac{1}{2}\Big(\,\mathrm{Tr}(|0\rangle\langle 0|) \otimes |0\rangle\langle 0| + \mathrm{Tr}(|0\rangle\langle 1|) \otimes |0\rangle\langle 1| + \mathrm{Tr}(|1\rangle\langle 0|) \otimes |1\rangle\langle 0| + \mathrm{Tr}(|1\rangle\langle 1|) \otimes |1\rangle\langle 1|\,\Big) \\ &= \frac{1}{2}\Big(\,\langle 0|0\rangle \otimes |0\rangle\langle 0| + \langle 0|1\rangle \otimes |0\rangle\langle 1| + \langle 1|0\rangle \otimes |1\rangle\langle 0| + \langle 1|1\rangle \otimes |1\rangle\langle 1| \\ &= \frac{1}{2}\Big(\,|0\rangle\langle 0| + |1\rangle\langle 1|\,\Big).\end{aligned} \tag{2.3.6}$$

2.4 Bases

In this thesis, we use the common fact about the Pauli operators, which says that $\mathcal{P} = \{\mathbb{1}, X, Y, Z\}$ forms a basis for all linear operators in $\mathbb{C}^2$, and that

$$\mathcal{P}^{\otimes n} = \{P_1 \otimes P_2 \otimes \cdots \otimes P_n | P_i \in \mathcal{P}\} \tag{2.4.1}$$

forms a basis for all linear operators of $(\mathbb{C}^2)^{\otimes n}$ [BR03]. The Paulis therefore form a basis for $\mathcal{H}_{2^n}$. The set of n qubit density operators are a subset of all linear operators of $(\mathbb{C}^2)^{\otimes n}$, which implies that any n qubit density operator ρ can be written as

$$\rho = \sum_{P \in \mathcal{P}^{\otimes n}} c_P \cdot P, \quad c_P \in \mathbb{C}\,. \tag{2.4.2}$$

2.5 Entanglement

Another classification of quantum states is whether they are separable or entangled. A quantum state $|\varphi\rangle$ from the Hilbert space $W' = V \otimes W$ is called *separable* if it can be written as a tensor product $|\varphi\rangle = |\phi\rangle \otimes |\psi\rangle$, where $|\phi\rangle$ and $|\psi\rangle$ are pure states in V and W, respectively. If $|\varphi\rangle$ cannot be written this way, it is called *entangled*. Examples of entangled states of two qubits are what are known as the *Bell states*,

$$\begin{aligned}
\left|\Phi^+\right\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \\
\left|\Phi^-\right\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) \\
\left|\Psi^+\right\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \\
\left|\Psi^-\right\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right).
\end{aligned} \tag{2.5.1}$$

The state $|\Phi^+\rangle$ is also known as an EPR pair, and is described as having two 'halves'. It has the property that if a measurement is made to one of the halves, both halves end in the same post-measurement state, which we illustrate with an example.

Example 2.5.1. Suppose a computational basis measurement is made to the first half of $|\Phi^+\rangle$, where we label the first half as being from some system A and the second half is from system B. This corresponds to a projective measurement with $\{M_0 = |0_A\rangle\langle 0_A| \otimes \mathbb{1}_B, M_1 = |1_A\rangle\langle 1_A| \otimes \mathbb{1}_B\}$. This results in

$$\begin{aligned}
|0_A\rangle\langle 0_A| \otimes \mathbb{1}_B\Big(\frac{1}{\sqrt{2}}\left(|0_A 0_B\rangle + |1_A 1_B\rangle\right)\Big) &= \frac{1}{\sqrt{2}}\Big(|0_A\rangle\langle 0_A|\,|0_A\rangle \otimes |0_B\rangle + |0_A\rangle\langle 0_A|\,|1_A\rangle \otimes |1_B\rangle\Big) \\
&= \frac{1}{\sqrt{2}}|0_A 0_B\rangle \\
|1_A\rangle\langle 1_A| \otimes \mathbb{1}_B\Big(\frac{1}{\sqrt{2}}\left(|0_A 0_B\rangle + |1_A 1_B\rangle\right)\Big) &= \frac{1}{\sqrt{2}}\Big(|1_A\rangle\langle 1_A|\,|0_A\rangle \otimes |0_B\rangle + |1_A\rangle\langle 1_A|\,|1_A\rangle \otimes |1_B\rangle\Big) \\
&= \frac{1}{\sqrt{2}}|1_A 1_B\rangle\,,
\end{aligned} \tag{2.5.2}$$

which has $p(0) = \frac{1}{2}$ with post measurement state $|0_A 0_B\rangle$ and $p(1) = \frac{1}{2}$ with post measurement state $|1_A 1_B\rangle$. Notice how the identity was applied to the second half of the EPR pair, but it still collapsed to the same quantum state as the first half after measuring.

Our results later in this thesis make use of two EPR pairs, and it is helpful to define λ number of EPR pairs as

$$|EPR_\lambda\rangle = \frac{1}{\sqrt{2^\lambda}} \sum_{q\in\{0,1\}^\lambda} |q\rangle\,|q\rangle\,, \tag{2.5.3}$$

where $\lambda \in \mathbb{N}$. This is simply re-ordering the middle qubits so that the first $|q\rangle$ in the above equation describes the first half of the λ EPR pairs and the second $|q\rangle$ describes the second half of the λ EPR pairs.

2.6 Schmidt Decomposition

The Schmidt decomposition is defined as follows, from [NC10].

Theorem 2.6.1 (Schmidt decomposition)**.** *Suppose $|\psi\rangle$ is a pure state of a composite system AB. There then exists orthonormal states $|i_A\rangle$ for system A, and orthonormal states $|i_B\rangle$ of system B such that*

$$|\psi\rangle = \sum_i \lambda_i\,|i_A\rangle\,|i_B\rangle\,, \tag{2.6.1}$$

where λ_i are non-negative real numbers satisfying $\sum_i \lambda_i^2 = 1$ known as Schmidt coefficients.

This result is useful for pure quantum states ρ_{ME} where this system E is an auxiliary space that may or may not be entangled with the message space M. Quantum encryption schemes need to consider this possible entanglement, and the Schmidt decomposition is a tool we use to prove the security of two of our encryption schemes.

2.7 Haar measure

As explained in [Wat15], the *Haar measure* is a probability measure over the set of unitary operators. It is invariant to left and right multiplication of unitary matrices, which means that $\int_{\mathcal{U}(d)} AU\ dU = \int_{\mathcal{U}(d)} UA\ dU = \int_{\mathcal{U}(d)} U\ dU$, where the integral is with respect to the Haar measure, for $A, U \in \mathcal{U}(d)$, the group of $d \times d$ unitary matrices.

The Haar measure over the unitary group is a probability measure that plays the role of uniform randomness, and a unitary matrix chosen with the Haar measure is called a *Haar-random matrix*. However, in practice, generating Haar-random unitaries is expensive with respect to time and resources. Therefore, unitary matrices that appear Haar-random but are from a much smaller, finite set of unitaries, are an ideal choice if one needs a Haar-random unitary. This property is precisely the definition of a unitary t-design, which we explain in Chapter 5. Our usage of the Haar measure is limited to the context of integrals. Throughout this thesis, when we have integrals taken over the whole unitary group $\mathcal{U}(d)$, these are taken with respect to the Haar measure. An example of such an integral is

$$\int_{\mathcal{U}(d)} U^{\otimes t} \rho (U^\dagger)^{\otimes t} dU,$$

where $U \in \mathcal{U}(d)$ and $\rho \in \mathcal{D}(\mathcal{H}_d^{\otimes t})$. Since the Haar measure is invariant to left and right multiplication, the following equation is also true, for $V \in \mathcal{U}(d)$,

$$\int_{\mathcal{U}(d)} U^{\otimes t} \rho (U^\dagger)^{\otimes t} dU = \int_{\mathcal{U}(d)} (UV)^{\otimes t} \rho ((UV)^\dagger)^{\otimes t} dU$$

Curious readers can find more about the technical definitions and usages of the Haar measure in [Wat15].

2.8 Norms and Distance

Transformations between quantum states are formalized by quantum channels, that is, completely positive trace preserving maps. Determining the distinguishability of the outputs from two such channels $\Psi, \Phi : \mathcal{L}(\mathcal{H}_M) \to \mathcal{L}(\mathcal{H}_M)$ is done with the *trace norm* $||\cdot||_1$, where $||A||_1 = \mathrm{Tr}\left(\sqrt{AA^\dagger}\right)$ for linear operator A and $\mathcal{L}(\mathcal{H}_M)$ denotes the set of linear operators in $\mathcal{H}_M$. This trace norm is the sum of the singular values of A, while the infinity norm $||\cdot||_\infty$ is the maximum singular value. The quantum channels themselves are compared with the *diamond norm* $||\cdot||_\diamond$, which is the maximum trace norm when an auxiliary space is considered, along with the original Hilbert spaces [Wat11, BS10]. For example, $||\Psi - \Phi||_\diamond = \max_{\rho_{ME}} ||(\Psi \otimes \mathbb{1}_E)\rho_{ME} - (\Phi \otimes \mathbb{1}_E)\rho_{ME}||_1$. This is considered a better determination of the distinguishability of two quantum channels than the $1 \to 1$ norm, that is, $||\Psi - \Phi||_{1\to 1} = \max_{\rho_M} ||\Psi(\rho_M) - \Phi(\rho_M)||_1$, because it accounts for the original space $\mathcal{H}_M$ being entangled with another auxiliary space $\mathcal{H}_E$.

2.9 Symmetric Subspace

We define the symmetric subspace along the same lines as [Har13].

Definition 2.9.1. The *symmetric subspace* over $(\mathcal{H}_d)^{\otimes t}$ is defined as

$$\mathrm{Sym}(d^t) := \{|\phi\rangle \in (\mathcal{H}_d)^{\otimes t} : P_d(\pi)\,|\phi\rangle = |\phi\rangle\,, \forall \pi \in S_t\}, \tag{2.9.1}$$

where

$$P_d(\pi) = \sum_{i_1,\ldots,i_t \in [d]} \left|i_{\pi^{-1}(1)}, \ldots, i_{\pi^{-1}(t)}\right\rangle\!\left\langle i_1, \ldots, i_t\right|$$

for $[d] = \{0, \ldots, d-1\}$ integers and $\pi \in S_t$, the symmetric (permutation) group for t elements, i.e. all the permutations of t elements. The dimension for this subspace is $d_{\mathrm{Sym}} = \binom{d+t-1}{t}$ [Har13].

The symmetric subspace are those elements in $\mathcal{H}_d^{\otimes t}$ which are invariant under tensor product permutations. For example, in the two qubit case, $|00\rangle\,, |11\rangle$, and $\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$ are all in $\mathrm{Sym}(2^2)$ because permuting the qubits leaves the quantum state unchanged. However, there are states which are not in the symmetric subspace, such as $\frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$, which is $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ when a qubit permutation other than the identity is applied.

There are quantum states which are *permutationally symmetric* (i.e. are invariant when permuted tensor product wise) but are not elements of the symmetric subspace. This gap appears when discussing elements in $\mathcal{D}(\mathcal{H}_d^{\otimes 2})$. One such example is $\frac{\mathbb{1}}{2} \otimes \frac{\mathbb{1}}{2} = \frac{\mathbb{1}}{4} \in \mathcal{D}(\mathcal{H}_2^{\otimes t})$, a two-qubit state that is invariant under tensor product permutations but is not an element of the symmetric subspace. Note that for t copies of a pure quantum state, the definitions of symmetric and permutationally symmetric are equivalent. As $|\varphi\rangle^{\otimes t}$ is invariant to permutations, this naturally implies that it is an element of the symmetric subspace.

We use the notation $\mathcal{U}(\mathrm{Sym}(d^t))$ to denote unitaries from $\mathrm{Sym}(d^t) \otimes \mathrm{Sym}(d^t)$ of size $d_{\mathrm{Sym}} \times d_{\mathrm{Sym}}$, in the same way that $\mathcal{U}(d)$ denotes unitaries from $\mathcal{H}_d \otimes \mathcal{H}_d$ of size $d \times d$. Here, d_{Sym} denotes the dimension of $\mathrm{Sym}(d^t)$. We can also restrict unitaries in $\mathcal{U}(d^t)$ to unitaries acting on the symmetric subspace. Such unitaries $U \in \mathcal{U}(d^t)$ are necessarily of the following shape

$$U = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}, \tag{2.9.2}$$

where $A \in \mathcal{U}(\mathrm{Sym}(d^t))$ and B is an element of the group of unitaries on the Hilbert space $W = (\mathrm{Sym}(d^t))^{\perp}$, which is orthogonal to the symmetric subspace. Unitaries of this structure are indeed unitaries and map elements in the symmetric subspace to elements in the symmetric subspace as required.

To extend unitaries in $\mathcal{U}(\mathrm{Sym}(d^t))$ to unitaries in $\mathcal{U}(d^t)$, we can simply apply the map

$$A \mapsto \begin{bmatrix} A & 0 \\ 0 & \mathbb{1} \end{bmatrix}, \tag{2.9.3}$$

which is now a $d^t \times d^t$ unitary.

The notation $\mathcal{D}(\mathrm{Sym}(d^t))$ is for the density operators on $\mathrm{Sym}(d^t)$. In other words, $\rho \in \mathcal{D}(\mathrm{Sym}(d^t))$ if ρ is a density operator and $\Pi_{\mathrm{Sym}}\rho\Pi_{\mathrm{Sym}} = \rho$, where Π_{Sym} is the projector into $\mathrm{Sym}(d^t)$. Furthermore, one can write density matrices in the symmetric subspace as a real linear combination of rank 1 density matrices [Har13], that is,

$$\mathcal{D}(\mathrm{Sym}(d^t)) \subset \mathrm{span}_{\mathbb{R}}\{(|\varphi\rangle\langle\varphi|)^{\otimes t} : |\varphi\rangle \in \mathcal{H}_d\}. \tag{2.9.4}$$

In a similar fashion to how we can restrict unitaries in $\mathcal{U}(d^t)$ to acting on the symmetric subspace, we can restrict $\rho \in \mathcal{D}(\mathcal{H}_{d^t})$ to acting on the symmetric subspace. Using Schur-Weyl duality [FH91], we have $\mathcal{H}_{d^t} = \mathrm{Sym}(d^t) \perp W$ for some subspace W. This ρ is a positive operator with trace 1, as explained in Section 2.3. We are wanting this ρ to act in $\mathcal{D}(\mathrm{Sym}(d^t))$, which implies that $\mathrm{Tr}\big(\rho|_{\mathrm{Sym}(d^t)}\big) = 1$ and $\mathrm{Tr}(\rho|_W) = 0$, and since ρ is positive, its trace is zero if and only if it is the zero matrix. Therefore, this ρ is an operator that is zero on W, and we are able to have an element in $\mathcal{D}(\mathcal{H}_{d^t})$ that is restricted to acting on $\mathrm{Sym}(d^t)$.

Conversely, the elements of $\mathcal{D}(\mathrm{Sym}(d^t))$ are matrices of size $d_{\mathrm{Sym}} \times d_{\mathrm{Sym}}$ which can be extended to matrices of size $d^t \times d^t$. In particular, taking $A \in \mathcal{D}(\mathrm{Sym}(d^t))$,

$$A \mapsto \begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix}, \tag{2.9.5}$$

this is now a unique element of $\mathcal{D}(\mathcal{H}_{d^t})$.

2.10 Representation Theory

Using Schur-Weyl duality and Schur's Lemma [FH91] similarly to [LM20], one can write the following for $\rho \in \mathcal{D}(\mathcal{H}_d^{\otimes t})$:

$$\int_{\mathcal{U}(d)} U^{\otimes t}\rho(U^\dagger)^{\otimes t}dU = \mathrm{Tr}(\Pi_{\mathrm{Sym}}\rho\Pi_{\mathrm{Sym}})\tau_{\mathrm{Sym}} + \sum_b \mathrm{Tr}(\Pi_b\rho\Pi_b)\tau_b, \tag{2.10.1}$$

where Π_{Sym} is the projector into $\mathrm{Sym}(d^t)$ and $\tau_{\mathrm{Sym}} = \frac{\Pi_{\mathrm{Sym}}}{d_{\mathrm{Sym}}}$. These Π_b are projectors into subspaces orthogonal to the symmetric subspace which have dimension d_b, and $\tau_b = \frac{\Pi_b}{d_b}$. When $\rho \in \mathcal{D}(\mathrm{Sym}(d^t))$, the above equation reduces to τ_{Sym}. This integral is called the t-twirling channel, which we occasionally denote as $T^{(t)}$, and appears in the definition of unitary t-designs in Chapter 5.

2.11 Convexity

We define convex hulls and Carathéodory's theorem from [Roc70].

Definition 2.11.1 (Convex Hull)**.** The convex hull of a finite subset $\{b_0, \ldots, b_m\}$ of $\mathbb{R}^n$ consists of all the vectors of the form $\lambda_0 b_0 + \cdots + \lambda_m b_m$, with $\lambda_0 \geq 0, \ldots, \lambda_m \geq 0$, and $\lambda_0 + \cdots + \lambda_m = 1$.

In other words, the convex hull of a finite subset is all the convex combinations of the elements in the given subset.

Moreover, we need Carathéodory's Theorem, which is also defined in [Roc70].

Theorem 2.11.2 (Carathéodory)**.** *Let S be any set of points and directions in $\mathbb{R}^n$, and let C be the convex hull of S. Then $x \in C$ if and only if x can be expressed as a convex combination of $n+1$ of the points and directions in S.*

This result helps us to upper bound our new concept of symmetric unitary t-designs, explained in Chapter 6.

Chapter 3

Private Broadcasting

This chapter is split into two parts: a brief introduction to t-recipient private broadcasting where all parties are assumed to only have classical capabilities, and a new problem we define as t-recipient quantum private broadcasting (t-QPB). This presentation of t-QPB is original to this thesis and closely follows [BGGS21].

3.1 Classical Private Broadcasting

To fully appreciate the problem of quantum private broadcasting, let us first consider *t-recipient private broadcasting (t-PB)*. This is when t copies of a plaintext are encrypted and sent to t different recipients, with the requirement that each needs to independently decrypt their ciphertext. The plaintext, ciphertext, and the encryption scheme are all classical, meaning that they are described with classical bits and computed with modern classical computers.

We examine this problem with the One-Time Pad (OTP), a perfectly secure classical encryption scheme. The plaintext message m is a bit string of length n, and the encryption key k is a randomly generated bit string of the same length as m. Encryption is performed by calculating the exclusive-or $\oplus$, which is addition modulo 2, between the message string and the key. For example, if the message is $m = 00111$ and the key is $k = 10101$, the exclusive-or is

$$\begin{array}{r} 0\,0\,1\,1\,1 \\ \oplus\, 1\,0\,1\,0\,1 \\ \hline 1\,0\,0\,1\,0 \end{array} .$$

This result is the ciphertext c. Now considering t copies of this m, each encrypted

with k, gives

$$t\begin{cases} m \oplus k = c \\ m \oplus k = c \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ m \oplus k = c \end{cases}$$

Each cipertext c is clearly the same, and having t copies of this ciphertext gives no further information about the original message m that is not already gained by having a single copy. There is no information gained from an intercepted ciphertext beyond the length of the message. The reason for this is because both 0 and 1 in the original message can result in an output of 0 or 1 in the ciphertext with the same probability, given that the key k is uniform randomly generated. This is illustrated in Table 3.1.

Message	**Key**	**Output**
0	0	0
0	1	1
1	0	1
1	1	0

Table 3.1: One-Time Pad Ciphertext Outputs

Therefore, intercepting the resulting ciphertext from a message encrypted with the OTP gives no information about the original message, even if an adversary has unlimited resources. The OTP therefore has perfect security, and furthermore each copy of the message m is able to be encrypted with the same key k and maintain this perfect security. This implies that regardless of the value of t, this k has the same length and the total key length in bits is the same. Surprisingly, this is not true with t-recipient quantum private broadcasting, as seen with the quantum one-time pad in Theorem 4.3.1. In order to state and prove this result, we first define t-recipient quantum private broadcasting.

3.2 Quantum Private Broadcasting

Here we formally define *t-recipient Quantum Private Broadcasting* (t-QPB) as an encryption scheme with certain correctness and security definitions.

Definition 3.2.1. Let $\mathcal{H}_M = \mathcal{H}_d$ and $\mathcal{H}_C$ be the message and ciphertext Hilbert spaces, respectively, which in general are both of dimension d. A *δ-correct, t-recipient Quantum Private Broadcast scheme in $\mathcal{H}_M$* is a set of encryption maps $\mathsf{Enc}_k : \mathcal{H}_M^{\otimes t} \to \mathcal{H}_C^{\otimes t}$ along with decryption maps $\mathsf{Dec}_k : \mathcal{H}_C \to \mathcal{H}_M$, where $k \in K$, the set of possible

keys. We require that for each $k \in K$, $\| \left(\mathsf{Dec}_k^{\otimes t} \circ \mathsf{Enc}_k\right)\big|_{\mathrm{Sym}(d^t)} - \mathbb{1}_{\mathrm{Sym}(d^t)}\|_\diamond \leq 1 - \delta$, where the notation $|_{\mathrm{Sym}(d^t)}$ denotes that the input messages are restricted to being elements of $\mathrm{Sym}(d^t)$, and $\mathbb{1}_{\mathrm{Sym}}$ is the identity map in $\mathrm{Sym}(d^t)$.

A diamond norm of 0 corresponds to a perfectly correct t-QPB, while a result of 1 corresponds to a perfectly 'incorrect' t-QPB. We are only concerned with input messages which are pure quantum states of dimension d. Therefore, t copies of such a state is an element of the symmetric subspace $\mathrm{Sym}(d^t)$ as explained in Section 2.9, and we incorporate this requirement into our definition of t-QPB. This restriction is also necessary to prove security properties later in Chapter 5 and Chapter 6.

We note that a 1-correct t-QPB, (that is, a perfect t-QPB) must necessarily be implemented via unitary matrices. Moreover, in this case, as the definition imposes local identical decryption, the decryption operation needs to be the t-fold tensor product of a unitary matrix. Thus, although the encryption maps are not necessarily t-fold tensor products of a unitary matrix, the action of each of them over the symmetric subspace can be written as a t-fold tensor product of a unitary matrix. Such a perfect t-QPB is illustrated in Fig. 3.1.

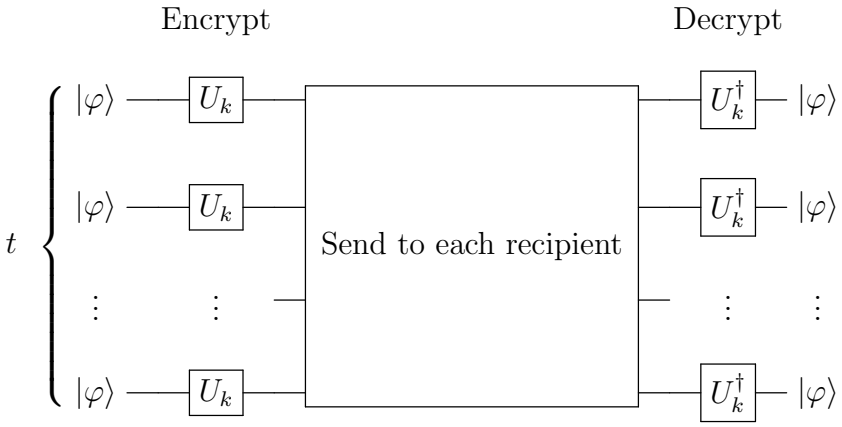

Figure 3.1: Quantum Private Broadcasting

The indistinguishability of ciphertexts for our QPB encryption scheme is based on the definitions from [LM20], which compares the encryption scheme with that of a 'state replacement channel' $\langle\sigma\rangle$. For a fixed $\sigma \in \mathcal{D}(\mathcal{H}_d^{\otimes t})$, the state replacement channel is defined as $\langle\sigma\rangle(R) = \mathrm{Tr}(R)\sigma$, for any $R \in \mathcal{L}(\mathcal{H}_d^{\otimes t})$, the linear operators on $\mathcal{H}_d^{\otimes t}$.

