SECURE QUANTUM ENCRYPTION

By
Michael St-Jules
November 2016

A Thesis
submitted to the School of Graduate Studies and Research
in partial fulfillment of the requirements
for the degree of
Master of Science in Mathematics[1]

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

Abstract

To the field of cryptography, quantum mechanics is a game changer. The exploitation of quantum mechanical properties through the manipulation of *quantum information*, the information encoded in the state of quantum systems, would allow many protocols in use today to be broken as well as lead to the expansion of cryptography to new protocols. In this thesis, *quantum* encryption, i.e. encryption schemes for quantum data, is defined, along with several definitions of security, broadly divisible into semantic security and ciphertext indistinguishability, which are proven equivalent, in analogy to the foundational result by Goldwasser and Micali. Private- and public-key quantum encryption schemes are also constructed from quantum-secure cryptographic primitives, and their security is proven. Most of the results are in the joint paper *Computational Security of Quantum Encryption*, to appear in the 9th International Conference on Information Theoretic Security (ICITS2016).

Acknowledgements

I would like to thank my supervisor, Anne, for her support, guidance, patience and understanding, and the last two particularly when I was distracted by coursework, taking away from our research and my work on this thesis.

I'd also like to thank her and my other coauthors, Gorjan Alagic, Bill Fefferman, Tommaso Gagliardoni and Christian Schaffner, for their work on our joint paper and the stimulating discussions that accompanied it.

Contents

List of Figures

List of Acronyms

CCA1	Non-adaptive chosen ciphertext attack, e.g. in Definition 4.1.3
CPA	Chosen plaintext attack, e.g. in Definition 4.1.3
IND	Indistinguishability, Definition 4.1.3
PPT	Probabilistic polynomial-time algorithm, Definition 3.6.1
PT	Polynomial-time algorithm, Definition 3.6.1
QOTP	Quantum one-time pad, Definition 3.8.7
qOWF	Quantum-secure one-way function, Definition 4.3.1
qPKE	Quantum public-key encryption scheme, Definition 4.1.2
qPRG	Quantum-secure pseudorandom generator, Definition 4.3.9
qPRF	Quantum-secure pseudorandom function, Definition 4.3.2
QPT	Quantum polynomial-time algorithm, Definition 3.6.3
qSKE	Quantum symmetric-key encryption scheme, Definition 4.1.1
qTOWP	Quantum-secure trapdoor one-way permutation, Definition 4.3.5
SEM	Semantic security, Definition 4.2.1

List of Notation

$x \xleftarrow{\$} X$	x is distributed uniformly randomly in X, Section 3.1
$0^n, 1^n$	The strings consisting of n 1's and 0's, respectively, Section 3.1
$\mathcal{H}$	A Hilbert space, Definition 3.2.2
$\dagger$	The adjoint operator, Definition 3.2.4
$\|\psi\rangle, \langle\psi\|$	Bra-ket notation, Notation 3.2.11
$\otimes$	The tensor product, Definition 3.2.12
Tr	The trace operator, Definition 3.2.14
ρ, σ	Density operators or matrices, Definition 3.3.2
$\mathcal{H}_A, \rho_{AB}, \mathrm{Tr}_A(\rho_{AB}), \mathbb{1}_A$	Subscript notation, Notation 3.4.11
negl	A negligible function, Definition 3.7.1

Chapter 1

Introduction

1.1 Overview

Cryptography is the study and practice of secure communication in the presence of malicious entities, and one of its pillars is the secure encryption of messages, transforming them into information unintelligible except to the intended receiver, who may read them only after decryption. Quantum mechanics leads to new possibilities in cryptography. Three important properties of quantum mechanics separating it from classical physics are quantum superposition, which allows a quantum system to be in two or more states simultaneously; quantum entanglement, the existence of quantum systems whose behaviour cannot be adequately through classical (probabilistic) correlations between their subsystems; and the impossibility of copying arbitrary quantum states, a consequence of the *no-cloning theorem* (see Theorem 3.4.1). The exploitation of such properties through the manipulation of *quantum information*, the information encoded in the state of quantum systems and whose basic building block is the *qubit*, would allow many protocols in use today to be broken — by the application of *Shor's algorithm for integer factorization* [Sho94] implemented on a *quantum computer* — as well as lead to the expansion of cryptography to new protocols. These new tasks, falling under the heading of *quantum* cryptography, include, perhaps most prominently, the information-theoretically secure distribution of keys in the presence of eavesdroppers, by *quantum key distribution* [BB84].

This thesis seeks to add to them. *Quantum* encryption, i.e. encryption schemes for quantum data, is defined. Quantum *homomorphic* encryption, in particular, as described in [BJ15], would allow one to delegate computations on quantum information to a more powerful quantum computer, and *if secure*, this more powerful quantum computer would learn nothing from the states sent. Of course, then, *what does it mean for a quantum encryption scheme to be secure*? This is one of the major questions this thesis answers. Several security definitions are given, broadly divisible into the intuitive–and intuitively strong–definitions of semantic security and the more easily verifiable definitions of ciphertext indistinguishability, all of which are proven equivalent in the same settings, in analogy to the foundational result by Goldwasser and Micali in [GM84]. Private- and public-key quantum encryption schemes are also constructed from quantum-secure cryptographic primitives (one-way functions and trapdoor one-way permutations), and their security is proven. Most of the results are in the joint paper *Computational Security of Quantum Encryption* [ABF+16], to appear in the 9th International Conference on Information Theoretic Security (ICITS2016), that makes up a chapter of this thesis.

Section 1.2, Section 1.3, Section 3.1, and the conclusion Chapter 7 are also taken directly from the paper. It is noted again at the beginning of each when this is done. Some modifications have been made to some of them, and these are also noted.

1.2 Summary of Contributions and Techniques

This section (except for Subsection 1.2.3) is taken from the joint paper [ABF+16].

In this work, we establish quantum versions of several fundamental classical (*i.e.* "non-quantum") results in the setting of computational security. Following Broadbent and Jeffery [BJ15], we consider private-key and public-key encryption schemes for quantum data. In these schemes, the key is a classical bitstring[1], but both the plaintext and the ciphertext are quantum states. Key generation, encryption, and decryption are implemented by polynomial-time quantum algorithms. Such schemes

[1]While quantum keys might be of interest, they are not necessary for constructing secure schemes [BJ15].

admit an appropriate definition of indistinguishability security, following the classical approach [BJ15]: the quantum adversary is given access to an encryption oracle, and must output a challenge plaintext; given either the corresponding ciphertext or the encryption of $|0\rangle\langle 0|$ (each with probability 1/2), the adversary must decide which was the case.

Our main contributions are the following. First, we give several natural formulations of semantic security for quantum encryption schemes, and show that all of them are equivalent to indistinguishability. This cements the intuition that possession of the ciphertext should not help the adversary in computing anything about the plaintext. Second, we give two constructions of encryption schemes with semantic security: a private-key scheme, and a public-key scheme. The private-key scheme satisfies a stronger notion of security: indistinguishability against chosen ciphertext attacks (IND-CCA1). A more detailed summary of these contributions follows.

1.2.1 Semantic Security vs. Indistinguishability

Semantic security formalizes the notion of security of an encryption scheme under computational assumptions. Originally introduced by Goldwasser and Micali [GM84], this definition posits a game: an adversary is given the encryption of a message m and some side information σ, and is challenged to output the value of an objective function f evaluated at m. An encryption scheme is deemed secure if every adversary can be closely approximated by a *simulator* who is given only σ; crucially, the simulator must work for every possible choice f of objective function. This models the intuitive notion that having access to a ciphertext gives the adversary essentially no advantage in computing functions related to the plaintext.

While semantic security corresponds to a notion of security that is intuitively strong, it is cumbersome to use in terms of security proofs. In order to address this problem, Goldwasser and Micali [GM84] showed the equivalence of semantic security with another cryptographic notion, called *indistinguishability*. The intuitive description of indistinguishability is also in terms of a game, this time with a *single* adversary. The adversary prepares a pair of plaintexts m_0 and m_1 and submits them to

a challenger, who chooses a uniformly random bit b and returns the encryption of m_b. The adversary then performs a computation and outputs a bit v; the adversary wins the game if $v = b$ and loses otherwise. An encryption scheme is deemed secure if no adversary wins the game with probability significantly larger than $1/2$. This definition models the intuitive notion that the ciphertexts are indistinguishable: whatever the adversary does with one ciphertext, the outcome is essentially the same if run on the other ciphertext.

In Section 4.2, we define semantic security for the encryption of *quantum* data—thus establishing a parallel with the notions and results of encryptions as laid out by Goldwasser and Micali. When attempting to transfer the definition of semantic security to the quantum world, the main question one encounters is to determine the quantum equivalents of σ and $f(m)$ as described above (because of the no-cloning theorem [WZ82], we cannot postulate a polynomial-time experiment that simultaneously involves some quantum plaintext *and* a function of the plaintext—see Subsections 4.2.1 and 6.3.4 for further discussions related to this issue). We propose a number of alternative definitions in order to deal with this situation (Definition 4.2.1, Definition 4.4.2, and Definition 4.4.5.) Perhaps the most surprising is our definition of SEM (Definition 4.2.1), which does away completely with the need to explicitly define an analogues of the function f, instead relying on a *message generator* that outputs three registers, consisting of the "plaintext", "side information" and "target output" (there is no further structure imposed on the contents of these registers). Intuitively, we think of the adversary's goal being to output the value contained in the "target output" register. Formally, however, Definition 4.2.1 shows that the role of the "target output" register is actually to help the distinguisher: semantic security corresponding to the situation where no distinguisher has a non-negligible advantage in telling apart the real scenario (involving the adversary) and the ideal scenario (involving the simulator), *even given access to the "target output" system.* Our main result in this direction (see Section 4.2.3) is the equivalence between semantic security and indistinguishability for quantum encryption schemes:

Theorem 1.2.1. *A quantum encryption scheme is semantically secure if and only if it has indistinguishable encryptions.*

What is more, because our definitions and proofs hold when restricted to the classical case (and in fact can be shown as generalizations of the standard classical definitions), our contribution sheds new light on semantic security: to the best of our knowledge, this is the first time that semantic security has been defined *without* the need to explicitly refer to the function f.

1.2.2 Quantum Encryption Schemes

In Section 4.3, we give two constructions of quantum encryption schemes that achieve semantic security (and thus also indistinguishability, by Theorem 1.2.1.) Our constructions make use of two basic primitives. The first is a *quantum-secure one-way function* (qOWF). This is a family of deterministic functions which are efficiently computable in classical polynomial time, but which are impossible to invert even in quantum polynomial time. It is believed that such functions can be constructed from certain algebraic problems [MRV07, KK07]. The existence of qOWFs implies the existence of *quantum-secure pseudorandom functions* (qPRFs) [Zha12]. We show that a qPRF can, in turn, be used to securely encrypt quantum data with classical private keys. More precisely, we have the following:

Theorem 1.2.2. *If quantum-secure one-way functions exist, then so do IND-CCA1-secure private-key quantum encryption schemes.*

The second basic primitive we consider is a *quantum-secure one-way permutation with trapdoors* (qTOWP). In analogy with the classical case, a qTOWP is a qOWF with an additional property: each function in the family is a permutation whose efficient inversion is possible if one possesses a secret string (the trapdoor). While our results appear to be the first to consider applications to quantum data, the notion of quantum security for trapdoor permutations is of obvious relevance in the security of classical cryptosystems against quantum attacks. Some promising candidate qTOWPs from lattice problems are known [PW08, GPV08]. We show that such functions can be used to give secure public-key encryption schemes for quantum data, again using only classical keys.

Theorem 1.2.3. *If quantum-secure trapdoor one-way permutations exist, then so do semantically secure public-key quantum encryption schemes.*

We remark that Theorem 1.2.2 and Theorem 1.2.3 are analogues of standard results in the classical literature [Gol04].

1.2.3 Author's Contributions

The main contributions of the author of this thesis to the joint paper Computational Security of Quantum Encryption [ABF+16], which makes up Chapter 4 of this thesis, are the definitions for semantic security SEM (Definition 4.2.1), SEM2 (Definition 4.4.2), SEM3 (Definition 4.4.5), their equivalence (Theorem 1.2.1, Theorem 4.2.2 and Theorem 4.2.3) with IND (Definition 4.1.3) and IND' (Definition 4.4.7). This includes the definitions and results in Sections 4.2 and 4.4, but not the proof of Theorem 4.2.3 as it appears in Section 4.2, nor the definitions for IND and IND' in Section 4.4. Further contributions in this thesis include, in Chapter 5, full proofs for results for cryptographic primitives used (and sketched or omitted) in the paper, closely following the treatment in [Gol04]. These are the quantum version of the Goldreich-Levin theorem (Theorem 5.2.1), and a stronger proof of security for the construction of a qPRG from a qTOWP (Theorem 5.3.1). Finally, in Section 6.3, more alternative definitions for semantic security are given and semantic security is further motivated. In Subsection 6.3.4, in particular, obstacles to defining semantic security with a channel or noncomputable classical function for F are discussed in detail.

1.3 Related Work

This section is from the joint paper [ABF+16].

Prior work has considered the computational security of quantum methods to encrypt classical data [OTU00, Kos07, XY12]. Information-theoretic security for the encryption of quantum states has been considered in the context of the one-time pad [AMTdW00, BR03, HLSW04, Leu02], as well as entropic security [Des09, DD10].