Definition 3.2.2. Let K be the set of possible keys in the QPB. A QPB has ϵ-*indistinguishable ciphertexts* if there exists a fixed $\sigma \in \mathcal{D}(\mathcal{H}_d^{\otimes t})$ such that

$$\left\| \left(\mathop{\mathbb{E}}_{k \in K} \mathsf{Enc}_k - \langle\sigma\rangle \right) \Big|_{\mathrm{Sym}(d^t)} \right\|_{1\to 1} \leq \epsilon. \tag{3.2.1}$$

We note that the above does not consider quantum side information. The encryption scheme has ϵ-*indistinguishable ciphertexts against adversaries with side information* if there exists a fixed $\sigma \in \mathcal{D}(\mathcal{H}_d^{\otimes t})$ such that

$$\left\| \left(\mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k - \langle \sigma \rangle \right) \Big|_{\mathrm{Sym}(d^t)} \right\|_\diamond \leq \epsilon. \tag{3.2.2}$$

Indistinguishability against adversaries with side information necessarily implies indistinguishability from the $1 \to 1$-norm being upper bounded by the $\diamond$-norm.

When the above norms equal zero, we call such encryption schemes *perfectly secure* and *perfectly secure against adversaries with side information*, respectively.

When $t = 1$, Definition 3.2.2 corresponds to the conventional information theoretic encryption [LM20], where there is no restriction in the input space.

The following lemma follows naturally from the setting where t-copies of a pure quantum state are used as the input for a t-QPB.

Lemma 3.2.3. *Let* $\mathsf{Enc}_k^{(t)} : \mathcal{H}_M^{\otimes t} \to \mathcal{H}_C^{\otimes t}$ *and* $\mathsf{Dec}_k : \mathcal{H}_C \to \mathcal{H}_M$*, defined as* $\mathsf{Enc}_k^{(t)}(\rho) = U_k^{\otimes t} \rho (U_k^{\otimes t})^\dagger$ *and* $\mathsf{Dec}_k(\gamma) = U_k^\dagger \gamma U_k$*, respectively. Suppose* $(\mathsf{Enc}_k^{(t)}, \mathsf{Dec}_k)$ *is a perfectly secure and perfectly correct* t*-QPB scheme. Then* $(\mathsf{Enc}_k^{(t-1)}, \mathsf{Dec}_k)$ *is a perfectly secure and perfectly correct* $(t-1)$*-QPB scheme.*

Proof: By definition of encoding and decoding maps it is clear that for any $\rho \in \mathcal{D}(\mathcal{H}_d^{\otimes t-1} \otimes \mathcal{H}_A)$, we have $\left(\mathsf{Dec}_k^{\otimes t-1} \circ \mathsf{Enc}_k^{(t-1)}\right) \otimes \mathbb{1}_A(\rho) = \rho$ and thus

$\left\| \left(\mathsf{Dec}_k^{\otimes t-1} \circ \mathsf{Enc}_k^{(t-1)}\right)\Big|_{\mathrm{Sym}(d^{t-1})} - \mathbb{1}_{\mathrm{Sym}(d^{t-1})} \right\|_\diamond = 0$ showing correctness.

Let $\rho = (|\varphi\rangle\langle\varphi|)^{\otimes t-1}$, with $|\varphi\rangle \in \mathcal{H}_d$, then we have

$$\mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k^{(t-1)}(\rho) = \mathrm{Tr}_1 \left(\mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k^{(t)} \left(\rho \otimes |\varphi\rangle\langle\varphi|\right) \right) = \mathrm{Tr}_1 \left(\tau_{\mathrm{Sym},t}\right) = \tau_{\mathrm{Sym},t-1},$$

where the first equality follows from linearity, and the second follows from the definition of a perfectly correct t-QPB scheme. This last equality can be seen by choosing a specific value of ρ when calculating the averaged encryption. In particular, substituting $\tau_{\mathrm{Sym},t-1}$ for ρ, this yields $\mathbb{E}_{k\in K} \mathsf{Enc}_k^{(t-1)}(\tau_{\mathrm{Sym},t-1}) = \tau_{\mathrm{Sym},t-1}$, which gives the final equality as it necessarily holds for any $\rho = (|\varphi\rangle\langle\varphi|)^{\otimes t-1}$. Note that we use the notation $\tau_{\mathrm{Sym},t}$ to make explicit that it is the maximally mixed state in $\mathcal{D}(\mathrm{Sym}(d^t))$. Moreover, using Eq. (2.9.4) and linearity, we know that this equation holds for any $\rho \in \mathcal{D}(\mathrm{Sym}(d^{t-1}))$. Thus,

$$\left\| \left(\mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k^{(t-1)} - \langle \tau_{\mathrm{Sym},t-1} \rangle \right) \Big|_{\mathrm{Sym}(d^{t-1})} \right\|_{1\to 1} = 0.$$

∎

Chapter 4

Quantum One-Time Pad

This chapter is divided into three sections. The first introduces the quantum one-time pad for 2-dimensions and illustrates why this encryption scheme is both perfectly secure as well as perfectly secure against side information. We introduce the 2-dimensional case first as this is the simplest example and the proof techniques are easier to follow. We then expand to the general dimension case with the general Paulis and the general quantum one-time pad. Lastly, we connect the quantum one-time pad back to the t-QPB problem, closely following [BGGS21]. We demonstrate why using the same encryption key to encrypt two copies with the quantum one-time pad does not yield perfect security, overcoming this obstacle by using independent keys for each copy in the t-QPB. This is done by allowing different encryption/decryption keys for the different t recipients. The bounds on the number of unitaries and classical bits needed for t-independent uses of the quantum one-time pad are summarized in Table 4.1 and Table 4.2.

4.1 Paulis and 2-Dimensional QOTP

When considering encryption schemes, we are concerned with what a possible adversary would see. This is the summation over all possible encryption outputs, divided by the number of possible encryption keys. In other words, we are concerned with the encrypted output, averaged over all possible encryption keys. The reason for this is because while it is possible the adversary knows the set of possible encryption keys, they do not know which key is chosen. We therefore need to consider this expectation over all the encryption keys.

The first quantum encryption scheme we consider for t-QPB is the quantum one-time pad (QOTP), which is discussed in [AMTdW00] and [BR03]. It is defined in the following way for $\rho \in \mathcal{D}(\mathcal{H}_{2^n})$ and $a, b \in \{0,1\}^n$

$$\mathsf{QOTP}_{a,b}(\rho) = X^a Z^b \rho Z^b X^a, \tag{4.1.1}$$

where X and Z are Pauli operators. The encryption key is composed of the bit strings a and b, and in this case is of length $2n$. This QOTP is both perfectly secure and perfectly secure against adversaries with side information [BR03], and it is this property that makes the QOTP a common choice for encrypting a quantum state. For completeness, we present these security results in Lemma 4.1.1 and Lemma 4.1.2.

Lemma 4.1.1. *The quantum one-time pad is perfectly secure.*

Proof: To simplify these calculations, we assume $n = 1$, and the results extend to any $n \in \mathbb{N}$. Recall that the set $\{\mathbb{1}, X, Y, Z\}$ forms a basis for all linear operators of $\mathbb{C}^2$ and that $Y = iXZ$, which means that ρ can be written as

$$\rho = \alpha_i \mathbb{1} + \alpha_x X + \alpha_y XZ + \alpha_z Z \tag{4.1.2}$$

for $\alpha_i, \alpha_x, \alpha_y, \alpha_z \in \mathbb{C}$. We can simplify this equation further by recalling that since ρ is a density operator, this means that its trace must be 1. The trace operator is linear, which means that $\mathrm{Tr}(A + B) = \mathrm{Tr}(A) + \mathrm{Tr}(B)$ and $\mathrm{Tr}(cA) = c\,\mathrm{Tr}(A)$ for constant c. This yields

$$\begin{aligned} \mathrm{Tr}(\rho) &= \mathrm{Tr}(\alpha_i \mathbb{1} + \alpha_x X + \alpha_y XZ + \alpha_z Z) \\ 1 &= \mathrm{Tr}(\alpha_i \mathbb{1}) + \mathrm{Tr}(\alpha_x X) + \mathrm{Tr}(\alpha_y XZ) + \mathrm{Tr}(\alpha_z Z) \\ &= \alpha_i \,\mathrm{Tr}(\mathbb{1}) + \alpha_x \,\mathrm{Tr}(X) + \alpha_y \,\mathrm{Tr}(XZ) + \alpha_z \,\mathrm{Tr}(Z) \\ &= 2 \cdot \alpha_i \\ \frac{1}{2} &= \alpha_i, \end{aligned} \tag{4.1.3}$$

which implies that ρ can be written as $\frac{1}{2}\mathbb{1} + \alpha_x X + \alpha_y XZ + \alpha_z Z$. For two linear operators to commute, this means that $AB = BA$. Simple matrix multiplication shows that each of X, Y and Z commute with themselves as well as the identity operators. Furthermore, they anticommute (i.e. $AB = -BA$) with the other two operators. For example, we have $XZ = -ZX$, which we use shortly.

We now look at the expectation of the QOTP. Simplifying with the commuting and anticommuting properties gives us

$$\mathop{\mathbb{E}}_{a,b\in\{0,1\}} \mathsf{QOTP}_{a,b}(\rho) = \frac{1}{4}\Big(\rho + X\rho X + Z\rho Z + XZ\rho ZX\Big), \tag{4.1.4}$$

whose terms are

$$\begin{aligned} X\rho X &= \frac{1}{2}X(\mathbb{1})X + \alpha_x X(X)X + \alpha_y X(XZ)X + \alpha_z X(Z)X \\ &= \frac{1}{2}\mathbb{1} + \alpha_x X - \alpha_y XZ - \alpha_z Z \\ Z\rho Z &= \frac{1}{2}Z(\mathbb{1})Z + \alpha_x Z(X)Z + \alpha_y Z(XZ)Z + \alpha_z Z(Z)Z \\ &= \frac{1}{2}\mathbb{1} - \alpha_x X - \alpha_y XZ + \alpha_z Z \\ XZ\rho ZX &= \frac{1}{2}XZ(\mathbb{1})ZX + \alpha_x XZ(X)ZX + \alpha_y XZ(XZ)ZX + \alpha_z XZ(Z)ZX \\ &= \frac{1}{2}\mathbb{1} - \alpha_x X + \alpha_y XZ - \alpha_z Z. \end{aligned} \tag{4.1.5}$$

Bringing everything back together, we have

$$\begin{aligned} \mathop{\mathbb{E}}_{a,b\in\{0,1\}} \mathsf{QOTP}_{a,b}(\rho) &= \frac{1}{4}\left(\left(\frac{1}{2}\mathbb{1} + \alpha_x X + \alpha_y XZ + \alpha_z Z\right) + \left(\frac{1}{2}\mathbb{1} + \alpha_x X - \alpha_y XZ - \alpha_z Z\right)\right. \\ &\qquad \left. + \left(\frac{1}{2}\mathbb{1} - \alpha_x X - \alpha_y XZ + \alpha_z Z\right) + \left(\frac{1}{2}\mathbb{1} - \alpha_x X + \alpha_y XZ - \alpha_z Z\right)\right) \\ &= \frac{1}{4}(2\cdot\mathbb{1}) \\ &= \frac{\mathbb{1}}{2}. \end{aligned} \tag{4.1.6}$$

Taking $\langle\sigma\rangle$ to be $\frac{\mathbb{1}}{2}$, this gives

$$\left\| \left(\mathop{\mathbb{E}}_{a,b\in\{0,1\}} \mathsf{QOTP}_{a,b} - \langle\sigma\rangle \right) \right\|_{1\to 1} = 0, \tag{4.1.7}$$

and therefore the QOTP is perfectly secure, which corresponds to the conventional information theoretic security as explained in Section 3.2. ∎

Lemma 4.1.2. *The quantum one-time pad is perfectly secure against adversaries with side information.*

Proof: Now considering adversaries with side information, let the input be composed of two systems, M and E, where M is a single qubit system and E is an n-qubit system. We denote this $n+1$-qubit state as $\rho_{ME} \in \mathcal{D}(\mathcal{H}_M \otimes \mathcal{H}_E)$. We consider two scenarios,

1. $\frac{\mathbb{1}}{2} \otimes \rho_E$
2. $(\mathbb{E}_{a,b\in\{0,1\}} \mathsf{QOTP}_{a,b} \otimes \mathbb{1}_E)\rho_{ME}$.

Since $\mathcal{P}^{\otimes n+1} = \{P_1 \otimes P_2 \otimes \cdots \otimes P_{n+1} | P_i \in \mathcal{P}\}$ forms a basis for all linear operators of $(\mathbb{C}^2)^{n+1}$, we can rewrite ρ_{ME} in terms of Pauli operators:

$$\rho_{ME} = \sum_{P_i \in \mathcal{P}} c_{P_1,P_2,\ldots,P_{n+1}} \cdot P_1 \otimes P_2 \otimes \cdots \otimes P_{n+1}, \quad c_{P_1,P_2,\ldots,P_{n+1}} \in \mathbb{C}. \tag{4.1.8}$$

Henceforth, we use c_P to denote $c_{P_1,P_2,\ldots,P_{n+1}}$.

It is interesting to notice that regardless of whether the $n+1$ quantum state ρ_{ME} is entangled or not, the ability to decompose the density operator as a linear combination of tensored Pauli operators is always true.

Using the fact that $\mathrm{Tr}(\mathbb{1}) = 2$ and $\mathrm{Tr}(X) = \mathrm{Tr}(Y = iXZ) = \mathrm{Tr}(Z) = 0$, the first scenario can be simplified to

$$\begin{aligned}
\frac{\mathbb{1}}{2} \otimes \mathrm{Tr}_M(\rho_{ME}) &= \frac{\mathbb{1}}{2} \otimes \mathrm{Tr}_M \left(\sum_{P_i \in \mathcal{P}} c_P \cdot P_1 \otimes P_2 \otimes \cdots \otimes P_{n+1} \right) \\
&= \frac{\mathbb{1}}{2} \otimes \sum_{P_i \in \mathcal{P}} c_P \cdot \mathrm{Tr}(P_1) \otimes P_2 \otimes \cdots \otimes P_{n+1} \\
&= \frac{\mathbb{1}}{2} \otimes \sum_{\substack{P_i \in \mathcal{P} \\ P_1 = \mathbb{1}}} c_P \cdot \mathrm{Tr}(\mathbb{1}) \otimes P_2 \otimes \cdots \otimes P_{n+1} \\
&= \frac{\mathbb{1}}{2} \otimes \sum_{\substack{P_i \in \mathcal{P} \\ P_1 = \mathbb{1}}} 2 \cdot c_P \cdot P_2 \otimes \cdots \otimes P_{n+1} \\
&= \mathbb{1} \otimes \sum_{\substack{P_i \in \mathcal{P} \\ P_1 = \mathbb{1}}} c_P \cdot P_2 \otimes \cdots \otimes P_{n+1}
\end{aligned} \tag{4.1.9}$$

Now let us look at the second scenario. Applying the QOTP to each of the Pauli operators and taking the expectation yields

$$\begin{aligned}
\mathop{\mathbb{E}}_{a,b\in\{0,1\}} \mathsf{QOTP}_{a,b}(\mathbb{1}) &= \frac{1}{4}(\mathbb{1} + X\mathbb{1}X + Z\mathbb{1}Z + XZ\mathbb{1}ZX) \\
&= \frac{4\mathbb{1}}{4} = \mathbb{1}
\end{aligned}$$

$$\begin{aligned}
\mathop{\mathbb{E}}_{a,b\in\{0,1\}} \mathsf{QOTP}_{a,b}(X) &= \frac{1}{4}(X + XXX + ZXZ + XZXZX) \\
&= \frac{1}{4}(X + X - X - X) = 0
\end{aligned}$$

$$\begin{aligned}
\mathop{\mathbb{E}}_{a,b\in\{0,1\}} \mathsf{QOTP}_{a,b}(iXZ) &= \frac{1}{4}(iXZ + X(iXZ)X + Z(iXZ)Z + XZ(iXZ)ZX) \\
&= \frac{1}{4}(iXZ - iXZ - iXZ + iXZ) = 0
\end{aligned}$$

$$\begin{aligned}
\mathop{\mathbb{E}}_{a,b\in\{0,1\}} \mathsf{QOTP}_{a,b}(Z) &= \frac{1}{4}(Z + XZX + ZZZ + XZZZX) \\
&= \frac{1}{4}(Z - Z + Z - Z) = 0.
\end{aligned} \tag{4.1.10}$$

Bringing everything together, this second scenario can be simplified to

$$\begin{aligned}
\left(\mathop{\mathbb{E}}_{a,b\in\{0,1\}} \mathsf{QOTP}_{a,b} \otimes \mathbb{1}_E\right)\rho_{ME} &= \left(\mathop{\mathbb{E}}_{a,b\in\{0,1\}} \mathsf{QOTP}_{a,b} \otimes \mathbb{1}_E\right)\left(\sum_{P_i\in\mathcal{P}} c_P \cdot P_1 \otimes P_2 \otimes \cdots \otimes P_{n+1}\right) \\
&= \sum_{P_i\in\mathcal{P}} c_P \cdot \mathop{\mathbb{E}}_{a,b\in\{0,1\}} \mathsf{QOTP}_{a,b}(P_1) \otimes P_2 \otimes \cdots \otimes P_{n+1} \\
&= \sum_{\substack{P_i\in\mathcal{P} \\ P_1=\mathbb{1}}} c_P \cdot \mathop{\mathbb{E}}_{a,b\in\{0,1\}} \mathsf{QOTP}_{a,b}(\mathbb{1}) \otimes P_2 \otimes \cdots \otimes P_{n+1} \\
&= \sum_{\substack{P_i\in\mathcal{P} \\ P_1=\mathbb{1}}} c_P \cdot \mathbb{1} \otimes P_2 \otimes \cdots \otimes P_{n+1} \\
&= \mathbb{1} \otimes \sum_{\substack{P_i\in\mathcal{P} \\ P_1=\mathbb{1}}} c_P \cdot P_2 \otimes \cdots \otimes P_{n+1}.
\end{aligned} \tag{4.1.11}$$

These two scenario are therefore the same, and we can conclude that with

$\langle\sigma\rangle = \frac{\mathbb{1}}{2}$,

$$\left\| \left(\mathop{\mathbb{E}}_{a,b\in\{0,1\}} \mathsf{QOTP}_{a,b} - \langle\sigma\rangle \right) \right\|_{\diamond} = 0, \tag{4.1.12}$$

which implies that the QOTP is perfectly secure against adversaries with side information. ∎

4.2 General Paulis

In this section, we present the general Paulis and the general quantum one-time pad, which we include for completeness but is not required to understand the rest of the thesis.

The quantum one-time pad as discussed previously is solely for 2-dimensional quantum systems. This can be expanded to general d-dimensions so that instead of qubits, we are looking at qudits. The four Pauli matrices $\mathcal{P} = \{\mathbb{1}, X, Y, Z\}$ form what is called the Pauli group, which is generated by $\{i\mathbb{1}, X, Z\}$ since $Y = iXZ$. Therefore, for d-dimensions, only the X and Z need to be generalized. We follow the definition and properties for these matrices as explained in [Wat11]. They have the following shape:

$$X_d = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}_{d\times d}, \quad Z_d = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \omega & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega^{d-1} \end{bmatrix}_{d\times d}. \tag{4.2.1}$$

The value ω is a d^{th} root of unity. Explicitly, $\omega = e^{2\pi i/d}$, $\sum_{j=0}^{d-1} \omega^j = 0$, and $\omega^d = 1$. This implies that both X_d and Z_d have a trace of zero, just as in the 2-dimensional case. As explained in [Web16], X_d and Z_d act as $Z_d |n\rangle = \omega^n |n\rangle$ and $X_d |n\rangle = |(n+1) \mod d\rangle$ for a quantum state $|n\rangle$ from the d-dimensional computational basis $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ for $\mathcal{H}_d$. Clearly, Z_d^m continues to have diagonal elements that are roots of unity which sum to zero, and thus the trace remains zero. Meanwhile, X_d^m permutes the columns of X_d in such a way that each column in X_d moves to the left m times, where the first column in the matrix then becomes the last column in the matrix and so forth. The trace of X_d^m is also zero when $m < d$, and when $m = d$, $X_d^m = Z_d^m = \mathbb{1}_d$, the $d \times d$ identity matrix.

In the 2-dimensional case, we explained previously that each of the elements in $\mathcal{P}_1$ either commute or anticommute with the other elements. There are still commutation

relations between the general Paulis, except now there are d possible relations. They can be visualized as a d-valued function F such that

$$F(p_1, p_2) = j, \quad \text{where } p_1 p_2 = \omega^j p_2 p_1, \ (j = 0, \ldots, d-1), \tag{4.2.2}$$

for any $p_1, p_2 \in \{\mathbb{1}_d, X_d, Z_d\}$ [Web16]. Furthermore, the non-identity Paulis have this commutation relation j specified by F with $\frac{1}{d}$ of the other elements in generalized Pauli group.

The general Pauli group, generated by $\mathcal{P}_d = \{\tilde{\omega}\mathbb{1}_d, X_d, Z_d\}$, forms a basis for the linear operators of $\mathbb{C}^d$, and the group generated by $(\mathcal{P}_d)^{\otimes t}$ forms a basis for the linear operators on $(\mathbb{C}^d)^{\otimes t}$. As explained in [Web16], this $\tilde{\omega}$ is ω when d is odd and $e^{\pi i/d}$ when d is even. This is because a basis for the linear operators on $\mathbb{C}^d$ needs to have d^2 elements since an elementary basis can be formed with all the $d \times d$ matrices which have a 1 in a single entry and zeros elsewhere. There are d^2 such matrices, and therefore every basis must have d^2 elements. The general Paulis are of the form $X_d^m Z_d^n$ for $m, n \in \{0, 1, \ldots, d-1\}$. The order matters here because of the commutation relation $F(X_d^m, Z_d^n)$ which says that $X_d^m Z_d^n = \omega^j Z_d^n X_d^m$, and therefore we only need to take into account those matrices of the form $X_d^m Z_d^n$. There are d choices for X_d^m and d choices for Z_d^n, and therefore there are d^2 general Paulis.

It is true that the elements of the general Pauli group are still unitary matrices. One way to check whether a matrix is unitary is to observe how it acts on an orthonormal basis. A unitary matrix preserves both the inner product of two quantum states and the Euclidean norm. This means $\langle Ux|Uy\rangle = \langle x|y\rangle$ and $U|x\rangle$ has norm 1. Therefore, a unitary matrix applied to an orthonormal basis should necessarily output an orthonormal basis.