Computational indistinguishability notions for encryption in a quantum world were proposed in two independent and concurrent works [BJ15, GHS15]. While [BJ15] considers the encryption of quantum data (and proposes the first constructions based on hybrid classical-quantum encryption), [GHS15] considers the security of *classical* schemes which can be accessed in a quantum way by the adversary.

The results of [GHS15] are part of a line of research of *"quantum-secure classical cryptography"*, which investigates the security of classical schemes against quantum adversaries, with the goal of finding "quantum-safe" schemes. In this scenario, [BZ13] considers quantum indistinguishability under chosen plaintext and chosen ciphertext attacks. This definition was improved in [GHS15] to allow for a quantum challenge phase. The latter paper also initiates the study of quantum semantic security of classical schemes and gives the first classical construction of a quantumly secure encryption scheme from a family of quantum-secure pseudorandom permutations. Another quantum indistinguishability notion in the same spirit has been suggested (but not further analyzed) in [Vel13, Def. 5.3].

Several previous works have considered how classical security proofs change in the setting of quantum attacks (see, e.g., [Unr10, FKS+13, Son14].) Our results can be viewed as part of this line of work; one distinguishing feature is that we are able to extend classical security proofs to the setting of quantum functionality secure against quantum adversaries. This setting has seen increasing interest in the past decade, with progress being made on several topics: multi-party quantum computation [BOCG+06], secure function evaluation [DNS10, DNS12], one-time programs [BGS13], and delegated quantum computation [BFK09, Bro15].

1.4 Structure of This Thesis

The remainder of this thesis is structured as follows:

Chapter 2 gives some background on developments in modern cryptography, quantum information theory generally and quantum cryptography specifically. Section 2.8 is taken from the joint paper [ABF+16].

Preliminaries are given in Chapter 3, including background in linear algebra, quantum information and quantum computing, as well as the notation used in quantum information. The last section, Section 3.9 contains the definitions and results from modern cryptography whose quantum counterparts are given in this thesis. Section 3.1, Section 3.6 and Subsection 3.8.1 are taken from the joint paper [ABF+16].

Chapter 4 is taken from the joint paper [ABF+16]. In Section 4.1, private-key and public-key encryption for quantum states and the security of such schemes, as ciphertex indistinguishability (IND, IND-CPA and IND-CCA1), are defined. Section 4.2 defines semantic security (SEM) for quantum encryption schemes, and proves its equivalence with indistinguishability. Section 4.3 gives two constructions for quantum encryption schemes and proves their security from the existence of quantum-secure one-way functions and quantum-secure trapdoor one-way permutations. Section 4.4 defines semantic security in two more ways (SEM2, SEM3) and indistinguishability in another that is common in cryptography (IND'), and all of the security definitions given so far are proven equivalent.

Some omitted or sketched results for cryptographic primitives used in the constructions are proven in detail in Chapter 5.

In Chapter 6, further variations on security definitions are given and discussed, including indistinguishability between encryptions of pairs of generated messages, rather than a single message and a fixed trivial message in Section 6.1, extensions to multiple messages in Section 6.2, the omission of the absolute values in the semantic security definitions in Subsection 6.3.1, semantic security with the swap test as the distinguisher in Subsection 6.3.2, security in which the simulator never has oracle access under CPA or CCA1 in Subsection 6.3.3, semantic security with a channel as the target in Subsection 6.3.4, and security for more general message distributions in Subsection 6.3.5.

Finally, the concluding chapter, Chapter 7, also mostly taken from the joint paper [ABF+16], discusses extensions, including non-uniform adversaries, the open problems of the equivalence of IND and an appropriate definition of semantic security with a channel for F, and defining CCA2 security.

Chapter 2

Background

This chapter discusses some of the most important theoretical results in cryptography and quantum information leading up to the development of quantum cryptography. This starts with the development of modern cryptography, including provably secure encryption before computers in Section 2.1, followed by security and public-key cryptography against computationally-bounded adversaries in Section 2.2. Next, early important theoretical results in quantum mechanics and quantum information are outlined in Sections 2.3 and 2.4, respectively. Then, the initial motivation and development of quantum computers are summarized in Section 2.5, and the design of some important quantum algorithms and results about their computational power follow in Section 2.5. An important quantum protocol, quantum teleportation, is described in Section 2.7. Finally, quantum cryptography is discussed and motivated in Section 2.8.

2.1 Cryptography Before the Digital Computer

Historically, every cipher used to encrypt messages was eventually broken [KL07], and there wasn't even any notion of what it meant for a cipher to be unbreakable, that is, until Claude Shannon's 1949 paper *Communication Theory of Secrecy Systems* [Sha49]. In this paper, he introduced the definition of *perfect secrecy*: perfect secrecy holds if the probability that the message is x, given that its encryption is c, is equal to the probability that the message is x, for all possible x, c, i.e. knowing the encryption

of a message does not change the likelihood that it is a particular message. The *one-time pad* (or *Vernam's cipher*) is one such cipher having this property, and any other must be very similar in that the key space must be as large as the message space, effectively meaning that the keys must be as long as the messages themselves, a very impractical requirement. "One-time" refers to the fact that using the same key to encrypt multiple messages is not safe, making the cipher inefficient, too.

2.2 Cryptography in the Digital World

However, with the advent of the digital computer, the idea of computational security, in which the power of attackers is bounded, replaced perfect secrecy, and secure communication over an insecure channel without a previously shared secret (i.e. a private key) became possible. "*We stand today on the brink of a revolution in cryptography.*" Thus began the 1976 paper *New Directions in Cryptography* by Whitfield Diffie and Martin Hellman [DH76], in which they described the *Diffie-Hellman key exchange* (or *Diffie-Hellman-Merkle key exchange*, for Ralph Merkle's precursory and initially *rejected* work as an undergraduate [Mer78, Mer10]) and introduced the notion of a *public-key cryptosystem*, both allowing such secure communication. They also described *digital signatures*, which would allow an individual sending a message to sign it in such a way that anyone can verify its authenticity. These three ideas marked the birth of public-key cryptography, and public-key encryption schemes were soon published, the first being RSA (for Ronald L. Rivest, Adi Shamir and Leonard Adleman, the authors), based on the difficulty of prime factoring, in 1978 [RSA78]. It later became known that the concept of public-key encryption, RSA and Diffie-Hellman key exchange were discovered earlier and independently at the British intelligence agency GCHQ in 1970 by James Henry Ellis [Ell70], in 1973 by Clifford Cocks [Coc73] and in 1974 by Malcolm J. Williamson [Wil76], respectively; their research was classified until 1997.