Suppose $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ is an orthonormal basis for $\mathcal{H}_d$. The matrix X_d acts on each element as $X_d|n\rangle = |(n+1) \mod d\rangle$, which is simply a permutation of the basis elements. Thus X_d applied to the orthonormal basis outputs an orthonormal basis, and is the same orthonormal basis in this case. The matrix Z_d acts on each element as $Z_d|n\rangle = \omega^n|n\rangle$. Taking the inner product of any two of these elements yields $\langle \omega^n n|\omega^m m\rangle = (\omega^n)^\dagger \cdot \omega^m \cdot \langle n|m\rangle = 0$, and is thus still orthogonal. As mentioned previously, $\omega = e^{2\pi i/d}$, so $\omega^j = e^{2j\pi i/d}$, and it is easy to see that

$$|\omega^j|^2 = |\cos(2j\pi/d) + i\sin(2j\pi/d)|^2 = \cos^2(2j\pi/d) + \sin^2(2j\pi/d) = 1,$$

which implies that $Z_d|n\rangle$ has norm 1. Therefore the output from Z_d applied to orthonormal basis elements is again an orthonormal basis, and we conclude that X_d and Z_d are unitary matrices. It follows that any product of these two matrices is also unitary.

These facts about the general Pauli group can be used to show that the general quantum one-time pad is a perfectly secure encryption scheme for qudits.

4.2.1 General Quantum One-Time Pad

Before defining this general quantum one-time pad, let us first determine how to write $\psi \in \mathcal{D}(\mathcal{H}_d)$ in terms of the general Pauli operators since they form a basis for the linear operators on $\mathbb{C}^d$. The matrices X_d^m and Z_d^m have trace zero when $m < d$, and it is also true that $Z_d^n \cdot X_d^m$ and $X_d^m \cdot Z_d^n$ has trace zero when $n, m < d$. The reason for this is because X_d^m applied to Z_d^n permutes the columns of Z_d^n, whose diagonal always sums to 0 when $n < d$. This means that every non-identity element of the general Pauli group has trace zero, and ψ can be written as

$$\psi = \frac{1}{d}\mathbb{1}_d + \sum_{P \in \tilde{\mathcal{P}}_d} b_P \cdot P \tag{4.2.3}$$

where $\tilde{\mathcal{P}}_d = \mathcal{P}_d \backslash \mathbb{1}_d$ and $b_P \in \mathbb{C}$. The reason for this is because the trace of ψ must equal 1, which implies that

$$\begin{aligned}
\operatorname{Tr}(\psi) &= \operatorname{Tr}\left(\sum_{P \in \mathcal{P}_d} b_P \cdot P\right) \\
&= \operatorname{Tr}\left(\alpha \mathbb{1}_d + \sum_{P \in \tilde{\mathcal{P}}_d} b_P \cdot P\right), \quad \alpha \in \mathbb{C} \\
1 &= \operatorname{Tr}(\alpha \mathbb{1}_d) + \operatorname{Tr}\left(\sum_{P \in \tilde{\mathcal{P}}_d} b_P \cdot P\right) \\
1 &= \alpha \operatorname{Tr}(\mathbb{1}_d) + \sum_{P \in \tilde{\mathcal{P}}_d} b_P \cdot \operatorname{Tr}(P) \\
1 &= \alpha \cdot d + 0 \\
\frac{1}{d} &= \alpha.
\end{aligned} \tag{4.2.4}$$

Now consider the general quantum one-time pad (gQOTP), defined as

$$\mathsf{gQOTP}_a(\psi) = Q_a \psi Q_a^\dagger \tag{4.2.5}$$

for $Q_a \in \mathcal{P}_d$ with $a \in \{0, \ldots, d^2 - 1\}$. Following similar techniques to the proof of Lemma 4.1.1, we prove the following lemma.

Lemma 4.2.1. *The general quantum one-time pad is perfectly secure.*

Proof: Let us firstly examine the expectation of gQOTP_a applied to a state $\psi \in$

$\mathcal{D}(\mathcal{H}_d)$. This gives

$$\begin{aligned}\mathop{\mathbb{E}}_a \mathsf{gQOTP}_a(\psi) &= \frac{1}{d^2}\sum_a Q_a \psi Q_a^\dagger \\ &= \frac{1}{d^2}\left(\frac{1}{d}\sum_a Q_a \mathbb{1}_d Q_a^\dagger + \sum_a \sum_{P\in\tilde{\mathcal{P}}_d} b_P \cdot Q_a P Q_a^\dagger\right).\end{aligned} \tag{4.2.6}$$

We can simplify this expectation by using the commutation relations of $\mathcal{P}_d$, along with the fact that the generalized Paulis are still unitary matrices, so $Q_a Q_a^\dagger = \mathbb{1}_d$ for $Q_a \in \mathcal{P}_d$.

$$\begin{aligned}\sum_a \sum_{P\in\tilde{P}_d} b_P \cdot Q_a P Q_a^\dagger &= \sum_{P\in\tilde{\mathcal{P}}_d} b_P \cdot \sum_a Q_a P Q_a^\dagger \\ &= \sum_{P\in\tilde{\mathcal{P}}_d} b_P \cdot \left(\sum_{\substack{a \\ F(Q_a,P)=0}} Q_a P Q_a^\dagger + \cdots + \sum_{\substack{a \\ F(Q_a,P)=d-1}} Q_a P Q_a^\dagger\right) \\ &= \sum_{P\in\tilde{\mathcal{P}}_d} b_P \cdot \left(\sum_{\substack{a \\ F(Q_a,P)=0}} \omega^0 P Q_a Q_a^\dagger + \cdots + \sum_{\substack{a \\ F(Q_a,P)=d-1}} \omega^{d-1} P Q_a Q_a^\dagger\right) \\ &= \sum_{P\in\tilde{\mathcal{P}}_d} b_P \cdot \left(\sum_{\substack{a \\ F(Q_a,P)=0}} \omega^0 + \cdots + \sum_{\substack{a \\ F(Q_a,P)=d-1}} \omega^{d-1}\right) P\cdot\mathbb{1}_d \\ &= \sum_{P\in\tilde{\mathcal{P}}_d} b_P \cdot \left(\frac{1}{d}\cdot\omega^0 + \cdots + \frac{1}{d}\cdot\omega^{d-1}\right) P \\ &= \sum_{P\in\tilde{\mathcal{P}}_d} b_P \cdot \left(\frac{1}{d}\left(\sum_{j=0}^{d-1}\omega^j\right)\right) P \\ &= \sum_{P\in\tilde{\mathcal{P}}_d} b_P \cdot 0 \cdot P = 0\end{aligned} \tag{4.2.7}$$

The other half of the expectation of gQOTP_a is

$$\begin{aligned}\frac{1}{d}\sum_a Q_a \mathbb{1}_d Q_a^\dagger &= \frac{1}{d}\sum_a Q_a Q_a^\dagger \\ &= \frac{1}{d}\sum_a \mathbb{1}_d \\ &= \frac{1}{d}\cdot(d^2)\cdot\mathbb{1}_d\end{aligned} \tag{4.2.8}$$

Bringing together these simplifications, Eq. (4.2.6) now yields

$$\begin{aligned}\mathop{\mathbb{E}}_a \mathsf{gQOTP}_a(\psi) &= \frac{1}{d^2}\left(\frac{1}{d}\sum_a Q_a \mathbb{1}_d Q_a^\dagger + \sum_a \sum_{P\in\tilde{P}_d} b_P \cdot Q_a P Q_a^\dagger\right) \\ &= \frac{1}{d^2}\left(\left(\frac{1}{d}\cdot(d^2)\cdot\mathbb{1}_d\right)+0\right) \\ &= \frac{1}{d}\mathbb{1}_d.\end{aligned} \tag{4.2.9}$$

This is the maximally mixed state and is independent of the original input ψ. Letting $\langle\sigma\rangle = \frac{\mathbb{1}_d}{d}$, we can conclude that

$$\left\|\left(\mathop{\mathbb{E}}_a \mathsf{gQOTP}_a - \langle\sigma\rangle\right)\right\|_{1\to 1} = 0, \tag{4.2.10}$$

and the general quantum one-time pad is perfectly secure. ∎

As in the 2-dimensional case, the following lemma is true for the general quantum one-time pad.

Lemma 4.2.2. *The general quantum one-time pad is perfectly secure against adversaries with side information.*

Proof: The proof is similar to the proof of Lemma 4.1.2, using the result that $\mathbb{E}_a \mathsf{gQOTP}_a(P) = 0$ for $P \in \tilde{\mathcal{P}}_d$. ∎

4.3 QPB with the Quantum One-Time Pad

As we have illustrated, the quantum one-time pad (QOTP) is not only perfectly secure, but it is also perfectly secure against adversaries with side information. However, what if the QOTP is extended to twice encrypting the same quantum state with

the same encryption key? In the classical case with the one-time pad, this results in two copies of the same ciphertext. Both copies retain their perfect security, and having an additional copy of the ciphertext does not give an adversary an advantage in their task of determining the original plaintext. As we show next, this is not true in the quantum case with the QOTP.

Theorem 4.3.1. $\mathsf{QOTP}_{a,b} \otimes \mathsf{QOTP}_{a,b}$ *with the same key* a, b *is a 1-correct, 2-recipient QPB scheme, but it does not have* ϵ*-indistinguishable ciphertexts for any* $\epsilon < 1/2$.

Proof: This $\mathsf{QOTP}_{a,b} \otimes \mathsf{QOTP}_{a,b}$ can be defined as a "double quantum one-time pad" for $\varphi, \psi \in \mathcal{D}(\mathcal{H}_2)$ and $a, b \in \{0, 1\}$:

$$\mathsf{dQOTP}_{a,b}(\varphi \otimes \psi) = X^a Z^b \otimes X^a Z^b (\varphi \otimes \psi) Z^b X^a \otimes Z^b X^a. \tag{4.3.1}$$

Let us consider the scenario where we have two different quantum states, ρ_0 and ρ_1, which we want to encrypt with the double quantum one-time pad. By cleverly choosing these quantum states, we are able to show that their averaged encryption outputs are not the same. Let us take ρ_0 and ρ_1 and the following quantum states:

$$\begin{aligned} \rho_0 &= |0\rangle\langle 0| \otimes |0\rangle\langle 0| \\ \rho_1 &= |+\rangle\langle +| \otimes |+\rangle\langle +| \ . \end{aligned} \tag{4.3.2}$$

The expectation of $\mathsf{dQOTP}_{a,b}$ applied to each state results in

$$\begin{aligned} \mathop{\mathbb{E}}_{a,b} \mathsf{dQOTP}_{a,b}(\rho_0) &= \frac{1}{4}\Big(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + (X \otimes X) |0\rangle\langle 0| \otimes |0\rangle\langle 0| (X \otimes X) \\ &\quad + (Z \otimes Z) |0\rangle\langle 0| \otimes |0\rangle\langle 0| (Z \otimes Z) + (XZ \otimes XZ) |0\rangle\langle 0| \otimes |0\rangle\langle 0| (ZX \otimes ZX) \Big) \\ &= \frac{1}{4}\Big(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1| + |0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1| \Big) \\ &= \frac{1}{4}\Big(2\big(|0\rangle\langle 0| \otimes |0\rangle\langle 0| \big) + 2\big(|1\rangle\langle 1| \otimes |1\rangle\langle 1| \big) \Big) \\ &= \frac{1}{2}\Big(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1| \Big) \end{aligned} \tag{4.3.3}$$

$$\begin{aligned}
\mathop{\mathbb{E}}_{a,b} \mathsf{dQOTP}_{a,b}(\rho_1) &= \frac{1}{4}\Big(|+\rangle\langle+| \otimes |+\rangle\langle+| + (X\otimes X)\,|+\rangle\langle+| \otimes |+\rangle\langle+|\,(X\otimes X) \\
&\quad + (Z\otimes Z)\,|+\rangle\langle+| \otimes |+\rangle\langle+|\,(Z\otimes Z) \\
&\quad + (XZ\otimes XZ)\,|+\rangle\langle+| \otimes |+\rangle\langle+|\,(ZX\otimes ZX)\Big) \\
&= \frac{1}{4}\Big(\Big[\,|+\rangle\langle+| \otimes |+\rangle\langle+|\,\Big] + \Big[\,|+\rangle\langle+| \otimes |+\rangle\langle+|\,\Big] \\
&\quad + \Big[\,|-\rangle\langle-| \otimes |-\rangle\langle-|\,\Big] + \Big[\,|-\rangle\langle-| \otimes |-\rangle\langle-|\,\Big]\Big) \\
&= \frac{1}{4}\Big(2\Big[\,|+\rangle\langle+| \otimes |+\rangle\langle+|\,\Big] + 2\Big[\,|-\rangle\langle-| \otimes |-\rangle\langle-|\,\Big]\Big) \\
&= \frac{1}{2}\Big(\Big[\,|+\rangle\langle+| \otimes |+\rangle\langle+|\,\Big] + \Big[\,|-\rangle\langle-| \otimes |-\rangle\langle-|\,\Big]\Big)
\end{aligned} \tag{4.3.4}$$

We have that, for any state replacement channel $\langle\sigma\rangle$, where $\sigma \in \mathcal{D}(\mathcal{H}_2^{\otimes 2})$,

$$\begin{aligned}
&\left\| \Big(\mathop{\mathbb{E}}_{a,b} \mathsf{dQOTP}_{a,b} - \langle\sigma\rangle \Big)\Big|_{\mathrm{Sym}(2^2)} \right\|_{1\to 1} \\
&\quad = \max_{\rho\in\mathcal{D}(\mathrm{Sym}(2^2))} \left\| \mathop{\mathbb{E}}_{a,b} \mathsf{dQOTP}_{a,b}(\rho) - \langle\sigma\rangle(\rho) \right\|_1 \\
&\quad \geq \frac{1}{2}\left(\left\| \mathop{\mathbb{E}}_{a,b} \mathsf{dQOTP}_{a,b}(\rho_0) - \langle\sigma\rangle(\rho_0) \right\|_1 + \left\| \mathop{\mathbb{E}}_{a,b} \mathsf{dQOTP}_{a,b}(\rho_1) - \langle\sigma\rangle(\rho_1) \right\|_1 \right) \\
&\quad \geq \frac{1}{2} \left\| \mathop{\mathbb{E}}_{a,b} \mathsf{dQOTP}_{a,b}(\rho_0) - \mathop{\mathbb{E}}_{a,b} \mathsf{dQOTP}_{a,b}(\rho_1) \right\|_1 \geq \frac{1}{2}.
\end{aligned} \tag{4.3.5}$$

The last line in Eq. (4.3.5) is from the triangle inequality, since $\langle\sigma\rangle(\rho_0) = \langle\sigma\rangle(\rho_1)$. The value of $\frac{1}{2}$ is calculated using the definition of the trace norm for $||A-B||_1 = \left(\mathrm{Tr}\left(\sqrt{(A-B)^\dagger(A-B)}\right)\right)$, where $A = \mathbb{E}_{a,b}\,\mathsf{dQOTP}_{a,b}(\rho_0)$ and $B = \mathbb{E}_{a,b}\,\mathsf{dQOTP}_{a,b}(\rho_1)$. Running this through Python gives $\frac{1}{2}$, and we can conclude that $\mathsf{QOTP}_{a,b} \otimes \mathsf{QOTP}_{a,b}$ does not have ϵ-indistinguishable ciphertexts for $\epsilon < 1/2$. The code is given in Appendix A. ∎

Therefore, encryption using the QOTP with the same key is not sufficient to obtain perfect security when encrypting multiple copies of the same message. Using independent encryption keys for each copy of the message is one possible solution to this problem.

To allow for different decryption keys, we extend Definition 3.2.1 so that the encryption map becomes $\mathsf{Enc}_k : \mathcal{H}_M \to \mathcal{H}_C$. The correctness condition now considers

$(\mathsf{Dec}_{k_1} \otimes \cdots \otimes \mathsf{Dec}_{k_t}) \circ (\mathsf{Enc}_{k_1} \otimes \cdots \otimes \mathsf{Enc}_{k_t})$, and similarly for the security conditions. Note that this is the only place that we consider this extended definition.

If one uses different encryption keys for t copies of the QOTP, one can see in Table 4.1 that this leads to the amount of unitaries needed being exponential in t, the number of copies. It is known that to encrypt once an n-qubit state with the QOTP, 2^{2n} unitaries are needed [BR03]. To translate this to classical bits, the logarithm base 2 is taken of the total number of unitaries to give the total number of classical bits needed.

As we are concerned with t-QPB, we are interested in the number of classical bits required for t independent uses of the QOTP. We denote this encryption as $\mathsf{QOTP}^{\otimes t}_{a_i,b_i}$, where $a_i, b_i \in \{0,1\}^n$ for $i = 1, \ldots, t$. This can be extended more generally with the gQOTP, and the number of unitaries needed for the QOTP and the gQOTP is summarized in Table 4.1.

	$\mathsf{QOTP}_{a,b}$	$\mathsf{QOTP}^{\otimes t}_{a_i,b_i}$
Qubits $(d = 2^n)$	$d^2 = 4^n$	$d^{2t} = 4^{nt}$
General d^n	d^{2n}	d^{2nt}

Table 4.1: Quantum One-Time Pad Unitary Bounds

Moreover, the amount of bits needed to implement these encryption schemes is summarized in Table 4.2.

	$\mathsf{QOTP}_{a,b}$	$\mathsf{QOTP}^{\otimes t}_{a_i,b_i}$
Qubits $(d = 2^n)$	$\log_2(4^n) = 2n$	$\log_2(4^{nt}) = 2nt$
General d^n	$\log_2(d^{2n}) = 2n \log_2(d)$	$\log_2(d^{2nt}) = 2nt \log_2(d)$

Table 4.2: Quantum One-Time Pad Key Length Bounds

One can see that the key length necessary for t-copies increases linearly in t. As mentioned in the introduction, the question then became whether we could improve this key length so as to accomplish t-QPB with the same level of security as the QOTP but with less classical bits. Specifically, we need the function describing the key length to have a slope that is increasing at a more gradual pace than $2nt \log_2(d)$. This led us to examining unitary t-designs, which we define in the following section before examining how unitary t-designs can be used as encryption schemes for t-QPB.

Chapter 5

Unitary t-designs

This chapter focuses firstly on defining exact unitary t-designs and providing a few examples. Next we define approximate unitary t-designs, after which we discuss lower and upper bounds on the number of unitaries needed for a unitary t-design. We then examine how unitary t-designs can be used as encryption schemes for the t-QPB problem, and compare the key length needed with this scheme as opposed to with the quantum one-time pad. Section 5.4 and Section 5.5 are original contributions closely following [BGGS21], while the preceding sections are recalling results from previous work completed with unitary t-designs. We note that our notation for unitary t-designs and explanations in Section 5.2 closely follow [BGGS21].

5.1 Exact Designs

Unitary t-designs are a recent topic in the last two decades that have been examined in quantum information theory with multiple applications, such as quantum cryptography [ABW09, AM17, LM20], randomized benchmarking [ZZP17, NZO+21], and decoupling [SDTR13, NS20]. Unitary t-designs are of such great interest because they have the property that choosing a unitary matrix from a finite set of matrices appears the same as if a Haar-random matrix was chosen from the whole unitary group. Generating Haar-random unitary matrices is inefficient [DCEL09], and there are infinitely many unitary matrices, therefore a finite set of matrices that appear Haar-random is a more cost-effective option. However, there is a caveat with these t-designs, and it is that this chosen matrix only appears Haar-random when applied up to t-times. As soon as a matrix from a unitary t-design is applied $t+1$ times, one can no longer claim that it appears the same as a Haar-random unitary.

The term "unitary t-design" was first brought forth in the Master's thesis of Christoph Dankert [Dan05], where he discussed unitary 2-designs and possible strategies to extend this idea to general t. Shortly thereafter, work appeared studying unitary 2-designs [GAE07, DCEL09] and t-designs [AE07]. Follow-up work on t-designs

includes [RS09, CLLW16, LM20, AMR20, BNOZ20].

We define unitary t-designs in Definition 5.1.1, and show in Lemma 5.1.3 that this is equivalent to Definition 5.1.2. These definitions are based from those presented in [RS09], which we adapt to our notation.

Definition 5.1.1. Let $\{U_k\}_{k\in K}$ be a finite subset of $\mathcal{U}(d)$ and let $w : \{U_k\}_{k\in K} \to \mathbb{R}$ be a positive weight function such that $w(U_k) \geq 0$, $\sum_{k\in K} w(U_k) = 1$. Let $\rho \in \mathcal{D}(\mathcal{H}_d^{\otimes t})$. Then $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ is called a *unitary t-design* if

$$\mathbb{E}_{\mathfrak{U}}\left[U^{\otimes t}\rho(U^\dagger)^{\otimes t}\right] = \sum_{k\in K} w(U_k)\cdot U_k^{\otimes t}\rho(U_k^\dagger)^{\otimes t} = \int_{\mathcal{U}(d)} U^{\otimes t}\rho(U^\dagger)^{\otimes t}dU, \tag{5.1.1}$$

where the integral is over the whole unitary group with respect to the Haar measure.

Definition 5.1.2. Let $\mathrm{Hom}(\mathcal{U}(d), k, \ell)$ denote the polynomials that are homogeneous of degree k in the matrix entries of $U \in \mathcal{U}(d)$ and homogeneous of degree ℓ in the entries of $U^\dagger$. Let $w : \{U_k\}_{k\in K} \to \mathbb{R}$ be a positive weight function. Then $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ is a *unitary t-design* if for every $f \in \mathrm{Hom}(\mathcal{U}(d), t, t)$

$$\mathbb{E}_{\mathfrak{U}}[f(U)] = \sum_{k\in K} w(U_k)f(U_k) = \int_{\mathcal{U}(d)} f(U)dU. \tag{5.1.2}$$

When this $w(U_k) = \frac{1}{|K|}$ for every U_k, this is an *unweighted* unitary t-design. Otherwise, it is a *weighted* unitary t-design.

To illustrate further what this $\mathrm{Hom}(\mathcal{U}(d), k, \ell)$ really means, let us recall what is meant by polynomials that are homogeneous of degree k. This is when the degrees of each of the variables in each term of a polynomial sum to k. For example, $x^3y + x^2y^2 + y^4$ is a homogeneous polynomial of x and y because each term has a total degree of 4. A $d \times d$ matrix U can be written as

$$\begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1d} \\ \vdots & \vdots & \ddots & \vdots \\ u_{d1} & u_{d2} & \cdots & u_{dd} \end{bmatrix}, \tag{5.1.3}$$

where each entry can be seen as one variable for a total of d^2 variables. The entries of U^n are homogeneous polynomials of degree n, and the entries of $U^{\otimes n}$ are homogeneous monomials of degree n. Therefore, the entries of $U^{\otimes t} \otimes (U^\dagger)^{\otimes t}$ are monomials that are homogeneous of degree t in the matrix entries of U and homogeneous of degree t in the entries of $U^\dagger$, while the entries of $U^{\otimes t}\rho(U^\dagger)^{\otimes t}$ are homogeneous polynomials of degree t in the matrix entries of U and $U^\dagger$, respectively.

These two definitions of unitary t-designs are equivalent, which we now show along similar lines to [Kaz10] and [Ada13].

Lemma 5.1.3. *Definition 5.1.1 and Definition 5.1.2 are equivalent.*

Proof: ($\Rightarrow$) Assume that Definition 5.1.1 is true. In other words,

$$\hat{\sigma} = \sum_{k\in K} w(U_k) U_k^{\otimes t} \rho (U_k^\dagger)^{\otimes t} = \int_{\mathcal{U}(d)} U^{\otimes t} \rho (U^\dagger)^{\otimes t} dU = \tilde{\sigma}. \tag{5.1.4}$$

Let us denote $U^{(t,t)} = U^{\otimes t} \rho (U^\dagger)^{\otimes t}$. Every $U^{(t,t)}_{m,n}$ is a polynomial of $2d^2$ variables that is homogeneous of degree (t,t). The entries of $\hat{\sigma}$ are simply the expectations of these polynomials,

$$(\hat{\sigma})_{m,n} = \sum_{k\in K} w(U_k) {U_k}^{(t,t)}_{m,n}, \tag{5.1.5}$$

and from our beginning assumption, $\hat{\sigma} = \tilde{\sigma}$, which implies that $(\hat{\sigma})_{m,n} = (\tilde{\sigma})_{m,n}$. The entries of $(\tilde{\sigma})$ are the expectations of the corresponding polynomials when U is chosen from the Haar measure.

Furthermore, Eq. (5.1.4) holds for any $\rho \in \mathcal{D}(\mathcal{H}_d^{\otimes t})$, and in general for any $\rho \in \mathcal{L}(\mathcal{H}_d^{\otimes t})$. This implies that ρ can be chosen such that $U^{(t,t)}_{m,n}$ forms a basis for the functions in $\mathrm{Hom}(\mathcal{U}(d), t, t)$, and since $(\hat{\sigma})_{m,n} = (\tilde{\sigma})_{m,n}$, Definition 5.1.2 is true.

($\Leftarrow$) Assume that Definition 5.1.2 is true. Now let us define a function $f : U \mapsto U^{\otimes t} \rho (U^\dagger)^{\otimes t}$. Assuming U is a general $d \times d$ unitary matrix with distinct variable entries, it is clear that the entries of $U^{\otimes t}$ are monomials of d^2 variables that are homogeneous of degree t. This is similar for the entries of $(U^\dagger)^{\otimes t}$, and therefore the matrix entries of $U^{\otimes t} \rho (U^\dagger)^{\otimes t}$ are polynomials of $2d^2$ variables that are homogeneous of degree (t,t), and this implies that $f \in \mathrm{Hom}(\mathcal{U}(d), t, t)$. Therefore, Definition 5.1.1 is also true. ∎

As already mentioned directly prior to Lemma 5.1.3, the entries of $U^{\otimes t} \otimes (U^\dagger)^{\otimes t}$ are elements of $\mathrm{Hom}(\mathcal{U}(d), t, t)$. For this reason, an equivalent condition for a unitary t-design is

$$\sum_{k\in K} w(U_k) U_k^{\otimes t} \otimes (U_k^\dagger)^{\otimes t} = \int_{\mathcal{U}(d)} U^{\otimes t} \otimes (U^\dagger)^{\otimes t} dU. \tag{5.1.6}$$

We use Eq. (5.1.1) and Eq. (5.1.6) interchangeably throughout this thesis when discussing unitary t-designs, depending on the context.

There is an equation that is helpful determining whether a finite set of unitaries is a t-design, as explained and proved in [Sco08a] and [Kaz10].

Lemma 5.1.4. *For any finite $\{U_k\}_{k\in K} \subseteq \mathcal{U}(d)$,*

$$\sum_{k,\ell\in K} w(U_k) w(U_\ell) \left| \mathrm{Tr}\left(U_k^\dagger U_\ell\right) \right|^{2t} \geq \int_{\mathcal{U}(d)} \left| \mathrm{Tr}(U) \right|^{2t} dU, \tag{5.1.7}$$

with equality if and only if $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ is a unitary t-design.

Proof: Assume $\{U_k\}_{k\in K}$ is a finite subset of $\mathcal{U}(d)$ and $w : \{U_k\}_{k\in K} \to \mathbb{R}$ is a positive weight function. Let us define

$$D := \underbrace{\sum_{k\in K} w(U_k) U_k^{\otimes t} \otimes (U_k^\dagger)^{\otimes t}}_{A} - \underbrace{\int_{\mathcal{U}(d)} U^{\otimes t} \otimes (U^\dagger)^{\otimes t} dU}_{B}, \tag{5.1.8}$$

which clearly equals zero if and only if $\mathfrak{U}$ is a unitary t-design. Since A and B are both linear operators, their difference is also a linear operator. Let $|\psi\rangle \in \mathcal{H}_{d^t}$ be a vector, and consider $\langle\psi|D^\dagger D|\psi\rangle$. This is the inner product of the vector $D|\psi\rangle$ with itself, which equals $\sum_i c_i^\dagger c_i \geq 0$, where c_i are the entries of $D|\psi\rangle$ with respect to an orthonormal basis. This implies that $D^\dagger D$ is a positive semi-definite operator since the definition for a linear operator M to be semi-definite is that $\langle\psi|M|\psi\rangle \geq 0$ for all vectors $|\psi\rangle$. Furthermore, the trace of M is $\mathrm{Tr}(M) = \sum_b \langle b|M|b\rangle$ for some fixed basis $|b\rangle$. If M is positive semi-definite, then this implies $\mathrm{Tr}(M) \geq 0$. Therefore, we know that $\mathrm{Tr}\big(D^\dagger D\big) \geq 0$, which equals zero only when $D = 0$.

Expanding $\mathrm{Tr}\big(D^\dagger D\big)$ becomes

$$\begin{aligned}\mathrm{Tr}\Big((A-B)^\dagger(A-B)\Big) &= \mathrm{Tr}\Big((A^\dagger - B^\dagger)(A-B)\Big) \\ &= \mathrm{Tr}\big(A^\dagger A\big) - \mathrm{Tr}\big(A^\dagger B\big) - \mathrm{Tr}\big(B^\dagger A\big) + \mathrm{Tr}\big(B^\dagger B\big).\end{aligned} \tag{5.1.9}$$

We now look at each of these terms. Starting with $\mathrm{Tr}\big(A^\dagger A\big)$, this becomes

$$\begin{aligned}&\mathrm{Tr}\left[\Big(\sum_{k\in K} w(U_k) U_k^{\otimes t} \otimes (U_k^\dagger)^{\otimes t}\Big)^\dagger \Big(\sum_{\ell\in K} w(U_\ell) U_\ell^{\otimes t} \otimes (U_\ell^\dagger)^{\otimes t}\Big)\right] \\ &= \sum_{k,\ell\in K} w(U_k) w(U_\ell)\, \mathrm{Tr}\left[(U_k^{\otimes t} \otimes (U_k^\dagger)^{\otimes t})^\dagger (U_\ell^{\otimes t} \otimes (U_\ell^\dagger)^{\otimes t})\right] \\ &= \sum_{k,\ell\in K} w(U_k) w(U_\ell)\, \mathrm{Tr}\left[(U_k^\dagger U_\ell)^{\otimes t} \otimes (U_k U_\ell^\dagger)^{\otimes t})\right] \\ &= \sum_{k,\ell\in K} w(U_k) w(U_\ell)\, \mathrm{Tr}\Big(U_k^\dagger U_\ell\Big)^t \cdot \mathrm{Tr}\Big(U_k U_\ell^\dagger\Big)^t \\ &= \sum_{k,\ell\in K} w(U_k) w(U_\ell) \left|\mathrm{Tr}\Big(U_k^\dagger U_\ell\Big)\right|^{2t},\end{aligned} \tag{5.1.10}$$

where the last equality comes from the fact that $\mathrm{Tr}\Big(U_k^\dagger U_\ell\Big)^\dagger = \mathrm{Tr}\Big(U_\ell^\dagger U_k\Big) = \mathrm{Tr}\Big(U_k U_\ell^\dagger\Big)$.

Considering now $\mathrm{Tr}\big(B^\dagger B\big)$ with $V \in \mathcal{U}(d)$ in the second integral, this becomes

$$\begin{aligned}&\mathrm{Tr}\left[\Big(\int_{\mathcal{U}(d)} U^{\otimes t} \otimes (U^\dagger)^{\otimes t} dU\Big)^\dagger \Big(\int_{\mathcal{U}(d)} V^{\otimes t} \otimes (V^\dagger)^{\otimes t} dV\Big)\right] \\ &= \int_{\mathcal{U}(d)} \int_{\mathcal{U}(d)} \left|\mathrm{Tr}\big(U^\dagger V\big)\right|^{2t} dV dU.\end{aligned} \tag{5.1.11}$$

Let $f(U) = \int_{\mathcal{U}(d)} \left|\mathrm{Tr}\left(U^\dagger V\right)\right|^{2t} dV$. This V varies throughout the whole unitary group, and by the left invariance of the Haar measure, this results in $f(U) = f(\mathbb{1})$, and $\mathrm{Tr}\left(B^\dagger B\right)$ becomes

$$\begin{aligned}\int_{\mathcal{U}(d)}\int_{\mathcal{U}(d)} \left|\,\mathrm{Tr}\left(U^\dagger V\right)\right|^{2t} dV\,dU &= \int_{\mathcal{U}(d)} f(U)dU \\ &= f(\mathbb{1})\int_{\mathcal{U}(d)} dU \\ &= \int_{\mathcal{U}(d)} \left|\,\mathrm{Tr}\left(\mathbb{1}^\dagger V\right)\right|^{2t} dV \\ &= \int_{\mathcal{U}(d)} \left|\,\mathrm{Tr}(V)\right|^{2t} dV.\end{aligned} \tag{5.1.12}$$

The middle terms $\mathrm{Tr}\left(A^\dagger B\right)$ and $\mathrm{Tr}\left(B^\dagger A\right)$ are very similar, and so we will only show $\mathrm{Tr}\left(A^\dagger B\right)$, where again $V \in \mathcal{U}(d)$ is used in B.

$$\begin{aligned}\mathrm{Tr}\left(A^\dagger B\right) &= \mathrm{Tr}\left[\left(\sum_{k\in K} w(U_k) U_k^{\otimes t} \otimes (U_k^\dagger)^{\otimes t}\right)^\dagger \left(\int_{\mathcal{U}(d)} V^{\otimes t} \otimes (V^\dagger)^{\otimes t} dV\right)\right] \\ &= \sum_{k\in K} w(U_k) \int_{\mathcal{U}(d)} \left|\mathrm{Tr}\left(U_k^\dagger V\right)\right|^{2t} dV \\ &= \int_{\mathcal{U}(d)} \left|\,\mathrm{Tr}(V)\right|^{2t} dV,\end{aligned} \tag{5.1.13}$$

where the last equality comes from $\sum_{k\in K} w(U_k) = 1$ and using the same arguments as above for $\mathrm{Tr}\left(B^\dagger B\right)$.

Bringing everything together, we have

$$\begin{aligned}\mathrm{Tr}\left(D^\dagger D\right) = \sum_{k,\ell\in K} w(U_k)w(U_\ell) \left|\mathrm{Tr}\left(U_k^\dagger U_\ell\right)\right|^{2t} - \int_{\mathcal{U}(d)} \left|\,\mathrm{Tr}(V)\right|^{2t} dV \geq 0 \\ \sum_{k,\ell\in K} w(U_k)w(U_\ell) \left|\mathrm{Tr}\left(U_k^\dagger U_\ell\right)\right|^{2t} \geq \int_{\mathcal{U}(d)} \left|\,\mathrm{Tr}(V)\right|^{2t} dV,\end{aligned} \tag{5.1.14}$$

which is equal only when $D = 0$, which as we said in the beginning is true if and only if $\mathfrak{U}$ is a unitary t-design. ∎

The reason this is helpful is because the right hand side of Eq. (5.1.7) is easy to compute for certain d and t. It was shown by [DS94] and [Rai98] that $\int_{\mathcal{U}(d)} |\mathrm{Tr}(U)|^{2t}\, dU = t!$ when $d \geq t$, so this provides a convenient method of checking if a finite subset of unitaries is indeed a unitary t-design.

5.1.1 Examples of Exact Designs

One example of a unitary 1-design is the subset $\mathcal{P} = \{\mathbb{1}, X, Y, Z\}$ along with weights $w(U_k) = 1/4$. In other words, the set of Paulis is an unweighted unitary 1-design. This can be seen through the analysis of the quantum one-time pad in Section 4.1, which shows that when $\mathfrak{U} = (w, \mathcal{P})$ and $\rho \in \mathcal{D}(\mathcal{H}_2)$,

$$\mathop{\mathbb{E}}_{\mathfrak{U}}[U\rho U^\dagger] = \sum_{k\in K} w(U_k) \cdot U_k \rho U_k^\dagger = \frac{\mathbb{1}}{2} = \int_{\mathcal{U}(2)} U\rho U^\dagger dU. \tag{5.1.15}$$

This further explains why the set of Paulis makes a great encryption scheme when used once because they are a unitary 1-design, which this means that applying a single Pauli appears the same as applying a Haar-random unitary matrix.

The Clifford group are those matrices that when applied to Pauli matrices by conjugation produce Pauli matrices [Got98]. It has been shown that the Clifford group (containing 11,520 elements [DM14]) forms a 2-design and a 3-design, but not a 4-design [ZKGG16]. The proof showing that the Clifford group is a 2-design is presented in [DCEL09] and further explained in [DM14].

In [Sco08b] they provide an explicit example of an exact unitary 2-design, specifically a weighted projective unitary 2-design. A *projective unitary t-design* is similar to a unitary t-design, except instead of considering the whole unitary group, the projective unitary group $\mathcal{PU}(d) = \mathcal{U}(d)/\mathcal{U}(1)$ is used. This projective unitary group is composed of equivalence classes of the unitary group because each $e^{i\theta}U$ is identified with $U \in \mathcal{U}(d)$, where $e^{i\theta}$ are all complex numbers that have an absolute value of 1.

This weighted projective unitary 2-design has 11 elements which are composed from the Pauli matrices using the following formula:

$$e^{i\theta}U = r_0\mathbb{1} + i(r_1X + r_2Y + r_3Z), \tag{5.1.16}$$

where (r_0, r_1, r_2, r_3) is a unit vector in $\mathbb{R}^4$. Specifically, these unit vectors are the columns of Eq. (5.1.17), where the first column has weight $\frac{1}{16}$ and the remaining 10 columns have weight $\frac{3}{32}$.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ 0 & \frac{1}{\sqrt{3}} & \frac{-1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \sqrt{\frac{2}{3}} & \sqrt{\frac{-2}{3}} & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{-1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & 0 & 0 & \sqrt{\frac{2}{3}} & \sqrt{\frac{-2}{3}} & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{-1}{\sqrt{3}} & 0 & 0 & 0 & 0 & \sqrt{\frac{2}{3}} & \sqrt{\frac{-2}{3}} \end{bmatrix} \tag{5.1.17}$$

Equation (5.1.7) can be used to show that these 11 matrices do indeed form a weighted 2-design. This can be done easily by writing a code in Python to calculate $\sum_{k,\ell\in K} w(U_k)w(U_\ell)|\operatorname{Tr}\left(U_k^\dagger U_\ell\right)|^{2t}$, where k, ℓ specify the column of the matrix in

Eq. (5.1.17). This results in a summation of 121 elements, and evaluates in Python to $2 + 4.48774203859064 \times 10^{-29}i$. Equation (5.1.7) claims that if this summation is equal to $\int_{\mathcal{U}(d)} |\mathrm{Tr}(U)|^{2t}\, dU = t!$ when $d \geq t$, then $\mathfrak{U}$ is a unitary t-design. In this case, $d = t = 2$ and $t! = 2$, and therefore we have overwhelming evidence that these 11 elements with the corresponding weights are a unitary t-design.

5.2 Approximate Designs

The definitions presented thus far are for *exact* unitary t-designs. There are also what are called *approximate unitary t-designs*, which are similar to unitary t-designs except that instead of the expectation over all the unitaries being equal to the integral over the whole unitary group, their difference is less than or equal to some small variable ϵ.

Definition 5.2.1. Let $\{U_k\}_{k\in K}$ be a finite subset of $\mathcal{U}(d)$ and let $w : \{U_k\}_{k\in K} \to \mathbb{R}$ be a positive weight function such that $w(U_k) \geq 0$, $\sum_{k\in K} w(U_k) = 1$. Then $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ is called an *ϵ-approximate unitary t-design* if

$$\left\| \mathbb{E}_{\mathfrak{U}} \left[\mathcal{E}_{U_k}^{(t)} \right] - T^{(t)} \right\|_{1\to 1} < \epsilon, \tag{5.2.1}$$

where $T^{(t)}$ is the t-twirling channel $T^{(t)}(\rho) = \int_{\mathcal{U}(d)} U^{\otimes t} \rho (U^\dagger)^{\otimes t} dU$ and $\mathcal{E}_{U_k}^{(t)}(\rho) = U_k^{\otimes t} \rho (U_k^\dagger)^{\otimes t}$ for $\rho \in \mathcal{D}(\mathcal{H}_{d^t})$.

Note that there are other definitions of ϵ-approximate unitary t-designs depending on the norm used in Eq. (5.2.1) or a different norm comparing the left and right terms of Eq. (5.1.1). We use the $1 \to 1$ norm as it is the one needed for our specific application of quantum private broadcasting in Section 5.4.

There has been extensive work completed around approximate designs because unlike exact unitary t-designs, they have been shown to be generated efficiently [BHH16]. Specifically, they are able to be constructed with local random circuits that are polynomial in n (the number of qubits), t, and $\log(1/\epsilon)$. Further work has been completed to try and reduce the circuit depth needed for approximate designs, specifically [HM18, MGDM19, HMMH+20], building on the work of [BHH16].

The construction of approximate designs considered in this thesis are those from [LM20], where they prove an upper bound for when the unitaries are sampled from an exact t-design. The theorem that is of most interest to us is the following, which is theorem 3.1 from [LM20].

Theorem 5.2.2. *[LM20] Let $0 < \epsilon < 1$. Assume that the probability measure μ on $\mathcal{U}(d)$ is a t-design, and let $U_1, \ldots, U_n$ be sampled independently from μ. Then there exists a universal constant $C > 0$ such that, if $n \geq C(td)^t (t \log d)^6/\epsilon^2$, then with*

probability at least 1/2, we have

$$\forall\ \rho \in \mathcal{D}(d^t),\ \left\| \frac{1}{n}\sum_{i=1}^{n} U_i^{\otimes t}\rho(U_i^\dagger)^{\otimes t} - T^{(t)}(\rho) \right\|_\infty \leq \frac{\epsilon}{d^t} \tag{5.2.2}$$

Note that in Theorem 5.2.2, the probability measure μ is defined as a t-design, after which a finite number of unitaries are sampled from this measure. This is fundamentally the same as our unitary t-design definition with $\mathfrak{U} = (w, \{U_k\}_{k\in K})$, where we encompass this finite set of unitaries into our definition, and this weight function behaves as a probability measure. We have kept Theorem 5.2.2 as presented in [LM20] for completeness. Later in Chapter 6, we adapt this theorem when we discuss symmetric unitary t-designs.

5.3 Bounds for Designs

In this section, we recall previous results regarding lower and upper bounds for the size of weighted and unweighted unitary t-designs. We are concerned with these bounds because they determine how many unitaries are needed to generate a unitary t-design. We can then take the logarithm base 2 of these bounds to connect back to necessary key length for t-QPB, as seen in Fig. 5.1 and Fig. 5.2 in Section 5.5.

5.3.1 Lower Bounds

In [RS09], they provide lower and upper bounds for the sizes of weighted and unweighted unitary t-designs, which we now briefly explain.

They consider the vector space $\text{span}\{U^{\otimes k} \otimes (U^\dagger)^{\otimes \ell}\}$, whose dual space is the homogeneous polynomials of degree k in the entries of U and degree ℓ in the entries of $U^\dagger$, denoted $\text{Hom}(\mathcal{U}(d), k, \ell)$. This is because the dual space in this case is the linear maps that take matrices of the form $U^{\otimes k} \otimes (U^\dagger)^{\otimes \ell}$ to complex scalars. These maps are homogeneous degree 1 polynomials of the entries of $U^{\otimes k} \otimes (U^\dagger)^{\otimes \ell}$, whose entries are homogeneous monomials of degree k in the entries of U and degree ℓ in the entries of $U^\dagger$.

The dimension of a vector space and its dual space are the same, so Roy and Scott are able to determine the dimension of $\text{Hom}(\mathcal{U}(d), k, \ell)$, denoted $D(d, k, \ell)$, by finding the dimension of $\text{span}\{U^{\otimes k} \otimes (U^\dagger)^{\otimes \ell}\}$.

Relating this $D(d, k, \ell)$ back to unitary t-designs is done through the following theorem and proof from [RS09].

Theorem 5.3.1. *If $(w, \{U_k\}_{k\in K})$ is a unitary t-design, then*

$$|K| \geq D(d, \lceil t/2 \rceil, \lfloor t/2 \rfloor). \tag{5.3.1}$$

Proof: Since $(w, \{U_k\}_{k\in K})$ is a unitary t-design, this means it is true that for every $f \in \mathrm{Hom}(\mathcal{U}(d), t, t)$,

$$\sum_{k\in K} w(U_k) f(U_k) = \int_{\mathcal{U}(d)} f(U) dU.$$

To continue this proof, we need to consider the inner product for functions on $\mathcal{U}(d)$. For two functions f and g, this inner product corresponds to the average value of $\bar{f}g$, which is denoted

$$\langle f, g\rangle := \int_{\mathcal{U}(d)} \overline{f(U)} g(U) dU, \tag{5.3.2}$$

and $\langle f, g\rangle_{U_k}$ denotes the average value of $\bar{f}g$ over the subset $\{U_k\}_{k\in K}$. From the assumption that $(w, \{U_k\}_{k\in K})$ is a unitary t-design, this implies that $\langle f, g\rangle = \langle f, g\rangle_{U_k}$.

Now suppose that $S_1, \ldots, S_N$ is an orthonormal basis for $\mathrm{Hom}(\mathcal{U}(d), \lceil t/2\rceil, \lfloor t/2\rfloor)$. This means that the product $\bar{S}_i S_j$ is an element of $\mathrm{Hom}(\mathcal{U}(d), t, t)$. Using the average value, we can see that

$$\begin{aligned}
\langle S_i, S_j\rangle &= \int_{\mathcal{U}(d)} \bar{S}_i S_j dU \\
&= \int_{\mathcal{U}(d)} 1 \cdot \bar{S}_i S_j dU \\
&= \langle 1, \bar{S}_i S_j\rangle \\
&= \langle 1, \bar{S}_i S_j\rangle_{U_k} = \langle S_i, S_j\rangle_{U_k}.
\end{aligned} \tag{5.3.3}$$

From the assumption that $S_1, \ldots, S_N$ form an orthonormal basis, this implies they are orthogonal, and from the above equality, they are also orthogonal on $\{U_k\}_{k\in K}$ when one considers them as functions $S_i : \{U_k\}_{k\in K} \to \mathbb{C}$. The space of functions on this set $\{U_k\}_{k\in K}$ has dimension $|K|$, and since there are at least N independent orthogonal functions on this set, this implies

$$|K| \geq N = D(d, \lceil t/2\rceil, \lfloor t/2\rfloor).$$

∎

This theorem implies that for a unitary t-design $(w, \{U_k\}_{k\in K})$, we have the lower bound of $|K| \geq D(d, k, \ell)$ when $k + \ell = t$. It is known that there are $\binom{n+k-1}{k}$ independent homogeneous polynomials of degree k in n variables. This is from the result that says there are $\binom{n+k-1}{k}$ ways to select k objects from a set of size n with replacement [Sta11]. In this case, a spanning, independent set for homogeneous polynomials of degree k in n variables is the set of monomials of degree k in n variables. This degree k is composed from the combination of the n variables, and therefore simplifies to the task of selecting k variables (to have a monomial of degree k) from the total n variables, with replacement. To illustrate this further, consider the following example.