Yet it wasn't until 1982 that the notion of security of a cryptosystem was actually made rigorous in the computational setting, by Shafi Goldwasser and Silvio Micali [GM82]. In their 1984 paper [GM84], they furthered their defininition to *semantic*

security: an encryption scheme is semantically secure if access to the encryption of a message does not allow an attacker to compute partial information about the message that he or she could not compute without the ciphertext. While intuitive, this "partial information" was actually modelled as a function from the message space, and semantic security then means quantifying over *all* such functions—even *non-computable* ones—and *all* message distributions (generated in polynomial time), a daunting task. However, in the same paper, Goldwasser and Micali reduced verifying semantic security to checking if what they called *polynomial security* (now usually called *ciphertext indistinguishability*) holds, which is defined to be the case when, given the ciphertext of one from a pair of two chosen equal-length messages, no polynomially bounded adversary can tell to which message it corresponds.

Not only did they define security intuitively and rigorously, they provided a practical means to prove an encryption scheme secure. It was for this paper—and their other work on digital signatures, random functions, interactive proofs and zero-knowledge protocols—that they received the Turing award, the "Nobel prize of computing", in 2012; Goldwasser and Micali "*laid the foundations of modern theoretical cryptography, taking it from a field of heuristics and hopes to a mathematical science*" [ACM13].

Since Goldwasser and Micali, there have been numerous variations in the definitions of security, reflecting variations in the definitions of the adversaries; these include security for multiple messages, and security under chosen plaintext attacks (CPA) and two different kinds of chosen ciphertext attacks (non-adaptive or a priori, CCA1 [NY90], and adaptive or a posteriori, CCA2 [RS92]). Furthermore, in 1993, Goldreich contributed a uniform-complexity treatment of security, replacing the (non-uniform) families of circuits with Turing machines, and also renamed polynomial security *indistinguishability of encryptions* or *ciphertext indistinguishability* [Gol93].

Cryptographic primitives have also been important in the construction of secure encryption schemes, in particular starting from one-way functions in the private-key setting [HILL99, GGM86, Gol04] and trapdoor one-way permutations in the public-key setting [GL89, Gol04].

A candidate trapdoor one-way permutation that is secure against classical adversaries and still widely used to this day is the RSA function, on which the RSA cryptosystem is based and whose security depends on the difficulty of factoring. However, the RSA function, and the RSA scheme, by extension, are not secure against quantum adversaries, due to *Shor's algorithm for integer factorization* [Sho94].

Some of these definitions and results that are most relevant to this thesis are given in Section 3.9.

2.3 The Quantum Era

Quantum mechanics, to this day still extremely accurate in its predictions, has refuted much of our classical intuition about the universe. Several important experiments mark its development, but this section will focus on outlining some of the most important theoretical results.

In 1923, in his research for his PhD thesis [dB24], Louis de Broglie hypothesized that matter behaves like waves, having wavelengths (the *de Broglie wavelength*), so that, for example, the interference patterns in the double-slit experiment could even be observed with electrons instead of light. His so-called *matter waves* fall under the more general concept of *wave-particle duality*, the property of physical objects situationally exhibiting both wave and particle properties.

Werner Heisenberg, Max Born, and Pascual Jordan developed the first complete formulation of quantum mechanics as *matrix mechanics* in 1925 [Hei25, BJ26, BHJ26], which was followed by Erwin Schrödinger's *wave mechanics* and his proof of equivalence in 1926. In wave mechanics, one of the fundamental postulates is the evolution of quantum systems according to *Schrödinger's equation*, a partial differential equation involving the system's Hamiltonian, which describes its energy states.

In 1927, Heisenberg introduced his *uncertainty principle* [Hei27], which predicts that the more precisely a particle's momentum is measured, the less precisely can its position be, and vice-versa, as an inequality bounding the product of their standard deviations from below (by the reduced Planck's constant, divided by 2). If quantum

mechanics were complete as a theory, this principle suggested that particles do not even have simultaneously well-defined positions and momenta.

That same year, John von Neumann [vN27] and Lev Landau [SS82] independently introduced the *density matrix*; von Neumann, for quantum statistical mechanics and a theory of measurement; and, Landau, to describe subsystems of composite systems.

Then, in 1930 and 1932, Dirac [Dir30] and von Neumann [vN55], respectively, laid the mathematical foundations of quantum mechanics, including the Dirac–von Neumann axioms, describing the evolution of quantum systems in the language of Hilbert spaces and operators on them, preceded by von Neumann's 1927 paper with David Hilbert and Lothar Wolfgang Nordheim [HvN28]. In von Neumann's 1932 text, he also introduced what later become known as the von Neumann entropy, the starting point of Quantum Shannon theory. Of course, before this, Hilbert had initiated the study of infinite-dimensional Hilbert spaces [Hil06] (concrete ones for integral equations, von Neumann gave their abstract definition) and their corresponding spectral theory, remarking later "*I developed my theory of infinitely many variables from purely mathematical interests, and even called it 'spectral analysis' without any presentiment that it would later find application to the actual spectrum of physics.*" [Ste73]

Several new predictions from the theory followed, and notably that made by the *EPR paradox* [EPR35] in 1935 by Albert Einstein, Boris Podolsky and Nathan Rosen. They described a thought experiment in which a pair of particles could interact in such a way that the measuring the position of one completely determines the position of the other, and similarly for the momenta. Then, one particle's position could be measured, and the other's momentum, each to arbitrary precision, and from each of these, the other two quantities could be inferred, contrary to the uncertainty principle. If the uncertainty principle must hold, then somehow a measurement of one particle "affects" the other, to break these correlations, and this can occur instantaneously and independently of the distance between the two, and hence faster than the speed of light. EPR rejected this, with Einstein calling it "*spooky action at a distance*", and concluded that quantum mechanics was incomplete, so that hidden variables (for the positions and momenta of particles, among others) were necessary for a complete

description of physical reality. However, in 1964, John Stewart Bell derived *Bell's inequality* [Bel64], which put the predictions made by any local hidden variable theory (in particular, for particle *spin*) and those of quantum mechanics in conflict, concluding with *Bell's theorem*, ruling out such local hidden variables. The phenomenon described in EPR is what Schrödinger named *entanglement*, calling it not "*one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought.*" [Sch35] Since Bell's inequality and the derivation of other so-called *Bell inequalities*, there have been several tests of them, and recently, a loophole-free test [HBD+15].

2.4 Quantum Information Theory

Scientists took further interest in the information encoded in quantum systems and more abstract mathematical characterizations of open quantum systems and their evolution.

In 1955 and in 1940, William Forrest Stinespring [Sti55] and Mark Naimark [Nai40] published their dilation theorems, respectively. *Stinespring's dilation theorem* (stated in Theorem 3.4.12, although different from the original result) allows one to represent every *quantum channel*, which characterize the evolution of open quantum systems without measurement, as a unitary operator, which captures the deterministic evolution of closed quantum systems, on a larger Hilbert space, while *Naimark's dilation theorem* allows one to represent every *positive operator-valued measure (POVM)*, the most general type of measurement, as a *projection-valued measure (PVM) or spectral measure*, on a larger Hilbert space.