Example 5.3.2. Suppose we want to find how many monomials of degree 3 exist in 2 variables, say x and y. This corresponds to the following monomials

$$y^3,\ y^2x,\ yx^2,\ x^3, \tag{5.3.4}$$

and there are $\binom{2+3-1}{3} = \binom{4}{3} = 4$ such monomials.

Therefore, there are $\binom{n+k-1}{k}$ independent homogeneous polynomials of degree k in n variables. In our case, we want homogeneous polynomials of degree t in d^2 variables, since we are dealing with matrices in $\mathcal{U}(d)$, which have d^2 entries. We therefore have

$$|K| \geq D(d,t,0) = \binom{d^2+t-1}{t},$$

which is an element of $\Omega(t^{d^2-1})$ when d is fixed.

It is easy to see that $\mathrm{Hom}(\mathcal{U}(d),k,\ell)$ is able to be embedded into $\mathrm{Hom}(\mathcal{H}_{d^2},k,\ell)$ since these polynomials from the elements of $\mathcal{U}(d)$ have d^2 variables, which are contained in $\mathcal{H}_{d^2}$. This implies that an upper bound for $\dim(\mathrm{Hom}(\mathcal{H}_{d^2},k,\ell))$ gives an upper bound for $D(d,k,\ell)$, specifically,

$$D(d,k,\ell) \leq \binom{d^2+k-1}{k}\binom{d^2+\ell-1}{\ell}. \tag{5.3.5}$$

One particular example is that of unitary 2-designs. It has been shown by [GAE07] that the lower bound for unweighted unitary 2-designs is d^4-2d^2+2. Roy and Scott also come to this conclusion, which, following their notation, they denote as $D(d,1,1)$.

5.3.2 Upper Bounds

Roy and Scott provide an upper bound for weighted unitary t-designs, which is the following.

Theorem 5.3.3. *For any t and d, there exists a weighted unitary t-design $(w,\{U_k\}_{k\in K})$ with*

$$|K| \leq D(d,t,t) \leq \binom{d^2+t-1}{t}^2. \tag{5.3.6}$$

In [AMR20] they bring together results from [Kan15] and [RS09] to show an upper bound for unweighted unitary t-designs. The theorem of interest from [Kan15] is the following:

Theorem 5.3.4. *Let X be a homogeneous space, μ an invariant measure on X and W an M-dimensional vector subspace of the space of real functions on X that is invariant under the symmetry group of X, where $M>1$. Then for any $N>M(M-1)$, there exists a W-design for X of size N. Furthermore, there exists a design for X of size at most $M(M-1)$.*

The homogeneous space X in our case is $\mathcal{U}(d)$, which is acting on itself. This W is the vector space of $\mathrm{Hom}(\mathcal{U}(d), t, t)$. We know the dimension of this space from Roy and Scott,

$$M_t = D(d,t,t) \leq \binom{d^2+t-1}{t}^2 \leq \left(\frac{e(d^2+t-1)}{t}\right)^t.$$

Kane's theorem says there exists a design for X of size at most $M(M-1)$, so this leads to an upper bound of $\left(\frac{e(d^2+t-1)}{t}\right)^{2t}$ for unweighted unitary t-designs.

These lower and upper bounds are summarized in Table 5.1.

	Lower	**Upper**
Weighted	$\binom{d^2+t-1}{t} \in \Omega(t^{d^2-1})$ [RS09]	$\binom{d^2+t-1}{t}^2 \in O(t^{2(d^2-1)})$ [RS09]
Unweighted	$\binom{d^2+t-1}{t} \in \Omega(t^{d^2-1})$ [RS09]	$\left(\binom{d^2+t-1}{t}^2\right)^2 \leq \left(\frac{e(d^2+t-1)}{t}\right)^{2t}$ [AMR20]

Table 5.1: Unitary t-design Bounds

5.4 Unitary t-designs and t-QPB

Unitary t-designs have the property that U_k is applied t times, which we can use for t-QPB. As illustrated in Fig. 3.1 and explained in Section 3.2, the necessary requirement of independent decryption in t-QPB leads to a decryption operation which is a t-fold tensor product of a unitary matrix. Defining the encryption map as $U_k^{\otimes t}\rho(U_k^{\otimes t})^\dagger$, this allows us to use unitary t-designs as t-QPB encryption schemes, as the resulting decrypting operation is the t-fold tensor product of a unitary matrix. We formalize this in the following theorem.

Theorem 5.4.1. *Let $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ be an ϵ-approximate unitary t-design. Then the set of maps $\mathsf{Enc}_k(\rho) = U_k^{\otimes t}\rho(U_k^{\otimes t})^\dagger$ and its inverse maps $\mathsf{Dec}_k(\gamma) = U_k^\dagger \gamma U_k$ for $k \in K$, $\rho \in \mathcal{D}(Sym(d^t))$ and $\gamma \in \mathcal{D}(\mathcal{H}_d)$ form a perfect t-QPB which has ϵ-indistinguishable ciphertexts. Moreover, in the case of exact unitary t-designs, we have a perfect t-QPB perfectly secure against adversaries with side information.*

Proof: The fact that Enc_k and $\mathsf{Dec}_k^{\otimes t}$ are inverses of each other automatically shows correctness, and implies that the encrypting and decrypting maps form a perfect t-QPB. Denote $T^{(t)}$ the t-twirling channel $T^{(t)}(\rho) = \int_{\mathcal{U}(d)} U^{\otimes t}\rho(U^\dagger)^{\otimes t}dU$. For $\rho \in \mathcal{D}(\mathrm{Sym}(d^t))$, $T^{(t)}(\rho) = \tau_{\mathrm{Sym}}$, that is, $T^{(t)}|_{\mathrm{Sym}(d^t)} = \langle\tau_{\mathrm{Sym}}\rangle|_{\mathrm{Sym}(d^t)}$. Using Definition 5.2.1 we get

$$\left\| \left(\mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k - \langle \tau_{\mathrm{Sym}} \rangle \right) \Big|_{\mathrm{Sym}(d^t)} \right\|_{1\to 1} = \left\| \left(\mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k - T^{(t)} \right) \Big|_{\mathrm{Sym}(d^t)} \right\|_{1\to 1} \leq \left\| \mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k - T^{(t)} \right\|_{1\to 1} < \epsilon.$$

This shows that ϵ-approximate unitary t-designs have ϵ-indistinguishable ciphertexts when used as encryption schemes, and this extends to being perfectly secure when the design is an exact unitary t-design.

Consider now the security against side information for the case of exact unitary t-designs. Suppose the plaintext to be encrypted is $|\psi\rangle \in \mathcal{H}_A \otimes \mathrm{Sym}(d^t)$, which can be written as

$$\begin{aligned} |\psi\rangle &= \sum_{i=1}^{D} \lambda_i |a_i\rangle \otimes |\varphi_i\rangle \\ |\psi\rangle\langle\psi| &= \sum_i \sum_j \lambda_i \lambda_j^* |a_i\rangle\langle a_j| \otimes |\varphi_i\rangle\langle\varphi_j| \end{aligned} \tag{5.4.1}$$

using the Schmidt decomposition, where $|a_i\rangle$ and $|\varphi_i\rangle$ are orthonormal states for $\mathcal{H}_A$ and $\mathrm{Sym}(d^t)$, respectively. The λ_i values are non-negative real numbers such that $\sum_i \lambda_i^2 = 1$.

Applying $\mathbb{1}_A \otimes \mathsf{Enc}_k$ to $|\psi\rangle\langle\psi|$ and taking the expectation gives

$$\begin{aligned} &\sum_i \sum_j \lambda_i \lambda_j^* |a_i\rangle\langle a_j| \otimes \sum_{k\in K} w(U_k) U_k^{\otimes t} |\varphi_i\rangle\langle\varphi_j| (U_k^\dagger)^{\otimes t} \\ &= \sum_i \sum_j \lambda_i \lambda_j^* |a_i\rangle\langle a_j| \otimes \int_{\mathcal{U}(d)} U^{\otimes t} |\varphi_i\rangle\langle\varphi_j| (U^\dagger)^{\otimes t} dU \\ &= \sum_i \sum_j \lambda_i \lambda_j^* |a_i\rangle\langle a_j| \otimes \Big(\mathrm{Tr}(\Pi_{\mathrm{Sym}} |\varphi_i\rangle\langle\varphi_j| \Pi_{\mathrm{Sym}}) \tau_{\mathrm{Sym}} + \sum_b \mathrm{Tr}(\Pi_b |\varphi_i\rangle\langle\varphi_j| \Pi_b) \tau_b \Big). \end{aligned} \tag{5.4.2}$$

The second equality follows from Eq. (2.10.1), whose notation is explained in Section 2.10. This $\mathrm{Tr}(\Pi_{\mathrm{Sym}} |\varphi_i\rangle\langle\varphi_j| \Pi_{\mathrm{Sym}}) = \langle\varphi_j|\Pi_{\mathrm{Sym}}\Pi_{\mathrm{Sym}}|\varphi_i\rangle$ equals 0 when $i \neq j$ since $|\varphi_i\rangle$ and $|\varphi_j\rangle$ are orthonormal. For $\mathrm{Tr}(\Pi_b |\varphi_i\rangle\langle\varphi_j| \Pi_b)$, this always equals zero because $|\varphi_i\rangle, |\varphi_j\rangle \in \mathrm{Sym}(d^t)$ which is orthogonal to subspace b, and so Π_b applied to these states gives zero. Therefore the only terms that remain are when $i = j$, which gives

$$\begin{aligned} &\sum_i |\lambda_i|^2 |a_i\rangle\langle a_i| \otimes \int_{\mathcal{U}(d)} U^{\otimes t} |\varphi_i\rangle\langle\varphi_i| (U^\dagger)^{\otimes t} dU \\ &= \sum_i |\lambda_i|^2 |a_i\rangle\langle a_i| \otimes \tau_{\mathrm{Sym}}, \end{aligned} \tag{5.4.3}$$

and this τ_{Sym} is independent of b. This implies that the encrypted plaintext always looks the same, regardless of what the adversary has as side information. This implies

$$\left\| \left(\mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k - \langle \tau_{\text{Sym}} \rangle \right) \Big|_{\text{Sym}(d^t)} \right\|_\diamond = 0$$

∎

Notice that we restricted ρ to being a density operator over the symmetric subspace $\text{Sym}(d^t)$. The reason for this is to obtain perfect security, both with and without side information. As we show below, if ρ is only permutationally symmetric, (i.e. when the different qudits of ρ are permuted, this does not change ρ), unitary t-designs no longer have perfect security.

Theorem 5.4.2. *Quantum Private Broadcasting with designs for t-recipients fails to be perfectly secure with a generalized version of security following Definition 3.2.2 when used to broadcast quantum states of the form $\nu^{\otimes t} \notin \mathcal{D}(Sym(d^t))$.*

Proof: Consider for example, the totally mixed state $\tau = \frac{\mathbb{1}}{2} \otimes \frac{\mathbb{1}}{2} \in \mathcal{D}(\mathcal{H}_{d^t})$ for $d = t = 2$. The averaged encryption of τ is

$$\mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k(\tau) = \sum_{k\in K} w(U_k) U_k \otimes U_k \left(\frac{\mathbb{1}}{4}\right) U_k^\dagger \otimes U_k^\dagger = \frac{1}{4} \sum_{k\in K} w(U_k)(U_k \otimes U_k)\mathbb{1}(U_k^\dagger \otimes U_k^\dagger) = \frac{\mathbb{1}}{4} = \tau, \tag{5.4.4}$$

since $(U_k \otimes U_k)\mathbb{1}(U_k^\dagger \otimes U_k^\dagger) = \mathbb{1}$ and $\sum_{k\in K} w(U_k) = 1$. On the other hand, any state $\rho_0 \in \mathcal{D}(\text{Sym}(2^2))$ is mapped to $\mathbb{E}_{k\in K}\mathsf{Enc}_k(\rho_0) = \tau_{\text{Sym}}$, the maximally mixed state in the symmetric subspace. Clearly $\frac{\mathbb{1}}{4} \neq \tau_{\text{Sym}}$ because when $d = t = 2$,

$$\begin{aligned} \tau_{\text{Sym}} &= \frac{\Pi_{\text{Sym}}}{d_{\text{Sym}}} \\ &= \frac{\Pi_{\text{Sym}}}{3} \neq \frac{\mathbb{1}}{4}, \end{aligned} \tag{5.4.5}$$

and for any state replacement channel $\langle \sigma \rangle$,

$$\begin{aligned} \left\| \left(\mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k - \langle \sigma \rangle \right) \right\|_{1\to 1} &= \max_{\rho \in \mathcal{D}(\mathbb{C}(2^2))} \left\| \mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k(\rho) - \langle \sigma \rangle(\rho) \right\|_1 \\ &\geq \frac{1}{2} \left(\left\| \mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k(\tau) - \langle \sigma \rangle(\tau) \right\|_1 + \left\| \mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k(\rho_0) - \langle \sigma \rangle(\rho_0) \right\|_1 \right) \\ &\geq \frac{1}{2} \left(\left\| \mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k(\tau) - \mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k(\rho_0) \right\|_1 \right) \\ &\geq \frac{1}{2} \left\| \tau - \tau_{\text{Sym}} \right\|_1 \geq \frac{1}{4}. \end{aligned}$$

This does not fulfill the definition of perfect security with respect to a generalized version of security following Definition 3.2.2, and therefore supports why we restrict our input to the symmetric subspace in the definitions of security and correctness for t-QPB. ∎

Furthermore, we can insert a pre-broadcasting stage into the t-QPB where we perform a projective measurement $\{\tau_{\text{Sym}}, \mathbb{1} - \tau_{\text{Sym}}\}$ to determine whether or not our state is in the symmetric subspace. The state provided by an adversary is either projected into the symmetric subspace, whose action leaves symmetric states unchanged, or it is projected into a subspace orthogonal to the symmetric subspace. In the first case, the state is symmetric and the t-QPB is secure, as explained above. In the second case, the projective measurement result indicates that the state is not symmetric, and the encryption protocol is aborted, thus avoiding scenarios where the t-QPB is not secure.

To illustrate further why inputs need to be in the symmetric subspace, we consider the following example.

Example 5.4.3. Suppose the first half of two EPR pairs is the message to be encrypted with a unitary 2-design. The corresponding quantum state and density operator are

$$\begin{aligned} |EPR_2\rangle &= \frac{1}{\sqrt{2^2}} \sum_{q\in\{0,1\}^2} |q\rangle_M |q\rangle_E \\ &= \frac{1}{2}\Big(|00\rangle_M |00\rangle_E + |01\rangle_M |01\rangle_E + |10\rangle_M |10\rangle_E + |11\rangle_M |11\rangle_E \Big) \end{aligned} \tag{5.4.6}$$

and

$$\begin{aligned} \rho_{ME} = |EPR_2\rangle\langle EPR_2| &= \Big(\frac{1}{\sqrt{2^2}} \sum_{q\in\{0,1\}^2} |q\rangle_M |q\rangle_E\Big)\Big(\frac{1}{\sqrt{2^2}} \sum_{r\in\{0,1\}^2} \langle r|_M \langle r|_E\Big) \\ &= \frac{1}{4} \sum_{r,q\in\{0,1\}^2} |q\rangle\langle r|_M \otimes |q\rangle\langle r|_E \,. \end{aligned} \tag{5.4.7}$$

Note that since the elements of $\mathcal{D}(\text{Sym}(d^t))$ are in $\text{span}_{\mathbb{R}}\{(|\varphi\rangle\langle\varphi|)^{\otimes t} : |\varphi\rangle \in \mathcal{H}_d\}$, the density operator corresponding to the first half of two EPR pairs is *not* a density operator in the symmetric subspace. This is because when $q \neq r$, this cannot be written as $|\varphi\rangle\langle\varphi|$.

We look at two scenarios,

1. $(\mathbb{E}_{k\in K}\, \mathsf{Enc}_k(|0\rangle\langle 0| \otimes |0\rangle\langle 0|)) \otimes \rho_E$
2. $(\mathbb{E}_{k\in K}\, \mathsf{Enc}_k \otimes \mathbb{1}_E)\, \rho_{ME}$,

where Enc_k is the encryption scheme using unitary t-designs, which in this case is a unitary 2-design. We are able to make the following claim.

Lemma 5.4.4. *It is possible to distinguish between the averaged encrypted outputs of ρ_{ME} and $|0\rangle\langle 0| \otimes |0\rangle\langle 0| \otimes \rho_E$, which implies that a unitary 2-design is not perfectly secure when used to encrypt elements that are not in the symmetric subspace.*

Proof: To simplify the averaged encryption of $|0\rangle\langle 0| \otimes |0\rangle\langle 0| \otimes \rho_E$, we calculate the partial trace, which gives

$$\begin{aligned} \mathrm{Tr}_M |EPR_2\rangle\langle EPR_2| &= \frac{1}{4} \sum_{r,q\in\{0,1\}^2} \mathrm{Tr}(|q\rangle\langle r|_M) \otimes |q\rangle\langle r|_S \\ &= \frac{1}{4} \sum_{r,q\in\{0,1\}^2} \langle r|q\rangle_M \otimes |q\rangle\langle r|_S \\ &= \frac{1}{4} \sum_{q\in\{0,1\}^2} |q\rangle\langle q|_S \\ &= \frac{1}{4}\mathbb{I} \end{aligned} \tag{5.4.8}$$

since $\langle r|q\rangle = 1$ only when $q = r$ and is zero otherwise.

This first scenario becomes

$$\begin{aligned} \left(\mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k(|0\rangle\langle 0| \otimes |0\rangle\langle 0|) \right) \otimes \rho_E &= \sum_{k\in K} w(U_k) U_k \otimes U_k(|0\rangle\langle 0| \otimes |0\rangle\langle 0|)(U_k \otimes U_k)^\dagger \otimes \frac{\mathbb{1}}{4} \\ &= \int_{\mathcal{U}(d)} U \otimes U(|0\rangle\langle 0| \otimes |0\rangle\langle 0|)(U \otimes U)^\dagger \otimes \frac{\mathbb{1}}{4} dU, \end{aligned} \tag{5.4.9}$$

while the second scenario is

$$\begin{aligned} \left(\mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k \otimes \mathbb{1}_E \right) \rho_{ME} &= \sum_{k\in K} w(U_k)(U_k \otimes U_k \otimes \mathbb{1}_E)\rho_{ME}(U_k \otimes U_k \otimes \mathbb{1}_E)^\dagger \\ &= \int_{\mathcal{U}(d)} (U \otimes U \otimes \mathbb{1}_E)\rho_{ME}(U \otimes U \otimes \mathbb{1}_E)^\dagger dU. \end{aligned} \tag{5.4.10}$$

Naturally, Eq. (5.4.10) results in more terms within the integral than Eq. (5.4.9) because of the case when $q \neq r$. Since ρ_{ME} is a summation of terms within the integral over the unitary group, we can write this as a summation of integrals. To condense the terms, we use the result from Benoît Collins in [Col03], further explained in [CS06] with Piotr Śniady. This result says that when n is a positive integer and there are

n-tuples of positive integers $\mathbf{i} = (i_1, \ldots, i_n)$, $\mathbf{j} = (j_1, \ldots, j_n)$, $\mathbf{k} = (k_1, \ldots, k_n)$, and $\boldsymbol{\ell} = (\ell_1, \ldots, \ell_n)$, then

$$\int_{\mathcal{U}(d)} U_{i_1 j_1} \cdots U_{i_n j_n} \bar{U}_{k_1 \ell_1} \cdots \bar{U}_{k_n \ell_n} dU = \sum_{\sigma,\tau \in S_n} \delta_{i_1 k_{\sigma(1)}} \cdots \delta_{i_n k_{\sigma(n)}} \delta_{j_1 \ell_{\tau(1)}} \cdots \delta_{j_n \ell_{\tau(n)}} Wg(\tau\sigma^{-1}). \tag{5.4.11}$$

Here, S_n is the permutation group, δ_{ij} is the usual Kronecker delta, the integral is over the unitary group with respect to the Haar measure, and Wg is the Weingarten function. This Weingarten function has a precise definition, but all we need from Eq. (5.4.11) is the conclusion from the delta function.

In order for the delta terms to be non-zero, it needs to be true that $i_a = k_{\sigma(a)}$ and $j_b = \ell_{\tau(b)}$ for $a, b \in \{1, \ldots, n\}$. This means that when $\mathbf{k}$ is permuted according to σ, $\mathbf{k} = \mathbf{i}$ and likewise for $\boldsymbol{\ell}$ and $\mathbf{j}$ with τ. In other words, $\mathbf{k}$ is a permutation of $\mathbf{i}$ and $\boldsymbol{\ell}$ is a permutation of $\mathbf{j}$.