Further important initial developments in quantum information theory were made in the 1970s and 1980s. In 1970, Stephen Wiesner invented conjugate coding and unforgeable quantum money, but the results were unpublished until 1983 [Wie83], despite inspiring some of the first developments in quantum cryptography (see Section 2.8). In 1973, Alexander Holevo proved a theorem, now named in his sake [Hol73], which implies that from n qubits, only n classical bits of information can be

retrieved, despite requiring, in general, 2^n complex numbers to represent n qubits. Roman Stanisław Ingarden in his 1976 paper *Quantum Information Theory* showed that Shannon's information theory could not be generalized directly to quantum systems, but laid forth generalizations despite this obstacle [Ing76]. Then, William Wootters and Wojciech Zurek [WZ82], and independently Dennis Dieks [Die82] proved the no-cloning theorem in 1982, a no-go theorem for the impossibility to copy arbitrary quantum states. The no-cloning theorem is stated in the preliminaries as Theorem 3.4.1.

2.5 The Dawn of Quantum Computing

The idea of quantum computing, however, was not introduced until the early 1980s. Foreshadowing it, in 1975, R. P. Poplavskii showed that simulating quantum systems on classical computers is computationally infeasible: "*The quantum-mechanical computation of one molecule of methane requires* 10^{42} *grid points. Assuming that at each point we have to perform only 10 elementary operations, and that the computation is performed at the extremely low temperature* $T = 3 \times 10^{-3}K$*, we would still have to use all the energy produced on Earth during the last century.*" (as quoted by Manin) [Pop75]. Then, in 1980, Yuri Manin [Man80] proposed the idea of a quantum computer, suggesting that quantum computers could be used to more efficiently simulate quantum systems, with Richard Feynmann independently suggesting the same with a universal quantum simulator [Fey82]. In 1980, Paul Benioff proposed quantum mechanical Hamiltonian models of Turing machines [Ben80, Ben82], followed in 1993 by David Albert's quantum mechanical automaton, a true quantum computer [Alb83], and then in 1985, David Deutsch developed the more general quantum Turing machines, introducing a physical Church-Turing principle stating: "*Every finitely realizable physical system can be perfectly simulated by a universal model computing machine operating by finite means*", and introducing universal quantum Turing machines, quantum Turing machines that can simulate any other with at most a polynomial increase in running time [Deu85]. In 1989, Deutsch also proposed the quantum circuit model, then *quantum computational networks*, as well as the definition of a

universal gate set, a set of unitaries from which the constructable quantum circuits can approximate all n-qubit unitaries, for any n [Deu89]. In this paper, he also defined what's now known as the *Deutsch gate*, a 3-qubit quantum gate, and proved that it is universal. In 1993, quantum Turing machines were further developed by Ethan Bernstein and Umesh Vazirani [BV93], and the two models of quantum computers, quantum Turing machines and quantum circuits, were then shown equivalent by Andrew Yao [Yao93]. Further universal gate sets were subsequently identified, and in 1995 Robert Solovay [DN06] and in 1997 Alexei Kitaev [Kit97] independently proved the Solovay-Kitaev theorem, which states that any universal gate set can be used to approximate any unitary with only $O(\log^c(1/\epsilon))$ gates, where ϵ is the desired accuracy. Kitaev's proof was the design of an efficient algorithm to build such a circuit. In particular, this implies that quantum algorithms implemented with any gate set will have the same running time, up to polynomial increases or decreases. Finally, returning to the initial motivation for quantum computing, Seth Lloyd proved in 1996 that universal quantum computers, in the quantum circuit model, can simulate any local quantum system [Llo96].

The first *quantum error-correcting codes* were designed by Shor [Sho95] and Andrew Steane [Ste96] in 1995, and *fault-tolerant quantum computation* was also iniatiated Shor [Sho96]. Together, these would protect quantum data from accumulating errors in storage and during computations, respectively.

The density matrix formalism for quantum circuits, which is common in quantum computing and used in this thesis, allowing more general quantum channels and even measurements in the middle of computations, was developed and proven equivalent to the unitary gate model in 1998 by Dorit Aharonov, Kitaev and Noam Nisan [AKN98].

2.6 Quantum Algorithms and Quantum Complexity Theory

Around this time, too, the study of quantum complexity theory was initiated. In 1992, David Deutsch and Richard Jozsa conceived an exact polynomial-time quantum oracle algorithm (the Deutsch-Jozsa algorithm [DJ92]) to solve a problem that cannot be solved in polynomial-time on a deterministic classical computer, i.e. that there exists an oracle (or sequence of oracles, more specifically) f relative to which $\mathbf{EQP}^f \not\subseteq \mathbf{P}^f$, where $\mathbf{EQP}^f$ is the set of all decision problems solvable by exact polynomial-time quantum algorithms with oracle access to f, and $\mathbf{P}^f$ is the set of decision problems solvable by deterministic polynomial-time Turing machines with oracle access to f. Bernstein and Vazirani built upon the work of Deutsch and Jozsa in their 1993 paper [BV93] to prove the existence of an oracle f relative to which $\mathbf{EQP}^f \not\subseteq \mathbf{BPP}^f$, where $\mathbf{BPP}^f$ is the set of decision problems solvable with bounded error by probabilistic polynomial time Turing machines with oracle access to f, so that not even probabilistic classical computers with oracle access to f can solve the problem efficiently. They also remarked that deterministic polynomial-space algorithms, which solve the decision problems in **PSPACE**, could simulate polynomial-time quantum algorithms and hence concluded that $\mathbf{BQP} \subseteq \mathbf{PSPACE}$, where **BQP** is the set of decision problems solvable with bounded error and in polynomial time by quantum algorithms. Continuing along these lines, in 1994, Daniel Simon devised an oracle problem (Simon's problem) infeasible to probabilistic polynomial-time Turing machines and a polynomial-time quantum algorithm (Simon's algorithm) to solve it, proving the existence of an oracle A relative to which $\mathbf{BPP}^A \subsetneqq \mathbf{BQP}^A$ [Sim94].

Inspired by Simon's work, Peter Shor, in 1994, developed polynomial-time quantum algorithms for integer factorization (now known as *Shor's algorithm* [Sho94]) and the discrete logarithm, problems for which no known efficient classical algorithms exist, suggesting (but not proving) $\mathbf{BPP} \subsetneqq \mathbf{BQP}$. These two algorithms could be used to break many of the cryptographic protocols still used widely today, and the results were some of the first strong evidence that quantum computers were superior to classical computers (along with quantum simulation, as described in the previous

section, Section 2.5, and quantum key distribution, in the the last section of this chapter, Section 2.8). As a response, much more interest in the field developed, as well as in post-quantum cryptography, i.e. cryptography with classical computers that is secure against quantum computers.