To use Collins' result, we need to look at the specific elements of U, which can be done by $\langle i|U|j\rangle = U_{ij}$. As the encryption is of the form $U \otimes U$, this implies that

$$\begin{aligned} \langle i_1 i_2| (U \otimes U) |q_1 q_2\rangle\langle r_1 r_2| (U \otimes U)^\dagger |j_1 j_2\rangle &= U_{i_1 q_1} U_{i_2 q_2} U^\dagger_{r_1 j_1} U^\dagger_{r_2 j_2} \\ &= U_{i_1 q_1} U_{i_2 q_2} \bar{U}_{j_1 r_1} \bar{U}_{j_2 r_2}. \end{aligned} \tag{5.4.12}$$

By Collins' result, the terms where $q_1 q_2$ is not a permutation of $r_1 r_2$ are zero. The terms that remain are

$$\begin{aligned} \frac{1}{4}\Big(&\int_{\mathcal{U}(d)} U \otimes U(|00\rangle\langle 00|)(U \otimes U)^\dagger \otimes |00\rangle\langle 00|\, dU + \int_{\mathcal{U}(d)} U \otimes U(|01\rangle\langle 01|)(U \otimes U)^\dagger \otimes |01\rangle\langle 01|\, dU \\ &+ \int_{\mathcal{U}(d)} U \otimes U(|01\rangle\langle 10|)(U \otimes U)^\dagger \otimes |01\rangle\langle 10|\, dU + \int_{\mathcal{U}(d)} U \otimes U(|10\rangle\langle 01|)(U \otimes U)^\dagger \otimes |10\rangle\langle 01|\, dU \\ &+ \int_{\mathcal{U}(d)} U \otimes U(|10\rangle\langle 10|)(U \otimes U)^\dagger \otimes |10\rangle\langle 10|\, dU + \int_{\mathcal{U}(d)} U \otimes U(|11\rangle\langle 11|)(U \otimes U)^\dagger \otimes |11\rangle\langle 11|\, dU \Big). \end{aligned} \tag{5.4.13}$$

The invariance of the Haar measure to left and right multiplication implies that the Pauli X can be applied to certain terms in Eq. (5.4.13) with the goal of factoring common terms together.

$$
\begin{aligned}
&\frac{1}{4}\Big(\int_{\mathcal{U}(d)} U\otimes U(|00\rangle\langle 00|)(U\otimes U)^\dagger\otimes|00\rangle\langle 00|\,dU+\int_{\mathcal{U}(d)} U\otimes U(|01\rangle\langle 01|)(U\otimes U)^\dagger\otimes|01\rangle\langle 01|\,dU\\
&\quad+\int_{\mathcal{U}(d)} U\otimes U(|01\rangle\langle 10|)(U\otimes U)^\dagger\otimes|01\rangle\langle 10|\,dU\\
&\quad+\int_{\mathcal{U}(d)} UX\otimes UX(|10\rangle\langle 01|)(UX\otimes UX)^\dagger\otimes|10\rangle\langle 01|\,dU\\
&\quad+\int_{\mathcal{U}(d)} UX\otimes UX(|10\rangle\langle 10|)(UX\otimes UX)^\dagger\otimes|10\rangle\langle 10|\,dU\\
&\quad+\int_{\mathcal{U}(d)} UX\otimes UX(|11\rangle\langle 11|)(UX\otimes UX)^\dagger\otimes|11\rangle\langle 11|\,dU\Big)\\
&=\frac{1}{4}\Big(\int_{\mathcal{U}(d)} U\otimes U(|00\rangle\langle 00|)(U\otimes U)^\dagger\otimes|00\rangle\langle 00|\,dU+\int_{\mathcal{U}(d)} U\otimes U(|01\rangle\langle 01|)(U\otimes U)^\dagger\otimes|01\rangle\langle 01|\,dU\\
&\quad+\int_{\mathcal{U}(d)} U\otimes U(|01\rangle\langle 10|)(U\otimes U)^\dagger\otimes|01\rangle\langle 10|\,dU+\int_{\mathcal{U}(d)} U\otimes U(|01\rangle\langle 10|)(U\otimes U)^\dagger\otimes|10\rangle\langle 01|\,dU\\
&\quad+\int_{\mathcal{U}(d)} U\otimes U(|01\rangle\langle 01|)(U\otimes U)^\dagger\otimes|10\rangle\langle 10|\,dU+\int_{\mathcal{U}(d)} U\otimes U(|00\rangle\langle 00|)(U\otimes U)^\dagger\otimes|11\rangle\langle 11|\,dU\Big)\\
&=\frac{1}{4}\Big(\int_{\mathcal{U}(d)} U\otimes U(|00\rangle\langle 00|)(U\otimes U)^\dagger\otimes(|00\rangle\langle 00|+|11\rangle\langle 11|)dU\\
&\quad+\int_{\mathcal{U}(d)} U\otimes U(|01\rangle\langle 01|)(U\otimes U)^\dagger\otimes(|01\rangle\langle 01|+|10\rangle\langle 10|)dU\\
&\quad+\int_{\mathcal{U}(d)} U\otimes U(|01\rangle\langle 10|)(U\otimes U)^\dagger\otimes(|01\rangle\langle 10|+|10\rangle\langle 01|)dU\Big).
\end{aligned}
\tag{5.4.14}
$$

Now to simplify even further, we use a fact about integrals of the above form, as stated in [LM20]. If L is a linear operator on $\mathcal{H}_{2^2}$, then $\int_{\mathcal{U}(2)}(U\otimes U)L(U\otimes U)^\dagger dU$ can be written explicitly as

$$
T^{(2)}(X)=\frac{1}{3}\operatorname{Tr}\big(P_{\wedge^2(2)}LP_{\wedge^2(2)}\big)P_{\wedge^2(2)}+\operatorname{Tr}\big(P_{\vee^2(2)}LP_{\vee^2(2)}\big)P_{\vee^2(2)},
\tag{5.4.15}
$$

where $P_{\wedge^2(2)}$ is the projector onto the symmetric subspace and $P_{\vee^2(2)}$ is the projector onto the antisymmetric subspace of $\mathcal{H}_{2^2}$. In [LM20] they define these projectors as

$$
\begin{aligned}
P_{\wedge^2(2)}&=\frac{\mathbb{1}+F}{2}\\
P_{\vee^2(2)}&=\frac{\mathbb{1}-F}{2}
\end{aligned}
\tag{5.4.16}
$$

where F is the flip operator, also known as the SWAP operator. Explicitly, these are

$$F = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad P_{\wedge^2(2)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/2 & 1/2 & 0 \\ 0 & 1/2 & 1/2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad P_{\vee^2(2)} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1/2 & -1/2 & 0 \\ 0 & -1/2 & 1/2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{5.4.17}$$

Using this simplification, Eq. (5.4.9) is

$$\rho_0 = \frac{1}{3} P_{\wedge^2(2)} \otimes \frac{\mathbb{I}}{4}, \tag{5.4.18}$$

and Eq. (5.4.10) is

$$\begin{aligned} \rho_1 = \frac{1}{4} \Bigg(& \frac{1}{3} P_{\wedge^2(2)} \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|) + \left(\frac{1}{6} P_{\wedge^2(2)} + \frac{1}{2} P_{\vee^2(2)} \right) \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|) \\ & + \left(\frac{1}{6} P_{\wedge^2(2)} - \frac{1}{2} P_{\vee^2(2)} \right) \otimes (|01\rangle\langle 10| + |10\rangle\langle 01|) \Bigg). \end{aligned} \tag{5.4.19}$$

These two outputs are distinguishable, seen through direct calculation of the trace distance. This calculation is cumbersome, and so instead we examine a particular projective measurement and strategy to conclude that ρ_0 and ρ_1 are distinguishable.

Suppose there are two parties, Alice and Bob, who play the following game. Bob prepares ρ_{ME}, sending the first two halves to Alice to encrypt with Enc_k. She randomly decides whether to encrypt this quantum state or $|0\rangle\langle 0| \otimes |0\rangle\langle 0|$, sending the encrypted output to Bob, who must then determine which quantum state Alice encrypted. If this encryption schemes yields indistinguishable ciphertexts, then Bob should not be able to distinguish between ρ_0 and ρ_1 with probability greater than $1/2$, i.e. simply guessing which quantum state Alice encrypted. We show that there exists a strategy that allows Bob to win this game with probability greater than $1/2$, which implies that Enc_k does not result in indistinguishable ciphertexts.

Let Bob's projective measurement be

$$\begin{aligned} \Big\{ & P_{\vee^2(2)} \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|), P_{\vee^2(2)} \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|), \\ & P_{\wedge^2(2)} \otimes (|00\rangle\langle 00| + |11\rangle\langle 11|), P_{\wedge^2(2)} \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|) \Big\}. \end{aligned} \tag{5.4.20}$$

The elements sum to the identity and they are positive operators, so this is a valid measurement. Labelling these four elements as A, B, C, D and taking the trace of the projective measurement, one can find the observation probability.

	ρ_0	ρ_1
A	0	0
B	0	1/4
C	1/2	1/2
D	1/2	1/4

Table 5.2: Counterexample Measurement Outcomes

Using the strategy where Bob guesses ρ_1 if he sees $P_{\vee^2(2)}$ and ρ_0 if he sees $P_{\wedge^2(2)}$, this leads to a total success probability of $\frac{1}{2} \cdot \frac{1}{4} + \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{5}{8} > \frac{1}{2}$.

Therefore, it is possible to distinguish between ρ_0 and ρ_1, which implies a unitary 2-design is not perfectly secure as a 2-QPB when its input is not from the symmetric subspace. ∎

5.5 Comparison with QOTP

Comparing the upper bounds of weighted and unweighted unitary t-designs with those of the quantum one-time pad, we can generate the following graphs. Figure 5.1 compares the QOTP with weighted designs while Fig. 5.2 compares both weighted and unweighted designs with the QOTP. These calculations were made taking $d = 2$ and letting t vary in Table 4.1 and the upper bounds in Table 5.1. This calculates the number of unitaries needed, which is translated to the necessary key length by taking the log base 2 of these results. The specific values are listed in Appendix B. Note that we used the asymptotic upper bounds for these graphs. For the unweighted t-design upper bound, we used $\binom{d^2+t-1}{t}^4$ as mentioned below Theorem 5.3.4 since d and t are reasonably small. Unweighted t-designs have been discovered for $t = 1, 2, 3$, as explained in Section 5.1.1, which are denoted by single points in the graph.

One can see that when t is greater than 6, weighted unitary t-designs require less classical bits than the QOTP, while it takes until t is greater than 22 for unweighted unitary t-designs to surpass the QOTP.

The question now is whether there is another encryption scheme for t-QPB that needs even fewer classical bits than weighted unitary t-designs. We are able to answer in the affirmative by creating a new concept we call *symmetric unitary t-designs*, which make use of the input restriction to the symmetric subspace and are a relaxation of unitary t-designs on the symmetric subspace. We provide formal definitions and bounds in Chapter 6, ending with a comparison of how these symmetric t-designs fare against the QOTP and weighted unitary t-designs.

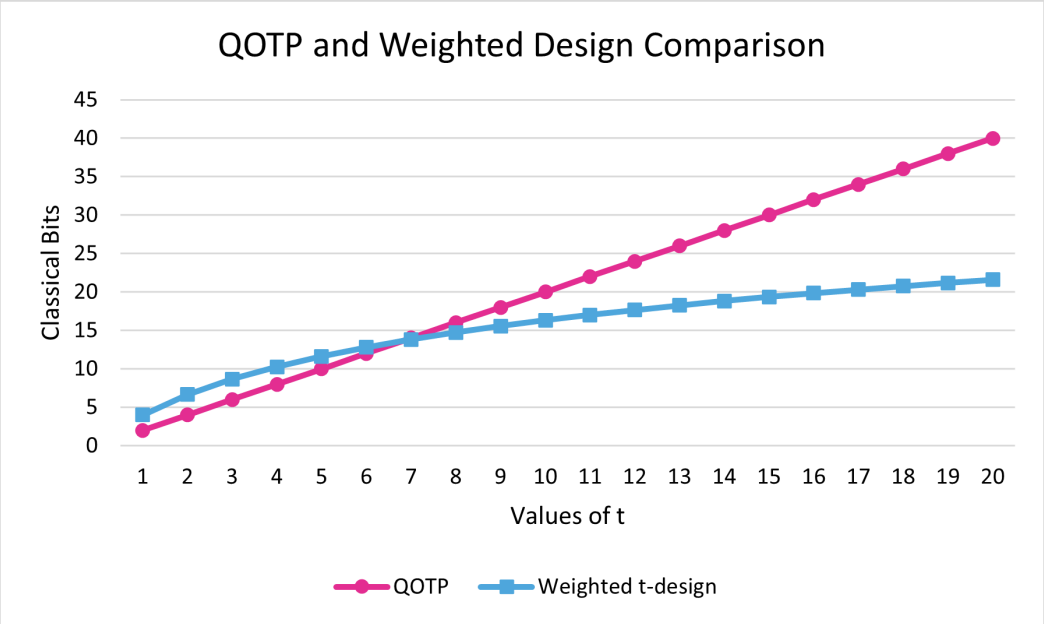

Figure 5.1: QOTP & Weighted t-design, $t \leq 20$, $d = 2$

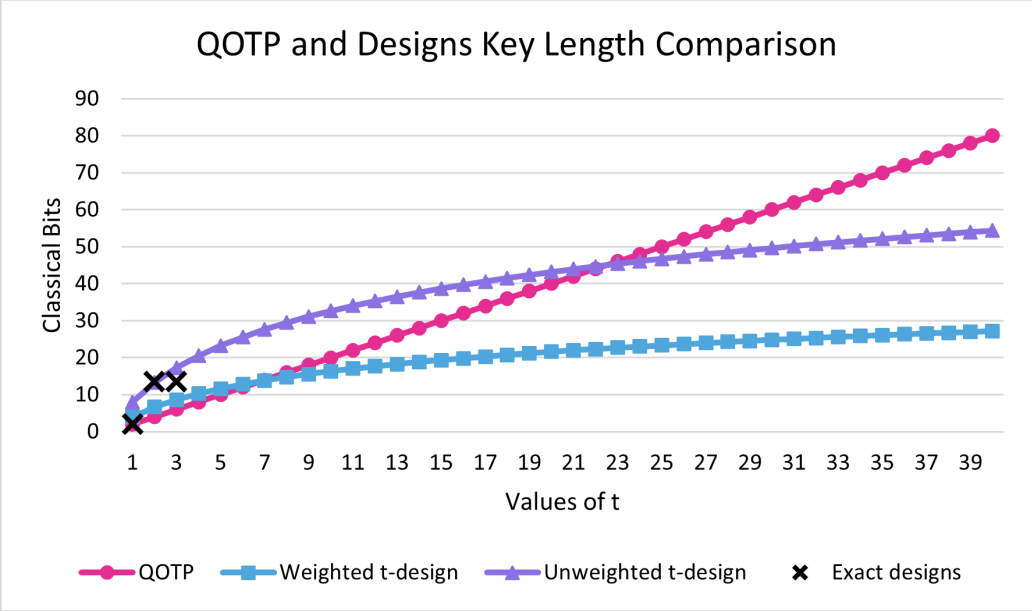

Figure 5.2: QOTP, Weighted t-design & Unweighted t-design, $t \leq 40$, $d = 2$

Chapter 6

Symmetric Unitary t-designs

This chapter introduces our new concept of symmetric unitary t-designs, which are a relaxation of unitary t-designs. We explain how these symmetric unitary t-designs provide another solution to the t-QPB problem, a natural conclusion resulting from our input quantum state being restricted to the symmetric subspace. We provide lower and upper bounds for exact and approximate weighted symmetric unitary t-designs, and compare the resulting key length for t-QPB with those of the quantum one-time pad and regular unitary t-designs. This chapter is composed of original contributions, as presented in [BGGS21].

6.1 Symmetric Unitary t-designs and t-QPB

As mentioned in Section 5.4, in order for unitary t-designs to be secure encryption schemes for t-QPB, we restrict our input message to be an element of the symmetric subspace. Applying $U^{\otimes t}$ to this input keeps everything in the symmetric subspace $\mathrm{Sym}(d^t)$, and therefore we are only working in the symmetric subspace. Motivated by this fact, we propose the new concept of symmetric unitary t-designs, which are a relaxation of unitary t-designs. Namely, they are a discrete set of unitaries together with a probability distribution that mimics the action of the Haar measure *in the symmetric subspace*. The reason they are relaxations of unitary t-designs is because every unitary t-design is also a symmetric unitary t-design, while the converse is not necessarily true. This is because the definition of unitary t-designs holds for any $\rho \in \mathcal{D}(\mathcal{H}_d^{\otimes t})$, which includes $\sigma \in \mathcal{D}(\mathrm{Sym}(d^t))$. The converse is not necessarily true, where a symmetric unitary t-design only satisfies the properties of a t-design for inputs $\sigma \in \mathcal{D}(\mathrm{Sym}(d^t))$ and fails for $\rho \in \mathcal{D}(\mathcal{H}_d^{\otimes t}) \setminus \mathcal{D}(\mathrm{Sym}(d^t))$. We now present the formal definition for symmetric unitary t-designs and how these symmetric designs relate to t-recipient Quantum Private Broadcasting. We then move on to explaining the lower and upper bounds associated with symmetric unitary t-designs.

Definition 6.1.1. Let $\{U_k\}_{k\in K}$ be a finite subset of $\mathcal{U}(d)$ and let $w : \{U_k\}_{k\in K} \to \mathbb{R}$ be a positive weight function such that $w(U_k) \geq 0$ and $\sum_{k\in K} w(U_k) = 1$. Then $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ is called an *ϵ-approximate symmetric unitary t-design* if

$$\left\| \left(\mathbb{E}_{\mathfrak{U}} \left[\mathcal{E}_{U_k}^{(t)} \right] - \langle \tau_{\mathrm{Sym}} \rangle \right) \Big|_{\mathrm{Sym}(d^t)} \right\|_{1\to 1} < \epsilon, \tag{6.1.1}$$

where $\mathcal{E}_{U_k}^{(t)}(\rho) = U_k^{\otimes t} \rho (U_k^\dagger)^{\otimes t}$.

Note that $\langle \tau_{\mathrm{Sym}} \rangle$ is equal to $T^{(t)}$, the t-twirling channel $T^{(t)}(\rho) = \int_{\mathcal{U}(d)} U^{\otimes t} \rho (U^\dagger)^{\otimes t} dU$, for symmetric states $\rho \in \mathcal{D}(\mathrm{Sym}(d^t))$ and the integral is over the whole unitary group with respect to the Haar measure.

We now connect these symmetric unitary t-designs with perfect t-QPB schemes.

Corollary 6.1.2. *Let $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ be an ϵ-approximate symmetric unitary t-design. Then the set of maps $\mathsf{Enc}_k(\rho) = U_k^{\otimes t} \rho (U_k^{\otimes t})^\dagger$ and its inverse maps $\mathsf{Dec}_k(\rho) = (U_k^{\otimes t})^\dagger \rho U_k^{\otimes t}$ for $k \in K$ and $\rho \in \mathcal{D}(Sym(d^t))$ form a perfect t-QPB which has ϵ-indistinguishable ciphertexts. Moreover, in the case of exact symmetric unitary t-designs, we have a perfect t-QPB perfectly secure against adversaries with side information.*

Proof: Note that the only properties of approximate or exact unitary t-designs we are using in the proof of Theorem 5.4.1 are those that are also fulfilled by symmetric unitary t-designs. Therefore, the same proof can be used here. ∎

Corollary 6.1.2 shows that symmetric unitary t-designs provide perfect t-QPB schemes. Furthermore, perfect t-QPB must be implemented via unitary matrices with local decryption matrices $U_k^\dagger$. Encryption can be performed with a general unitary, but looking at its action over the symmetric subspace, it is exactly the same as $(U_k)^{\otimes t}$. Therefore, it is also true that every perfect t-QPB comes from a symmetric unitary t-design.

Hence, Lemma 3.2.3 can be rephrased in terms of symmetric unitary t-designs.

Lemma 6.1.3. *Let $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ be a symmetric unitary t-design, then $\mathfrak{U}$ is a symmetric unitary $(t-1)$-design.*

We are able to prove lower and upper bounds for symmetric unitary t-designs (Lemma 6.1.4 and Lemma 6.1.5, respectively) by using the connections between regular unitary t-designs and symmetric unitary t-designs. The lower bounds correspond to both weighted and unweighted symmetric unitary t-designs, while the upper bounds are for weighted symmetric unitary t-designs.

Lemma 6.1.4. *A symmetric unitary t-design has at least d_{Sym}^2 unitaries.*

Proof: A symmetric t-design in $\mathcal{U}(d)$ gives a 1-design in $\mathcal{U}(\mathrm{Sym}(d^t))$ having a particular tensor product structure, via the map $U \in \mathcal{U}(d) \mapsto V_U = U^{\otimes t}|_{\mathrm{Sym}(d^t)} \in \mathcal{U}(\mathrm{Sym}(d^t))$, where $U^{\otimes t}|_{\mathrm{Sym}(d^t)} : \mathrm{Sym}(d^t) \to \mathrm{Sym}(d^t)$ is the restriction of $U^{\otimes t}$ to the symmetric subspace. This restriction implies that the starting input is in the symmetric subspace, and applying $U^{\otimes t}$ to this input still gives an element in the symmetric subspace. This V_U is an element of $\mathcal{U}(\mathrm{Sym}(d^t))$, and therefore a symmetric t-design with $\rho \in \mathcal{D}(\mathrm{Sym}(d^t))$ can be written as

$$\begin{aligned} \mathop{\mathbb{E}}_{k\in K} w(U_k) \cdot U_k^{\otimes t} \rho (U_k^\dagger)^{\otimes t} &= \int_{\mathcal{U}(d)} U^{\otimes t} \rho (U^\dagger)^{\otimes t} dU \\ \Rightarrow \mathop{\mathbb{E}}_{k\in K} w(V_{U_k}) \cdot V_{U_k} \rho V_{U_k}^\dagger &= \int_{\mathcal{U}(d)} V_U \rho V_U^\dagger dU, \end{aligned} \tag{6.1.2}$$

which is a 1-design in $\mathcal{U}(\mathrm{Sym}(d^t))$. Therefore, a lower bound for symmetric 1-designs also gives a lower bound for symmetric t-designs. From Table 5.1, the lower bound for a t-design in $\mathcal{U}(d)$ is $\binom{d^2+t-1}{t}$. This implies that the lower bound on the number of unitaries for a symmetric 1-design is $\binom{d_{\mathrm{Sym}}^2+1-1}{1} = d_{\mathrm{Sym}}^2$, where the dimension is now d_{Sym}, the dimension of $\mathrm{Sym}(d^t)$. ∎

Lemma 6.1.5. *There are symmetric unitary t-designs formed by n unitaries with $n \leq d_{Sym}^4 - 2d_{Sym} + 3$ unitaries.*

Proof: The proof follows using the results from [RS09] regarding the dimensions for sets of homogeneous polynomials and then applying Carathéodory's theorem.

A symmetric unitary design seen as a linear operator is an element of the convex hull of the set

$$A = \{U^{\otimes t} \otimes (\overline{U})^{\otimes t}|_{\mathrm{Sym}(d^t)\otimes\mathrm{Sym}(d^t)} : U \in \mathcal{U}(d)\}, \tag{6.1.3}$$

recalling from Section 2.11 that the convex hull of a set are all the convex combinations of the elements in that set. Clearly, the convex hull of A is a subset of the convex hull of $B = \{V \otimes \overline{V} : V \in \mathcal{U}(\mathrm{Sym}(d^t))\}$, where V does not necessarily have the tensor product structure. The span of set B has the same dimension as $\mathrm{Hom}(\mathcal{U}(\mathrm{Sym}(d^t)), 1, 1)$, the set of homogeneous polynomials of degree 1 in the entries of V and degree 1 in the entries of $\overline{V}$, where $V \in \mathcal{U}(\mathrm{Sym}(d^t))$. This dimension is $d_{\mathrm{Sym}}^4 - 2d_{\mathrm{Sym}} + 2$, as explained at the end of Section 5.3.1. Now applying Carathéodory's theorem from Section 2.11, elements of the convex hull of A can be written as convex combinations of at most $d_{\mathrm{Sym}}^4 - 2d_{\mathrm{Sym}} + 3$ elements in A. Therefore, there exists a weighted symmetric unitary t-design of at most $d_{\mathrm{Sym}}^4 - 2d_{\mathrm{Sym}} + 3 \in O(d_{\mathrm{Sym}}^4)$ elements. ∎

This shows a gap between the lower and upper bounds in line with the results for unitary t-designs. We now move on to looking at bounds for approximate symmetric unitary t-designs.

6.2 Approximate Symmetric Unitary t-designs

There are different methods in generating approximate unitary t-designs, and in this thesis we focus on the approach of [LM20], which we adjust in order to generate approximate symmetric unitary t-designs. In their work, the construction they use is when enough unitaries are sampled from an exact unitary t-design, then these unitaries form an approximate unitary t-design with probability at least $1/2$. Specifically, this is Theorem 5.2.2 that we presented in Section 5.2. We now restate this theorem, altering the wording and notation slightly so as to conform with how we have defined unitary t-designs. We note that the logarithm notation represents the natural logarithm unless otherwise stated to maintain consistency with the results of [Aub09, LM20].

Theorem 5.2.2. *[LM20] Let $0 < \epsilon < 1$. Let $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ be a unitary t-design, and let $U_1, \ldots, U_n$ be sampled independently from $\mathfrak{U}$. Then there exists a universal constant $C > 0$ such that, if $n \geq C(td)^t(t \log d)^6/\epsilon^2$, then with probability at least 1/2, we have*

$$\forall\ \rho \in \mathcal{D}(d^t),\quad \left\| \frac{1}{n}\sum_{i=1}^{n} U_i^{\otimes t}\rho(U_i^\dagger)^{\otimes t} - T^{(t)}(\rho) \right\|_\infty \leq \frac{\epsilon}{d^t} \tag{6.2.1}$$

We adapt this theorem to our symmetric t-design case, where we are only interested in the set of matrices over $\mathrm{Sym}(d^t)$. Our proof strategies closely resemble those of [LM20], with the alterations necessary so as to consider symmetric unitary t-designs. Our result is summarized in the following theorem, whose proof appears later.