Another important algorithm developed in this period is Grover's search algorithm [Gro96], an oracle algorithm, by Lov Grover in 1996, able to find a marked entry in a database of N entries in $O(\sqrt{N})$ time, a quadratic improvement over the classically optimal $O(N)$. Around the same time, the algorithm's asymptotic optimality was proven by Charles H. Bennett, Ethan Bernstein, Gilles Brassard and Umesh Vazirani [BBBV97], as a consequence of their more general result that "*relative to an oracle chosen uniformly at random, with probability 1, the class **NP** (of decision problems whose yes instances can be verified with polynomial-length proofs in polynomial-time by deterministic Turing machines) cannot be solved on a quantum Turing machine in time* $o(\sqrt{N})$". While not conclusive, this suggest that $\mathbf{NP} \not\subseteq \mathbf{BQP}$, i.e. there exist problems in **NP** that quantum computers still cannot solve efficiently. In fact, they also proved a similar oracle result for $\mathbf{NP} \cap \mathbf{co\text{-}NP}$ instead of simply **NP**.

2.7 Quantum Teleportation

In 1993, quantum teleportation was invented by Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William Wootters [BBC+93]. This protocol would allow one party to transfer an arbitrary quantum state to another, given only an entangled state shared between the two and using local operations and the communication of classical bits from the party sending the state to the receiver. The current record distance for quantum teleportation is 143 km, between the two Canary Islands of La Palma and Tenerife [MHS+12]. Quantum teleportation is used to illustrate quantum circuit notation, which is used minimally in this thesis, as Figure 1.

2.8 Cryptography in a Quantum World

The following section is from the joint paper [ABF+16].

Cryptography is one of the areas that is most seriously impacted by the potential of quantum information processing. As described in Section 2.6, the security of most cryptographic primitives in use today relies on the hardness of computational problems that are easily broken by adversaries having access to a quantum computer [Sho94].

While the impact of quantum computers on cryptanalysis is tremendous, quantum mechanics itself predicts physical phenomena that can be exploited in order to achieve new levels of security. These advantages were already mentioned in the late 1970's in pioneering work of Wiesner [Wie83] (as described in Section 2.4), and have led to the very successful theory of quantum key distribution (QKD) [BB84], which has already seen real-world applications [ABB+14]. QKD achieves information-theoretically secure key expansion, and has the advantage of relatively simple hardware requirements (notwithstanding a long history of successful attacks to QKD at the implementation level [ABB+14]).

The cryptographic possibilities of quantum information go well beyond QKD. Indeed, quantum copy-protection [Aar09], quantum money [Wie83, AC12, MS10] and revocable time-release encryption [Unr14] are just some examples where properties unique to quantum data enable new cryptographic constructions. Thanks in part to these tremendous cryptographic opportunities, we envisage an increasing need for an information infrastructure that enables quantum information. Such an infrastructure will be required to support:

- **Quantum functionality:** honest parties can store, exchange, and compute on quantum data;
- **Quantum security:** quantum functionality is protected against quantum adversaries.

The current state-of-the-art is lacking even the most basic cryptographic concepts in the context of quantum functionality and quantum adversaries. In particular, the

study of encryption of quantum data (which is arguably one of the most fundamental building blocks) has so far been almost exclusively limited to the quantum one-time pad [AMTdW00] and other aspects of the information-theoretic setting [Des09, DD10] (one notable exception being [BJ15]). The achievability of other basic primitives such as public-key encryption has not been thoroughly investigated for the case of fully quantum cryptography. This thesis and the joint paper [ABF+16] on which it is based take some of the first steps in this direction.

Chapter 3

Preliminaries

Most of the following preliminaries can be found in the standard quantum information and quantum computing textbooks [NC00] and [KLM07]. The chapter is structured as follows:

Basic notation for classical concepts is given in Section 3.1. Concepts in linear algebra important in quantum information are given in Section 3.2. Quantum states are defined in Section 3.3. Admissible maps on quantum states, i.e. the operations that can be applied to them, are defined and some results about them are presented in Section 3.4. Quantum circuits are defined in Section 3.5. Efficient classical and quantum computation are defined in Section 3.6. Negligible functions, informally, functions that decrease to 0 faster than any inverse polynomial, are defined and some of their basic properties are given in Section 3.7. Ensembles of quantum states and results on the probability of distinguishing them are given in Section 3.8, with the quantum one-time pad and computational indistinguishability defined in Subsections 3.8.1 and 3.8.2, respectively. Finally, definitions and results in modern cryptography in the classical setting whose quantum analogues this thesis uses or defines are given in Section 3.9.

3.1 Binary Strings, Functions on Them, and the One-time Pad

This section is taken from the joint paper [ABF+16].

Let $\mathbb{N}$ be the set of positive integers. For $n \in \mathbb{N}$, we set $[n] = \{1, \cdots, n\}$. Define $\{0,1\}^* := \cup_n \{0,1\}^n$. An element $x \in \{0,1\}^*$ is called a bitstring or binary string, and $|x|$ denotes its length, *i.e.*, its number of bits. We reserve the notation 0^n (resp., 1^n) to denote the n-bit string with all zeroes (resp., all ones).

For a finite set X, the notation $x \xleftarrow{\$} X$ indicates that x is selected uniformly at random from X, i.e. each x has probability $\frac{1}{|X|}$ of being selected. For a probability distribution S, the notation $x \leftarrow S$ indicates that x is sampled according to S. Given finite sets X and Y, the set of all functions from Y to X is denoted X^Y (or sometimes $\{X \to Y\}$).

We will usually consider functions f acting on binary strings, that is, of the form $f : \{0,1\}^n \to \{0,1\}^m$, for some positive integers n and m. We will also consider function families $f : \{0,1\}^* \to \{0,1\}^*$ defined on bitstrings of arbitrary size. One can construct such a family simply by choosing one function with input size n, for each n. We will sometimes abuse notation by stating that $f : \{0,1\}^n \to \{0,1\}^m$ defines a function family; in that case, it is implicit that n is a parameter that indexes the input size and m is some function of n (usually a polynomial) that indexes the output size. Given a bitstring y and a function family f, the preimage of f under y is defined by $f^{-1}(y) := \{x \in \{0,1\}^* : f(x) = y\}$.

Given two bitstrings x and y of equal length, we denote their bitwise XOR, or equivalently, their bitwise sum modulo 2, by $x \oplus y$. Recall that the *classical one-time pad* encrypts a plaintext $x \in \{0,1\}^n$ by XORing it with a uniformly random string (the key) $r \xleftarrow{\$} \{0,1\}^n$. Decryption is performed by repeating the operation, *i.e.*, by XORing the key with the ciphertext. Since the uniform distribution on $\{0,1\}^n$ is invariant under XOR by x, the ciphertext is uniformly random to parties having no knowledge about r [Sha49]. A significant drawback of the one-time pad is the key length. In order to reduce the key length, one may generate r pseudorandomly; this

key-length reduction requires making computational assumptions about the adversary.