Theorem 6.2.1. *Let $0 < \epsilon < 1$. Let $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ be a unitary t-design, and let $U_1, \ldots, U_n$ be sampled independently from $\mathfrak{U}$. Then there exists a universal constant $\alpha > 0$ such that, if $n \geq \alpha \frac{d_{Sym}}{\epsilon^2} \log(d_{Sym})^6 \log(1/\epsilon^2)$ then with probability at least $\frac{1}{2}$,*

$$\forall\ \rho \in \mathcal{D}(Sym(d^t)),\quad \left\| \frac{1}{n}\sum_{i=1}^{n} U_i^{\otimes t}\rho(U_i^\dagger)^{\otimes t} - T^{(t)}(\rho) \right\|_\infty \leq \frac{\epsilon}{d_{Sym}} \tag{6.2.2}$$

where $T^{(t)}(\rho)$ is the symmetric t-twirling channel which maps $\rho \in \mathcal{D}(Sym(d^t))$ to $\int_{\mathcal{U}(d)} U^{\otimes t}\rho(U^\dagger)^{\otimes t}dU$ with respect to the Haar measure. In other words, $T^{(t)}(\rho) = \langle \tau_{Sym} \rangle(\rho) = \tau_{Sym}$ for $\rho \in \mathcal{D}(Sym(d^t))$.

Note that, by relating the ∞-norm to the 1-norm, Theorem 6.2.1 gives an ϵ-approximate symmetric unitary t-design and thus a perfectly correct t-QPB scheme which has ϵ-indistinguishable ciphertexts. This is because the ∞-norm is the largest singular value, while the 1-norm is the sum of the singular values. Therefore, the 1-norm is naturally upper bounded by the number of singular values multiplied by the ∞-norm. In other words, $||\cdot||_1 \leq d_{\text{Sym}}||\cdot||_\infty$, and if we have $||\cdot||_\infty \leq \frac{\epsilon}{d_{\text{Sym}}}$, then this gives the desired result of $||\cdot||_1 \leq \epsilon$.

To prove Theorem 6.2.1, we use the following known fact,

$$\sup_{\rho\in\mathcal{D}(\text{Sym}(d^t))} \left\|T^{(t)}(\rho)\right\|_\infty = \frac{1}{d_{\text{Sym}}} \tag{6.2.3}$$

where d_{Sym} is the dimension of the symmetric subspace $\text{Sym}(d^t)$. Since $\rho \in \mathcal{D}(\text{Sym}(d^t))$, this $T^{(t)}(\rho) = \tau_{\text{Sym}}$, which is the normalized identity in the symmetric subspace (i.e. a diagonal matrix). The singular values of diagonal matrices correspond to the absolute values of these diagonal elements. In this case, the diagonal elements are $\frac{1}{d_{\text{Sym}}}$ or zero, which implies the maximum singular value of τ_{Sym} is $\frac{1}{d_{\text{Sym}}}$.

We need the following result from [Aub09], which we again adapt for our specific purposes in Lemma 6.2.3.

Lemma 6.2.2. *[Aub09] For $U_1, \ldots, U_N \in \mathcal{U}(d)$ deterministic unitary operators and (ε_i) being a sequence of independent Bernoulli random variables,*

$$\mathbb{E}\left(\sup_{\rho\in\mathcal{D}(\mathcal{H}_d)} \left\|\sum_{i=1}^N \varepsilon_i U_i\rho U_i^\dagger\right\|_\infty\right) \leq C(\log d)^{5/2}(\log N)^{1/2} \sup_{\rho\in\mathcal{D}(\mathcal{H}_d)} \left\|\sum_{i=1}^N U_i\rho U_i^\dagger\right\|_\infty^{1/2} \tag{6.2.4}$$

where $C > 0$ is a universal constant.

It is true that there exists an isometry (a linear map which preserves Euclidean norm and inner product [Wat15]) that maps everything in $\text{Sym}(d^t)$ to a complex Hilbert space $\mathcal{H}_{d_{\text{Sym}}}$ of dimension d_{Sym}. This isometry preserves scalar products and maps all non-symmetric elements to zero. This is because there are only symmetric elements in $\text{Sym}(d^t)$, therefore the isometry that exists is only mapping symmetric elements into this complex Hilbert space $\mathcal{H}_{d_{\text{Sym}}}$. Since there is an isometry between the Hilbert spaces, there is therefore an isometry between the density operators of these spaces, specifically $\mathcal{D}(\text{Sym}(d^t))$ and $\mathcal{D}(\mathcal{H}_{d_{\text{Sym}}})$. Thus, Lemma 6.2.2 can be applied to the case where $\rho \in \mathcal{D}(\text{Sym}(d^t))$ and U_i becomes $U_i^{\otimes t}$, which yields the following lemma:

Lemma 6.2.3. *Let $U_1, \dots, U_n \in \mathcal{U}(d)$ and (ε_i) be a sequence of independent Bernoulli random variables. Then we have*

$$\mathbb{E}\left(\sup_{\rho\in\mathcal{D}(Sym(d^t))}\left\|\sum_{i=1}^n \varepsilon_i U_i^{\otimes t}\rho(U_i^\dagger)^{\otimes t}\right\|_\infty\right)$$
$$\leq \alpha(\log d_{Sym})^{5/2}(\log n)^{1/2}\sup_{\rho\in\mathcal{D}(Sym(d^t))}\left\|\sum_{i=1}^n U_i^{\otimes t}\rho(U_i^\dagger)^{\otimes t}\right\|_\infty^{1/2},$$

where $\alpha > 0$ is a universal constant.

We now have the tools to prove Theorem 6.2.1, which as we mentioned, follows the steps of the proof of Theorem 3.1 in [LM20].

Proof of Theorem 6.2.1: Let $V_1, \dots, V_n$ be independent copies of $U_1, \dots, U_n$ and let $\varepsilon_1, \dots, \varepsilon_n$ be independent Bernoulli random variables. Let

$$M = \sup_{\rho\in\mathcal{D}(\mathrm{Sym}(d^t))}\left\|\frac{1}{n}\sum_{i=1}^n U_i^{\otimes t}\rho(U_i^\dagger)^{\otimes t} - T^{(t)}(\rho)\right\|_\infty.$$

Let us recall a few common results that we need. First is Jensen's inequality, which says that $\mathbb{E}(g(x)) \geq g(\mathbb{E}(x))$ when $g(x)$ is convex. The infinity norm is indeed convex, and therefore we can use this result when looking at the expectation of the infinity norm. Secondly, when looking at $\frac{1}{n}\sum_{i=1}^n U_i^{\otimes t}\rho(U_i^\dagger)^{\otimes t}$, scalar multiplication does not change the result and the distribution is the same as $\frac{1}{n}\sum_{i=1}^n \varepsilon_i U_i^{\otimes t}\rho(U_i^\dagger)^{\otimes t}$ for Bernoulli random variables ε_i. Lastly, we use the triangle inequality, which says that $|A+B| \leq |A| + |B|$.

Using the above, the expectation of M is simplified to

$$\begin{aligned}
\mathbb{E}(M) &= \mathop{\mathbb{E}}_{U}\left(\sup_{\rho\in\mathcal{D}(\mathrm{Sym}(d^t))}\left\|\frac{1}{n}\sum_{i=1}^n U_i^{\otimes t}\rho(U_i^\dagger)^{\otimes t} - \mathop{\mathbb{E}}_{V}\left(\frac{1}{n}\sum_{i=1}^n V_i^{\otimes t}\rho(V_i^\dagger)^{\otimes t}\right)\right\|_\infty\right)\\
&\leq \mathop{\mathbb{E}}_{U,V}\left(\sup_{\rho\in\mathcal{D}(\mathrm{Sym}(d^t))}\left\|\frac{1}{n}\sum_{i=1}^n \left(U_i^{\otimes t}\rho(U_i^\dagger)^{\otimes t} - V_i^{\otimes t}\rho(V_i^\dagger)^{\otimes t}\right)\right\|_\infty\right)\\
&= \mathop{\mathbb{E}}_{U,V,\varepsilon}\left(\sup_{\rho\in\mathcal{D}(\mathrm{Sym}(d^t))}\left\|\frac{1}{n}\sum_{i=1}^n \varepsilon_i\left(U_i^{\otimes t}\rho(U_i^\dagger)^{\otimes t} - V_i^{\otimes t}\rho(V_i^\dagger)^{\otimes t}\right)\right\|_\infty\right)\\
&\leq 2\mathop{\mathbb{E}}_{U,\varepsilon}\left(\sup_{\rho\in\mathcal{D}(\mathrm{Sym}(d^t))}\left\|\frac{1}{n}\sum_{i=1}^n \varepsilon_i U_i^{\otimes t}\rho(U_i^\dagger)^{\otimes t}\right\|_\infty\right).
\end{aligned} \tag{6.2.5}$$

Using Lemma 6.2.3, this expectation becomes

$$\begin{aligned}
\mathbb{E}(M) &\leq \frac{2\alpha}{\sqrt{n}}(\log d_{\mathrm{Sym}})^{5/2}(\log n)^{1/2}\,\mathbb{E}\left(\sup_{\rho\in\mathcal{D}(\mathrm{Sym}(d^t))}\left\|\frac{1}{n}\sum_{i=1}^{n}U_i^{\otimes t}\rho(U_i^\dagger)^{\otimes t}\right\|_\infty^{1/2}\right)\\
&= \frac{2\alpha}{\sqrt{n}}(\log d_{\mathrm{Sym}})^{5/2}(\log n)^{1/2}\,\mathbb{E}\left(\sup_{\rho\in\mathcal{D}(\mathrm{Sym}(d^t))}\left\|\frac{1}{n}\sum_{i=1}^{n}U_i^{\otimes t}\rho(U_i^\dagger)^{\otimes t}-T^{(t)}(\rho)+T^{(t)}(\rho)\right\|_\infty^{1/2}\right)\\
&\leq \frac{2\alpha}{\sqrt{n}}(\log d_{\mathrm{Sym}})^{5/2}(\log n)^{1/2}\,\mathbb{E}\left(M+\frac{1}{d_{\mathrm{Sym}}}\right)^{1/2}\\
&\leq \frac{2\alpha}{\sqrt{n}}(\log d_{\mathrm{Sym}})^{5/2}(\log n)^{1/2}\Big(\mathbb{E}\left(M+\frac{1}{d_{\mathrm{Sym}}}\right)\Big)^{1/2},
\end{aligned} \tag{6.2.6}$$

where we use the fact that $\sup_{\rho\in\mathcal{D}(\mathrm{Sym}(d^t))}\left\|T^{(t)}(\rho)\right\|_\infty=\frac{1}{d_{\mathrm{Sym}}}$, and Jensen's inequality again in the last inequality.

For $X,\nu,\beta\geq 0$, if $X\leq\nu\sqrt{X+\beta}$, then $X\leq\nu^2+\nu\sqrt{\beta}$. This can be applied to the above inequality where $X=\mathbb{E}(M)$, ν corresponds to the coefficients, and $\beta=\frac{1}{d_{\mathrm{Sym}}}$.

$$\mathbb{E}(M)\leq\frac{4\alpha^2}{n}(\log d_{\mathrm{Sym}})^5\log n+\frac{2\alpha}{\sqrt{n}}(\log d_{\mathrm{Sym}})^{5/2}(\log n)^{1/2}\left(\frac{1}{d_{\mathrm{Sym}}}\right)^{1/2}. \tag{6.2.7}$$

Next, we want to find a lower bound for n so that $\mathbb{E}(M)\leq\epsilon/d_{\mathrm{Sym}}$. Let us try

$$n=\frac{4\alpha^2}{\epsilon^2}d_{\mathrm{Sym}}(\log d_{\mathrm{Sym}})^6\cdot\log\big(1/\epsilon^2\big),$$

which implies that

$$\begin{aligned}
\sqrt{n} &= \frac{2\alpha}{\epsilon}(d_{\mathrm{Sym}})^{1/2}(\log d_{\mathrm{Sym}})^3\left(\log\big(1/\epsilon^2\big)\right)^{1/2}\\
\log n &= \log\big(4\alpha^2\big)-\log\big(\epsilon^2\big)+\log d_{\mathrm{Sym}}+\log(\log d_{\mathrm{Sym}})^6+\log\big(\log\big(1/\epsilon^2\big)\big)\\
(\log n)^{1/2} &= \Big(\log\big(4\alpha^2\big)-\log\big(\epsilon^2\big)+\log d_{\mathrm{Sym}}+\log(\log d_{\mathrm{Sym}})^6+\log\big(\log\big(1/\epsilon^2\big)\big)\Big)^{1/2}.
\end{aligned} \tag{6.2.8}$$

Now looking at the first term of Eq. (6.2.7), this becomes

$$
\begin{aligned}
&\frac{4\alpha^2}{n}(\log d_{\mathrm{Sym}})^5 \log n \\
&\quad= \frac{4\alpha^2}{\frac{4\alpha^2}{\epsilon^2} d_{\mathrm{Sym}}(\log d_{\mathrm{Sym}})^6 \cdot \log(1/\epsilon^2)} \cdot (\log d_{\mathrm{Sym}})^5 \\
&\qquad \cdot \Big(\log\big(4\alpha^2\big) - \log\big(\epsilon^2\big) + \log d_{\mathrm{Sym}} + \log(\log d_{\mathrm{Sym}})^6 + \log\big(\log\big(1/\epsilon^2\big)\big)\Big) \\
&\quad= \frac{\epsilon^2}{d_{\mathrm{Sym}}(\log d_{\mathrm{Sym}}) \cdot \log(1/\epsilon^2)} \cdot \Big(\log\big(4\alpha^2\big) - \log\big(\epsilon^2\big) + \log d_{\mathrm{Sym}} + \log(\log d_{\mathrm{Sym}})^6 + \log\big(\log\big(1/\epsilon^2\big)\big)\Big) \\
&\quad= \frac{\epsilon^2}{d_{\mathrm{Sym}}} \cdot \Bigg(\frac{\log d_{\mathrm{Sym}}}{(\log d_{\mathrm{Sym}}) \cdot \log(1/\epsilon^2)} + \frac{\log(1/\epsilon^2)}{(\log d_{\mathrm{Sym}}) \cdot \log(1/\epsilon^2)} \\
&\qquad + \frac{\log(4\alpha^2) + \log(\log d_{\mathrm{Sym}})^6 + \log(\log(1/\epsilon^2))}{(\log d_{\mathrm{Sym}}) \cdot \log(1/\epsilon^2)} \Bigg) \\
&\quad= \frac{\epsilon^2}{d_{\mathrm{Sym}}} \cdot \Bigg(\frac{1}{\log(1/\epsilon^2)} + \frac{1}{(\log d_{\mathrm{Sym}})} + \frac{\log(4\alpha^2)}{(\log d_{\mathrm{Sym}}) \cdot \log(1/\epsilon^2)} \\
&\qquad + \frac{\log(\log d_{\mathrm{Sym}})^6}{(\log d_{\mathrm{Sym}}) \cdot \log(1/\epsilon^2)} + \frac{\log(\log(1/\epsilon^2))}{(\log d_{\mathrm{Sym}}) \cdot \log(1/\epsilon^2)} \Bigg) \\
&\quad\leq \frac{\epsilon^2}{d_{\mathrm{Sym}}} \cdot \Big(1 + 1 + 1 + 1 + 1\Big) \\
&\quad\leq \frac{5\epsilon^2}{d_{\mathrm{Sym}}}.
\end{aligned}
\tag{6.2.9}
$$

Since $\log(\log d_{\mathrm{Sym}})^6$ and $\log(\log(1/\epsilon^2))$ are much smaller than $\log d_{\mathrm{Sym}}$ and $\log(1/\epsilon^2)$, respectively, the fractions $\frac{\log\left(\log d_{\mathrm{Sym}}\right)}{(\log d_{\mathrm{Sym}}) \cdot \log(1/\epsilon^2)}$ and $\frac{\log\left(\log\left(1/\epsilon^2\right)\right)}{(\log d_{\mathrm{Sym}}) \cdot \log(1/\epsilon^2)}$ are both less than or equal to 1. The $4\alpha^2$ is just a constant, so this fraction can be made to be less than or equal to 1, and $\log d_{\mathrm{Sym}} \geq 1$, so $\frac{1}{\log d_{\mathrm{Sym}}} \leq 1$. In order for $\log(1/\epsilon^2) \geq 1$, we require that $0 \leq \epsilon \leq \frac{1}{\sqrt{e}}$, and therefore $\frac{1}{\log(1/\epsilon^2)} \leq 1$. From the assumption that $\epsilon < 1$, this gives $\epsilon^2 < \epsilon$ and yields $\frac{5\epsilon^2}{d_{\mathrm{Sym}}} \leq \frac{\epsilon}{d_{\mathrm{Sym}}}$ up to relabelling of constants.

The second part of Eq. (6.2.7) becomes

$$
\begin{aligned}
&\frac{2\alpha}{\sqrt{n}}(\log d_{\mathrm{Sym}})^{5/2}(\log n)^{1/2}\left(\frac{1}{d_{\mathrm{Sym}}}\right)^{1/2} \\
&= \frac{2\alpha}{\frac{2\alpha}{\epsilon}(d_{\mathrm{Sym}})^{1/2}(\log d_{\mathrm{Sym}})^{3}(\log(1/\epsilon^2))^{1/2}}\cdot\left(\frac{1}{d_{\mathrm{Sym}}}\right)^{1/2}\cdot(\log d_{\mathrm{Sym}})^{5/2} \\
&\quad\cdot\left[\left(\log\left(4\alpha^2\right)-\log\left(\epsilon^2\right)+\log d_{\mathrm{Sym}}+\log(\log d_{\mathrm{Sym}})^6+\log\left(\log\left(1/\epsilon^2\right)\right)\right)^{1/2}\right] \\
&= \frac{\epsilon}{d_{\mathrm{Sym}}(\log d_{\mathrm{Sym}})^{1/2}(\log(1/\epsilon^2))^{1/2}}\cdot\left[\left(\log\left(4\alpha^2\right)-\log\left(\epsilon^2\right)+\log d_{\mathrm{Sym}}\right.\right. \\
&\quad\left.\left.+\log(\log d_{\mathrm{Sym}})^6+\log\left(\log\left(1/\epsilon^2\right)\right)\right)^{1/2}\right] \\
&= \frac{\epsilon}{d_{\mathrm{Sym}}}\cdot\left[\frac{\left(\log(4\alpha^2)-\log(\epsilon^2)+\log d_{\mathrm{Sym}}+\log(\log d_{\mathrm{Sym}})^6+\log(\log(1/\epsilon^2))\right)^{1/2}}{(\log d_{\mathrm{Sym}})^{1/2}(\log(1/\epsilon^2))^{1/2}}\right] \\
&\leq \frac{\epsilon}{d_{\mathrm{Sym}}}\cdot\left[\frac{\log(4\alpha^2)-\log(\epsilon^2)+\log d_{\mathrm{Sym}}+\log(\log d_{\mathrm{Sym}})^6+\log(\log(1/\epsilon^2))}{(\log d_{\mathrm{Sym}})(\log(1/\epsilon^2)}\right] \\
&= \frac{\epsilon}{d_{\mathrm{Sym}}}\cdot\left(\frac{1}{\log(1/\epsilon^2)}+\frac{1}{(\log d_{\mathrm{Sym}})}+\frac{\log(4\alpha^2)}{(\log d_{\mathrm{Sym}})\cdot\log(1/\epsilon^2)}\right. \\
&\quad\left.+\frac{\log(\log d_{\mathrm{Sym}})^6}{(\log d_{\mathrm{Sym}})\cdot\log(1/\epsilon^2)}+\frac{\log(\log(1/\epsilon^2))}{(\log d_{\mathrm{Sym}})\cdot\log(1/\epsilon^2)}\right) \\
&\leq \frac{5\epsilon}{d_{\mathrm{Sym}}}.
\end{aligned}
\tag{6.2.10}
$$

This gives $\mathbb{E}(M)\leq\frac{\epsilon}{d_{\mathrm{Sym}}}$, again up to relabelling of constants.

Lastly, to conclude that $P\left(M\leq\frac{\epsilon}{d_{\mathrm{Sym}}}\right)\geq\frac{1}{2}$, we use Markov's inequality, which says that $P(X\leq a)\geq 1-\frac{\mathbb{E}(X)}{a}$. This gives

$$
P\left(M\leq\frac{2\epsilon}{d_{\mathrm{Sym}}}\right)\geq 1-\frac{\mathbb{E}(M)}{2\epsilon/d_{\mathrm{Sym}}}\geq\frac{1}{2}, \tag{6.2.11}
$$

up to a relabelling of ϵ. ∎

This proves an upper bound for ϵ-approximate symmetric unitary t-designs, where we make explicit this $\log(1/\epsilon^2)$ term that is missing in the result of [Aub09]. The following lemma provides a lower bound for approximate symmetric unitary t-designs.

Lemma 6.2.4. *An ϵ-approximate symmetric unitary t-design has at least $(d_{Sym})^{1-\epsilon}$ unitaries.*

Proof: We adapt the arguments given in [LW17] to our case. As proven in [LW17], if two quantum channels T and $\hat{T}$ on $\mathcal{L}(\mathbb{C}^d)$ are ϵ-close in the 1-norm, then the following is true

$$\log r(\hat{T}) \geq (1-\epsilon) \max_{\rho \in \mathcal{D}(\mathbb{C}^d)} |S(T(\rho)) - S(\rho)|, \tag{6.2.12}$$

where $r(\hat{T})$ is the Kraus rank of $\hat{T}$ and $S(\cdot)$ is the von Neumann entropy.

A quantum channel can be written in terms of Kraus operators, which are matrices with the property that $\sum_i K_i^\dagger K_i = \mathbb{1}$. Specifically, for a quantum channel Φ acting on an input density operator ρ, it is true that $\Phi(\rho) \mapsto \sum_i K_i \rho K_i^\dagger$. These $\{K_i\}$ are the Kraus operators, and the minimal i needed to describe Φ is the Kraus rank of Φ. Interested readers can find more details in [NC10, Wat15] where the notation used in the former is 'operator-sum representation' and the latter is 'Kraus representation.' The von Neumann entropy is a measure of the amount of uncertainty in a quantum state, and is again further explained in [NC10, Wat15].

In [LM20] it is explained that if the quantum channel T has the property that there is some c such that $\|T(\rho)\|_\infty \leq \frac{c}{d}$ for $\rho \in \mathcal{D}(\mathbb{C}^d)$, then it can be said that

$$\max_{\rho \in \mathcal{D}(\mathbb{C}^d)} |S(T(\rho)) - S(\rho)| \geq \log\left(\frac{d}{c}\right), \tag{6.2.13}$$

which implies that $r(\hat{T}) \geq \left(\frac{d}{c}\right)^{(1-\epsilon)}$.

With respect to ϵ-approximate symmetric unitary t-designs, it is known that for $\rho \in \mathcal{D}(\mathrm{Sym}(d^t))$, $\left\|T^{(t)}(\rho)\right\|_\infty = \frac{1}{d_{\mathrm{Sym}}}$. Therefore, if a quantum channel $\hat{T}^{(t)}$ is ϵ-close to $T^{(t)}$ in the 1-norm, then the rank of Kraus operators for the channel $\hat{T}^{(t)}$ satisfies

$$r(\hat{T}^{(t)}) \geq (d_{\mathrm{Sym}})^{(1-\epsilon)}, \tag{6.2.14}$$

which gives a lower bound for the number of unitaries needed for an ϵ-approximate symmetric unitary t-design. ∎

Table 6.1 summarizes these bounds for symmetric unitary t-designs.

	Lower	**Upper**
Exact	d_{Sym}^2	$d_{\mathrm{Sym}}^4 - 2d_{\mathrm{Sym}}^2 + 3 \in O(d_{\mathrm{Sym}}^4)$
ϵ-Approximate	$(d_{\mathrm{Sym}})^{(1-\epsilon)}$	$\alpha \frac{d_{\mathrm{Sym}}}{\epsilon^2} \log(d_{\mathrm{Sym}})^6 \log(1/\epsilon^2)$

Table 6.1: Symmetric Unitary t-design Bounds

6.3 Comparison with QOTP and Unitary t-designs

Again using the example where $d = 2$ and letting t vary, we are able to compare the classical bits needed for exact symmetric unitary t-designs with the quantum one-

time pad with independent keys and unitary t-designs. We use the same calculations explained in Section 5.5, now including the exact symmetric upper bounds from Table 6.1. This comparison is in Fig. 6.1, whose data is in Appendix B.

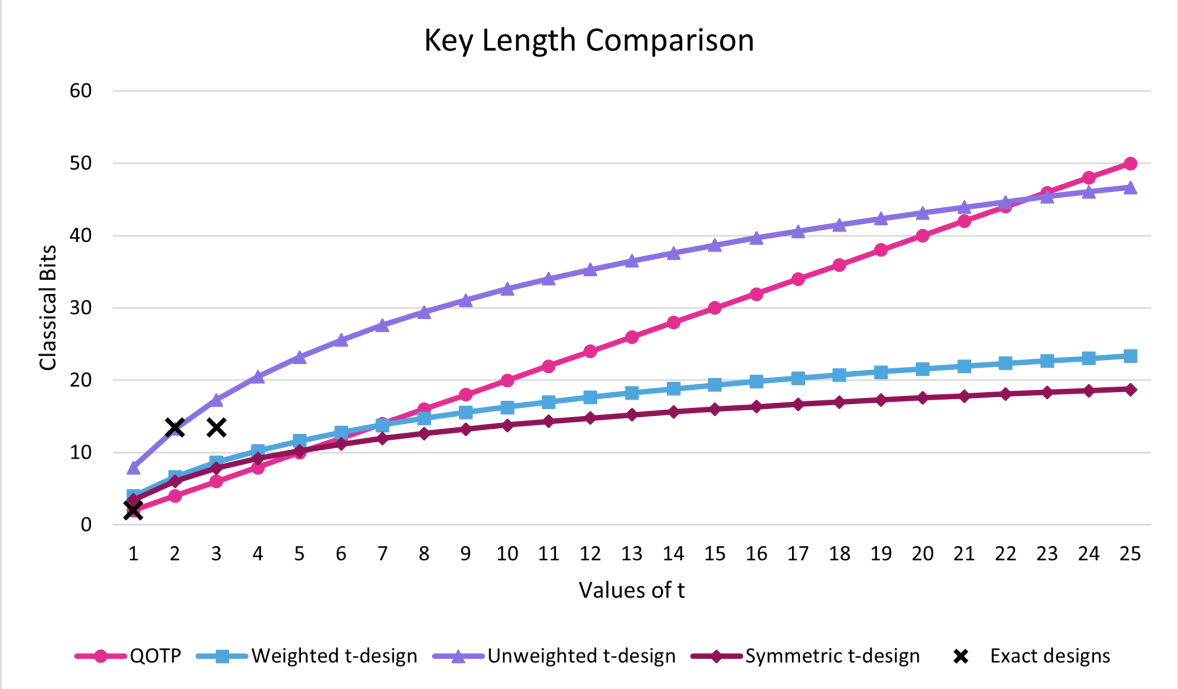

Figure 6.1: QOTP, Weighted/Unweighted t-design & Symmetric Weighted t-design, $t \leq 25$, $d = 2$

Once t is larger than 5, symmetric unitary t-designs require less classical bits than the QOTP, while it takes until t is larger than 6 for unitary t-designs for have less bits than the QOTP. Therefore, of these three solutions to t-QPB, symmetric unitary t-designs are the best option when t is large if the main concern is to have the smallest key length. On the other hand, if t is less than 5, using the QOTP with independent keys is the most efficient decision.

Chapter 7

Conclusion

As one can see in Fig. 6.1, symmetric unitary t-designs have the smallest key length for t-QPB with large t from the three solutions presented in this thesis. If $t \leq 5$, the quantum one-time pad with independent keys is the best choice, with the additional bonus of not needing to restrict the input plaintext to the symmetric subspace for perfect security.

We now focus on open problems and questions with regards to t-recipient quantum private broadcasting, regular and symmetric unitary t-designs.

Non-malleability. Past work with designs has shown that unitary 2-designs yield non-malleable encryption schemes [ABW09]. An encryption scheme is deemed *non-malleable* if an adversary is unable to tamper with an intercepted encrypted message. Specifically, the quantum channel representing an adversary's actions is a convex combination of either the identity or channels that map all inputs to a constant output [ABW09]. Conceptually, this corresponds to the adversary either doing nothing, or replacing the ciphertext with a different quantum state that decrypts to this constant output. It is an open problem whether unitary $2t$-designs form non-malleable encryption schemes, which can therefore be used for t-recipient quantum private broadcasting in the same way that a unitary 2-design is required for non-malleable encryption with one recipient. To consider this problem, it first needs to be determined which adversarial actions are categorized as non-malleable when $t > 1$. Once these are defined, it can be examined whether unitary $2t$-designs are non-malleable encryption schemes, and furthermore, whether this characterization of non-malleability can be applied to symmetric unitary $2t$-designs.

Applications of Symmetric t-designs. We leave as an open problem further applications of symmetric unitary t-designs. For example, recent work [BSZ20] shows that Haar random unitaries allow a private quantum channel to be implemented with multi-photon pulses, and shows that t-designs can be used to practically implement

such channels when the parity of the photon source is fixed. An interesting question is whether this result also appears with symmetric unitary t-designs.

Efficiency of Designs. Moreover, to the best of our knowledge, there do not appear to be efficient constructions of exact unitary t-designs for $t > 3$, although there has been recent work completed regarding such constructions [BNOZ20, NZO+21]. Approximate unitary t-designs are able to be constructed efficiently [BHH16], and different techniques have been used to reduce the circuit depth needed to construct these approximate designs [HM18, MGDM19, HMMH+20]. It is left open whether these techniques can also be applied to the constructions of approximate symmetric unitary t-designs.

Approximate Correctness. For simplicity throughout this thesis, we focused on t-QPB schemes with perfect correctness. We leave as an open problem the relaxation of this correctness to further improve the key length. Furthermore, we leave open whether there is another solution to t-QPB that has the same security and similar key length as presented here with symmetric unitary t-designs, but with fewer restrictions on the input plaintext message.

Appendix A

Python Codes

A.1 Code from Proof of Theorem 4.3.1

```
import sympy
from sympy import *
from sympy.physics.quantum import TensorProduct
from sympy import init_printing

# Plus and minus density matrices, one qubit and two qubits
pl = Matrix([[1/2,1/2],[1/2,1/2]])
ne = Matrix([[1/2,-1/2],[-1/2,1/2]])
pl2 = TensorProduct(pl,pl)
ne2 = TensorProduct(ne,ne)

# The two states, rho_0 and rho_1
a0 = Matrix([[1/2,0,0,0],[0,0,0,0],[0,0,0,0],[0,0,0,1/2]])
a1 = 1/2*(pl2+ne2)

# Trace distance
dqotp_prod = ((a0-a1).H)*(a0-a1)
dqotp_absv = dqotp_prod**(1/2)
dqotp_tr = 1/2*(Trace(dqotp_absv).simplify())
```

A.2 Code from Weighted 2-design in Eq. (5.1.17)

```
# Computed using Sage in Python
```

```
# Pauli matrices
Id = identity_matrix(2)
X = matrix([[0,1],[1,0]])
Y = matrix([[0,-I],[I,0]])
Z = matrix([[1,0],[0,-1]])

c=1/sqrt(3)
d=sqrt(2/3)
e=3/32

# Matrix of weights and unit vectors
M = matrix([[1/16,1,0,0,0],[e,0,c,c,c],[e,0,-c,c,c],[e,0,c,-c,c],
[e,0,c,c,-c],[e,c,d,0,0],[e,c,-d,0,0],[e,c,0,d,0],[e,c,0,-d,0],
[e,c,0,0,d],[e,c,0,0,-d]])

# Calculating the 11 matrices in the design
mat = []
for i in range(11):
    mat.append(M[i,1]*Id+M[i,2]*I*X+M[i,3]*I*Y+M[i,4]*I*Z)


# Isolating the weights
wt=[]
for i in range(11):
    wt.append(M[i,0])

# Summation calculation with weights and trace of matrix product
val=[]
for i in range(11):
    for j in range(11):
        val.append(wt[i]*wt[j]*(abs(((mat[i]).H*(mat[j])).trace())**4))

# Summation
sm = sum(val)

# Numerical evaluation of summation
N(sm)
```

A.3 Code from Proof of Theorem 5.4.2

```
import sympy
from sympy import *
from sympy.physics.quantum import TensorProduct
from sympy import init_printing

# Tau and Tau_Sym
p0 = Matrix([[1/4,0,0,0],[0,1/4,0,0],[0,0,1/4,0],[0,0,0,1/4]])
p1 = Matrix([[1/3,0,0,0],[0,1/6,1/6,0],[0,1/6,1/6,0],[0,0,0,1/3]])

# Trace distance
prod = ((p0-p1).H)*(p0-p1)
absv = prod**(1/2)
tr = 1/2*Trace(absv).simplify()
```

Appendix B

Data for Figures

t	**QOTP**	**Exact Weighted t-design**	**Exact Unweighted t-design**	**Exact Sym Weighted t-design**
1	4	16	256	11
2	16	100	10,000	66
3	64	400	160,000	227
4	256	1,225	1,500,625	578
5	1,024	3,136	9,834,496	1,227
6	4,096	7,056	49,787,136	2,306
7	16,384	14,400	207,360,000	3,971
8	65,536	27,225	741,200,625	6,402
9	262,144	48,400	2,342,560,000	9,803
10	1,048,576	81,796	6,690,585,616	14,402
11	4,194,304	132,496	17,555,190,016	20,451
12	16,777,216	207,025	42,859,350,625	28,226
13	67,108,864	313,600	98,344,960,000	38,027
14	268,435,456	462,400	213,813,760,000	50,178
15	1,073,741,824	665,856	443,364,212,736	65,027
16	4,294,967,296	938,961	881,647,759,521	82,946
17	17,179,869,184	1,299,600	1,688,960,160,000	104,331
18	68,719,476,736	1,768,900	3,129,007,210,000	129,602
19	274,877,906,944	2,371,600	5,624,486,560,000	159,203
20	1,099,511,627,776	3,136,441	9,837,262,146,481	193,602
21	4,398,046,511,104	4,096,576	16,781,934,923,776	233,291
22	17,592,186,044,416	5,290,000	27,984,100,000,000	278,786

23	70,368,744,177,664	6,760,000	45,697,600,000,000	330,627
24	281,474,976,710,656	8,555,625	73,198,719,140,625	389,378
25	1,125,899,906,842,620	10,732,176	115,179,601,694,976	455,627
26	4,503,599,627,370,500	13,351,716	178,268,320,144,656	529,986
27	18,014,398,509,482,000	16,483,600	271,709,068,960,000	613,091
28	72,057,594,037,927,900	20,205,025	408,243,035,250,625	705,602
29	288,230,376,151,712,000	24,601,600	605,238,722,560,000	808,203
30	1,152,921,504,606,850,000	29,767,936	886,130,013,700,095	921,602
31	4,611,686,018,427,390,000	35,808,256	1,282,231,197,761,540	1,046,531
32	18,446,744,073,709,600,000	42,837,025	1,835,010,710,850,620	1,183,746
33	73,786,976,294,838,200,000	50,979,600	2,598,919,616,160,000	1,334,027
34	295,147,905,179,353,000,000	60,372,900	3,644,887,054,410,000	1,498,178
35	1,180,591,620,717,410,000,000	71,166,096	5,064,613,219,881,220	1,677,027
36	4,722,366,482,869,650,000,000	83,521,321	6,975,811,061,585,040	1,871,426
37	18,889,465,931,478,600,000,000	97,614,400	9,528,571,087,360,000	2,082,251
38	75,557,863,725,914,300,000,000	113,635,600	12,913,049,587,360,000	2,310,402
39	302,231,454,903,657,000,000,000	131,790,400	17,368,709,532,160,000	2,556,803
40	1,208,925,819,614,630,000,000,000	152,300,281	23,195,375,592,679,000	2,822,402

Table B.1: Unitaries for QOTP, Weighted/Unweighted t-design, Symmetric Weighted t-design when $d = 2$

t	**QOTP**	**Exact Weighted t-design**	**Exact Unweighted t-design**	**Exact Symmetric Weighted t-design**
1	2	4	8	3.46
2	4	6.64	13.29	6.04
3	6	8.64	17.29	7.83
4	8	10.26	20.52	9.17
5	10	11.61	23.23	10.26
6	12	12.78	25.57	11.17
7	14	13.81	27.63	11.96
8	16	14.73	29.47	12.64
9	18	15.56	31.13	13.26
10	20	16.32	32.64	13.81
11	22	17.02	34.03	14.32
12	24	17.66	35.32	14.78
13	26	18.26	36.52	15.21
14	28	18.82	37.64	15.61

15	30	19.34	38.69	15.99
16	32	19.84	39.68	16.34
17	34	20.31	40.62	16.67
18	36	20.75	41.51	16.98
19	38	21.18	42.35	17.28
20	40	21.58	43.16	17.56
21	42	21.97	43.93	17.83
22	44	22.33	44.67	18.09
23	46	22.69	45.38	18.33
24	48	23.03	46.06	18.57
25	50	23.36	46.71	18.80
26	52	23.67	47.34	19.02
27	54	23.97	47.95	19.23
28	56	24.27	48.54	19.43
29	58	24.55	49.10	19.62
30	60	24.83	49.65	19.81
31	62	25.09	50.19	20.00
32	64	25.35	50.70	20.17
33	66	25.60	51.21	20.35
34	68	25.85	51.69	20.51
35	70	26.08	52.17	20.68
36	72	26.32	52.63	20.84
37	74	26.54	53.08	20.99
38	76	26.76	53.52	21.14
39	78	26.97	53.95	21.29
40	80	27.18	54.36	21.43

Table B.2: Classical bits for QOTP, Weighted/Unweighted t-design, Symmetric Weighted t-design when $d = 2$

Bibliography

[ABW09] A. Ambainis, J. Bouda, and A. Winter. Nonmalleable encryption of quantum information. *Journal of Mathematical Physics*, 50(4): 042106, 2009.
DOI: 10.1063/1.3094756.

[Ada13] M. Adam. Applications of unitary k-designs in quantum information processing. Master's thesis, Masarykova univerzita, Fakulta informatiky, 2013.

[AE07] A. Ambainis and J. Emerson. Quantum t-designs: t-wise independence in the quantum world. In *22nd Annual Conference on Computational Complexity—CCC 2007*, pages 129–140, 2007.
DOI: 10.1109/CCC.2007.26.

[AM17] G. Alagic and C. Majenz. Quantum non-malleability and authentication. In *Advances in Cryptology—CRYPTO 2017*, page 310–341, 2017.
DOI: 10.1007/978-3-319-63715-0_11.

[AMR20] G. Alagic, C. Majenz, and A. Russell. Efficient simulation of random states and random unitaries. In *Advances in Cryptology—EUROCRYPT 2020*, pages 759–787, 2020.
DOI: 10.1007/978-3-030-45727-3_26.

[AMTdW00] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *41st Annual Symposium on Foundations of Computer Science—FOCS 2000*, pages 547–553, 2000.
DOI: 10.1109/SFCS.2000.892142.

[Aub09] G. Aubrun. On almost randomizing channels with a short Kraus decomposition. *Communications in Mathematical Physics*, 288(3): 1103–1116, 2009.
DOI: 10.1007/s00220-008-0695-y.

[BGGS21] A. Broadbent, C. E. González-Guillén, and C. Schuknecht. Quantum private broadcasting, 2021.
arXiv: 2107.11474.

[BHH16] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki. Local Random Quantum Circuits are Approximate Polynomial-Designs. *Communications in Mathematical Physics*, 346(2): 397–434, 2016.
DOI: 10.1007/s00220-016-2706-8.

[BNOZ20] E. Bannai, Y. Nakata, T. Okuda, and D. Zhao. Explicit construction of exact unitary designs, 2020.
arXiv: 2009.11170.

[BR03] P. O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. *Physical Review A*, 67(4): 042317, 2003.
DOI: 10.1103/PhysRevA.67.042317.

[BS10] G. Benenti and G. Strini. Computing the distance between quantum channels: Usefulness of the Fano representation. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 43(21): 215508, 2010.
DOI: 10.1088/0953-4075/43/21/215508.

[BSZ20] J. Bouda, M. Sedlák, and M. Ziman. Private quantum channels for multi-photon pulses and unitary k-designs, 2020.
arXiv: 2009.06067.

[CLLW16] R. Cleve, D. Leung, L. Liu, and C. Wang. Near-linear constructions of exact unitary 2-designs. *Quantum Information and Computation*, 16(9&10): 721–756, 2016.
DOI: 10.26421/QIC16.9-10-1.

[Col03] B. Collins. Moments and cumulants of polynomial random variables on unitary groups, the itzykson-zuber integral, and free probability. *International Mathematics Research Notices*, 2003(17): 953–982, 2003.

[CS06] B. Collins and P. Śniady. Integration with Respect to the Haar Measure on Unitary, Orthogonal and Symplectic group. *Communications in Mathematical Physics*, 264(3): 773–795, 2006.
DOI: 10.1007/s00220-006-1554-3.

[CSD] I. T. L. Computer Security Division. Post-Quantum Cryptography: CSRC. Available at https://csrc.nist.gov/Projects/post-quantum-cryptography.

[Dan05] C. Dankert. Efficient simulation of random quantm states and operators. Master's thesis, University of Waterloo, Ontario, 2005.

[DCEL09] C. Dankert, R. Cleve, J. Emerson, and E. Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Physical Review A*, 80: 012304, 2009.
DOI: 10.1103/PhysRevA.80.012304.

[DM14] O. Di Matteo. Lecture notes in Applications of Haar Measure in Quantum Information, 2014. Available at https://glassnotes.github.io/OliviaDiMatteo_Unitary2Designs.pdf.

[DS94] P. Diaconis and M. Shahshahani. On the Eigenvalues of Random Matrices. *Journal of Applied Probability*, 31(A): 49–62, 1994.

[FH91] W. Fulton and J. Harris. *Representation Theory: A First Course*. Graduate Texts in Mathematics. Springer New York, 1991.

[GAE07] D. Gross, K. Audenaert, and J. Eisert. Evenly distributed unitaries: On the structure of unitary designs. *Journal of Mathematical Physics*, 48(5): 052104, 2007.
DOI: 10.1063/1.2716992.

[Got98] D. Gottesman. The Heisenberg representation of quantum computers. In *22nd International Colloquium on Group Theoretical Methods in Physics—GROUP 22*, pages 32–43, 1998.
arXiv: quant-ph/9807006.

[Har13] A. W. Harrow. The Church of the Symmetric Subspace, 2013.
arXiv: 1308.6595.

[HM18] A. Harrow and S. Mehraban. Approximate unitary t-designs by short random quantum circuits using nearest-neighbor and long-range gates, 2018.
arXiv: 1809.06957.

[HMMH+20] J. Haferkamp, F. Montealegre-Mora, M. Heinrich, J. Eisert, D. Gross, and I. Roth. Quantum homeopathy works: Efficient unitary designs with a system-size independent number of non-Clifford gates, 2020.
arXiv: 2002.09524.

[Kan15] D. Kane. Small designs for path-connected spaces and path-connected homogeneous spaces. *Transactions of the American Mathematical Society*, 367(9): 6387–6414, 2015.
DOI: 10.1090/tran/6250.

[Kaz10] A. Kaznatcheev. Structure of exact and approximate unitary t-designs, 2010. Available at https://www.cs.mcgill.ca/~akazna/kaznatcheev20100509.pdf.

[LM20] C. Lancien and C. Majenz. Weak approximate unitary designs and applications to quantum encryption. *Quantum*, 4: 313, 2020. DOI: 10.22331/q-2020-08-28-313.

[LW17] C. Lancien and A. Winter. Approximating quantum channels by completely positive maps with small Kraus rank, 2017. arXiv: 1711.00697.

[MGDM19] R. Mezher, J. Ghalbouni, J. Dgheim, and D. Markham. Efficient approximate unitary t-designs from partially invertible universal sets and their application to quantum speedup, 2019. arXiv: 1905.01504.

[NC10] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 10^{th} anniversary edition, 2010.

[NS20] A. Nema and P. Sen. A concentration of measure result for non-catalytic decoupling via approximate unitary t-designs, 2020. arXiv: 2002.00247.

[NZO+21] Y. Nakata, D. Zhao, T. Okuda, E. Bannai, Y. Suzuki, S. Tamiy, K. Heya, Z. Yan, K. Zuo, S. Tamate, Y. Tabuchi, and Y. Nakamura. Quantum circuits for exact unitary t-designs and applications to higher-order randomized benchmarking, 2021. arXiv: 2102.12617.

[Rai98] E. M. Rains. Increasing Subsequences and the Classical Groups. *The Electronic journal of combinatorics*, 5(1), 1998.

[Roc70] R. T. Rockafellar. *Convex analysis*, volume 36. Princeton university press, 1970.

[RS09] A. Roy and A. J. Scott. Unitary designs and codes. *Designs, Codes and Cryptography*, 53(1): 13–31, 2009. DOI: 10.1007/s10623-009-9290-2.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2): 120–126, 1978. DOI: 10.1145/359340.359342.

[Sco08a] A. J. Scott. Optimizing quantum process tomography with unitary 2-designs. *Journal of Physics A: Mathematical and Theoretical*, 41(5): 055308, 2008.
DOI: 10.1088/1751-8113/41/5/055308.

[Sco08b] A. J. Scott. Unitary design: bounds on their size, "Perimeter Institute" presentation, 2008. Available at perimeterinstitute.ca/videos/unitary-design-bounds-their-size.

[SDTR13] O. Szehr, F. Dupuis, M. Tomamichel, and R. Renner. Decoupling with unitary approximate two-designs. *New Journal of Physics*, 15(5): 053022, 2013.
DOI: 10.1088/1367-2630/15/5/053022.

[Sho94] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science—FOCS 1994*, pages 124–134, 1994.
DOI: 10.1109/SFCS.1994.365700.

[Sta11] R. P. Stanley. *Enumerative Combinatorics: Volume 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2011.

[Wat11] J. Watrous. The Theory of Quantum Information, Lecture Notes, 2011. Available at https://cs.uwaterloo.ca/~watrous/TQI-notes/.

[Wat15] J. Watrous. Theory of quantum information, 2015.
Online: https://cs.uwaterloo.ca/~watrous/TQI/.

[Web16] Z. Webb. The Clifford group forms a unitary 3-design. *Quantum Information and Computation*, 16(15–16): 1379–1400, 2016.

[ZKGG16] H. Zhu, R. Kueng, M. Grassl, and D. Gross. The Clifford group fails gracefully to be a unitary 4-design, 2016.
arXiv: 1609.08172.

[ZZP17] L. Zhang, C. Zhu, and C. Pei. Randomized Benchmarking Using Unitary t-Design for Average Fidelity Estimation of Practical Quantum Circuit, 2017.
arXiv: 1711.08098.