3.2 Linear Algebra

We are concerned with finite-dimensional vectors spaces only in this thesis. It is assumed that the reader is familiar with the basics of linear algebra (vectors spaces, bases and orthonormal bases, linear transformations and matrices, eigenvalues and eigenvectors, etc.).

Definition 3.2.1 (Normed vector space)**.** A *normed vector space* is a tuple $(V, \|\cdot\|)$, where V is a vector space over the field $\mathbb{F} = \mathbb{C}$ or $\mathbb{R}$, and $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ is a norm, i.e. it satisfies, for all $x, y \in V$ and $\alpha \in \mathbb{F}$:

1. $\|\alpha x\| = |\alpha| \|x\|$,
2. $\|x + y\| \leq \|x\| + \|y\|$, and
3. $\|x\| = 0 \iff x = 0$.

Definition 3.2.2 (Inner product space)**.** A *complex inner product space* is a tuple $(V, \langle\cdot,\cdot\rangle)$, where V is a complex vector space and $\langle\cdot,\cdot\rangle : V \times V \to \mathbb{C}$ is an inner product, i.e., it satisfies for all $x, y, z \in V$ and $\alpha \in \mathbb{C}$:

1. $\langle y, x\rangle = \overline{\langle x, y\rangle}$ (conjugate symmetry),
2. $\langle x, \alpha y\rangle = \alpha\langle x, y\rangle$
   $\langle x, y + z\rangle = \langle x, y\rangle + \langle x, z\rangle$ (linearity in the *second* argument, the physics convention), and
3. $\langle x, x\rangle \geq 0$, and
   $\langle x, x\rangle = 0 \iff x = 0$ (positive definiteness).

A norm $\|\cdot\| : V \to \mathbb{R}$ can be defined from the inner product by, for $x \in V$, $\|x\| = \sqrt{\langle x, x\rangle}$. This corresponds to the Euclidean norm, usually denoted by $\|\cdot\|_2$, but in this thesis, it will just be denoted by $\|\cdot\|$.

An inner product space which is a complete metric space with respect to the metric given by the above norm is called a *Hilbert space*. Finite-dimensional inner product spaces are Hilbert spaces. In this thesis, we are only concerned with finite dimensional complex vectors spaces, concretely $\mathbb{C}^n$, for $n \in \mathbb{N}$.

Definition 3.2.3 (Identity)**.** Let V be a vector space. The identity (on V) is the linear transformation $\mathbb{1}_V : V \to V$ defined by $\mathbb{1}_V(x) = x$, for all $x \in V$

The set of linear transformations $U \to V$ is denoted by $\mathcal{L}(U, V)$, and the set of linear transformations (or linear operators) $V \to V$ by $\mathcal{L}(V)$. These are also vector spaces.

Definition 3.2.4 (Adjoint)**.** Let $A : U \to V$ be a linear transformation from $(U, \langle\cdot,\cdot\rangle_U)$ to $(V, \langle\cdot,\cdot\rangle_V)$, finite-dimensional (complex) Hilbert spaces. The *adjoint* of T is a linear transformation $A^\dagger : V \to U$ satisfying $\langle v, Au\rangle_V = \langle A^\dagger v, u\rangle_U$ for all $u \in U, v \in V$.

Note that adjoints always exist for bounded/continuous linear operators between Hilbert spaces and is unique (hence the notation). For us, the matrix of the adjoint of a linear transformation is the conjugate transpose of the matrix of the linear transformation, i.e. $[A^\dagger]_{kj} = \overline{[A]_{jk}}$.

Proposition 3.2.5 (Adjoint properties)**.** *For $A, C : U \to V, B : V \to W, \alpha \in \mathbb{C}$,*

1. $(A^\dagger)^\dagger = A$,
2. $(BA)^\dagger = A^\dagger B^\dagger$, *and*
3. $(\alpha A + C)^\dagger = \overline{\alpha} A^\dagger + C^\dagger$.

Definition 3.2.6 (Normal operator)**.** A linear operator $A : \mathcal{H} \to \mathcal{H}$ is *normal* if $A^\dagger A = A A^\dagger$.

Definition 3.2.7 (Self-adjoint operator)**.** A linear operator $A : \mathcal{H} \to \mathcal{H}$ is *self-adjoint* (or *Hermitian*) if $A^\dagger = A$.

An operator is self-adjoint if and only if it is normal and its spectrum is real.

Definition 3.2.8 (Positive semidefinite operator)**.** A linear operator $A : \mathcal{H} \to \mathcal{H}$ is *positive semidefinite* if it is self-adjoint and $\langle x, Ax\rangle \geq 0$ for all $x \in \mathcal{H}$. This is often denoted by $A \geq 0$.

An operator is positive semidefinite if and only if it is normal and has only non-negative eigenvalues. $A : \mathcal{H} \to \mathcal{H}$ is also positive semidefinite if and only if $A = C^\dagger C$, for some operator $C : \mathcal{H} \to \mathcal{H}$. Furthermore, there is a unique positive semidefinite operator C satisfying this equality, and it is denoted by $\sqrt{A}$.

Definition 3.2.9 (Orthogonal projection)**.** A linear operator $P : \mathcal{H} \to \mathcal{H}$ is an *orthogonal projection* if $P^2 = P^\dagger = P$.

An operator is an orthogonal projection if and only if it is normal and its spectrum is a subset of $\{0, 1\}$. Orthogonal projections are therefore positive semidefinite.

Definition 3.2.10 (Unitary operator)**.** A linear operator $U : \mathcal{H} \to \mathcal{H}$ is *unitary* if $U^\dagger U = UU^\dagger = \mathbb{1}_{\mathcal{H}}$, so that $U^{-1} = U^\dagger$.

An operator is unitary if and only if it is normal and its spectrum is a subset of the complex unit circle.

Notation 3.2.11 (Dirac Bra-ket Notation)**.** *Hilbert spaces are denoted by $\mathcal{H}$, and every vector $x \in \mathcal{H}$ corresponds uniquely to a linear functional $L_x : \mathcal{H} \to \mathbb{C}$, defined by*

$$L_x(y) = \langle x, y\rangle . \tag{1}$$

By the Riesz representation theorem, this correspondence is a bijection between elements of $\mathcal{H}$ and linear functionals on $\mathcal{H}$, and it is also anti-linear, i.e. $L_{x+\alpha y} = L_x + \alpha L_y$. When $\mathcal{H} = \mathbb{C}^n$, linear transformations are given by matrix multiplication, and $L_x = x^\dagger$, i.e. the transpose of x, where x is interpreted as an n by 1 matrix. We denote vectors in $\mathcal{H}$ by kets, *$|\psi\rangle, |\varphi\rangle$ (or with subscripts or superscripts on ψ or φ within these kets), and the corresponding linear functionals as* bras, *$\langle\psi|, \langle\varphi|$ (or with subscripts or superscripts on ψ or φ within these kets), so that when $\mathcal{H} = \mathbb{C}^n$, $(|\psi\rangle + \alpha|\varphi\rangle)^\dagger = \langle\psi| + \overline{\alpha}\langle\varphi|$, and $\langle\psi|\varphi\rangle := \langle\psi||\varphi\rangle$ is the inner product of $|\psi\rangle$ (on the left) and $|\varphi\rangle$ (on the right). For convenience, $|i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle$ is written $|i_1 i_2 \ldots i_n\rangle$, for $i_j = 0, 1, +, -$, and*

$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$ is written $|\psi_1\rangle\,|\psi_2\rangle \ldots |\psi_n\rangle$, for any other ψ_i. Often, $|0^n\rangle$ will simply be written $|0\rangle$; this should be understood from the context, in which the state is composed of multiple qubits.

Definition 3.2.12 (Tensor product)**.** Let U and V be vector spaces. Then, the tensor product space $U \otimes V$ is the quotient of the set of all finite linear combinations of formal symbols $u \otimes v$, $u \in U, v \in V$ by equivalence relation $\sim$ generated by the following, for $u, u' \in U, v, v' \in V, \alpha \in \mathbb{C}$:

1. $(u + u') \otimes v \sim u \otimes v + u' \otimes v$, and $u \otimes (v + v') \sim u \otimes v + u \otimes v'$, and
2. $\alpha u \otimes v \sim u \otimes \alpha v \sim \alpha(u \otimes v)$.

By convention, $U \otimes \mathbb{C}$ and $\mathbb{C} \otimes U$ are defined simply to be U.

$U \otimes V$ is, in fact, a vector space.

Note that $U \otimes \mathbb{C}, \mathbb{C} \otimes U$ and U are all isomorphic, by $u \otimes \alpha \leftrightarrow \alpha \otimes u \leftrightarrow \alpha u$.

The definition can be extended straightforwardly to arbitrarily many vector spaces, or one can note that $(U \otimes V) \otimes W$ and $U \otimes (V \otimes W)$ are isomorphic as vector spaces and define finite tensor products recursively (noting that the tensor product is associative and symmetric, up to isomorphism).

Note that if B_U and B_V are bases for U and V, respectively, then

$$B_U \otimes B_V := \{u \otimes v | u \in U, v \in V\} \tag{2}$$

is a basis for $U \otimes V$. Hence $\dim(U \otimes V) = \dim(U) \dim(V)$.

Furthermore, if U and V are inner product spaces, then

$$\langle u \otimes v, u' \otimes v' \rangle_{U \otimes V} := \langle u, u' \rangle_U \langle v, v' \rangle_V \tag{3}$$

extends linearly to a well-defined inner product on $U \otimes V$, and the if B_U and B_V are orthonormal bases for U and V, respectively, then $B_U \otimes B_V$ is an orthonormal basis for $U \otimes V$.

Concretely, the tensor product of two complex matrices A and B (of any dimension, including vectors as columns and rows) is the matrix $A \otimes B$ that can be computed in block-matrix form as follows:

$$\text{If } A = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{m2} & \cdots & A_{mn} \end{bmatrix} \text{ and } B = \begin{bmatrix} B_{11} & B_{12} & \cdots & B_{1q} \\ B_{21} & B_{22} & \cdots & B_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ B_{p1} & B_{p2} & \cdots & B_{pq} \end{bmatrix}, \text{ then}$$

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

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

$$= \begin{bmatrix} A_{11}B_{11} & \cdots & A_{11}B_{1q} & & A_{1n}B_{11} & \cdots & A_{1n}B_{1q} \\ \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\ A_{11}B_{p1} & \cdots & A_{11}B_{pq} & & A_{1n}B_{p1} & \cdots & A_{1n}B_{pq} \\ & \vdots & & \ddots & & \vdots & \\ A_{m1}B_{11} & \cdots & A_{m1}B_{1q} & & A_{mn}B_{11} & \cdots & A_{mn}B_{1q} \\ \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\ A_{m1}B_{p1} & \cdots & A_{m1}B_{pq} & & A_{mn}B_{p1} & \cdots & A_{mn}B_{pq} \end{bmatrix}. \tag{4}$$

Proposition 3.2.13 (Tensor products of linear transformations)**.** *Let U, V, W and Z be vector spaces. Then $\mathcal{L}(U,V) \otimes \mathcal{L}(W,Z)$ is isomorphic to $\mathcal{L}(U \otimes W, V \otimes Z)$. In particular, let $A : U \to V, B : W \to Z$ be linear transformations. Then, $A \otimes B : U \otimes W \to V \otimes Z$ can be defined by extending $(A \otimes B)(u \otimes w) = Au \otimes Bw$ by linearity. Furthermore,*

1.
$$(A \otimes B)(C \otimes D) = AC \otimes BD, \tag{5}$$
provided these compositions are defined.

2.
$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger \,. \tag{6}$$

Definition 3.2.14 (Trace)**.** Let $A : V \to V$ be a linear operator on an n-dimensional vector space V. Then the *trace* of A is $\mathrm{Tr}(A) = \sum_{k=1}^{n} A_{kk}$, where $(A_{kj})_{kj}$ are the entries of any matrix representation of A (with respect to one basis used for both domain and codomain).

While the trace is defined in terms of a basis, the result does not depend on the basis chosen. Furthermore, the trace is a linear functional on the space of operators on V (a linear transformation $\mathcal{L}(V) \to \mathbb{C}$).

Proposition 3.2.15 (Trace properties)**.** *Let A, B, C be linear operators on finite-dimensional Hilbert spaces. Then*

1. *For $A : U \to U$ and $(\lambda_i)_i$, its eigenvalues,*
$$\mathrm{Tr}(A) = \sum_i \lambda_i \,. \tag{7}$$

2. *For $A : U \to V, B : V \to U$,*
$$\mathrm{Tr}(AB) = \mathrm{Tr}(BA) \,. \tag{8}$$

3. *For $A : U \to V, B : V \to W, C : W \to U$,*
$$\mathrm{Tr}(ABC) = \mathrm{Tr}(BCA) = \mathrm{Tr}(CAB) \,. \tag{9}$$

4. *For $A : U \to U, B : V \to V$,*
$$\mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A)\,\mathrm{Tr}(B) = \mathrm{Tr}((\mathrm{Tr} \otimes \mathbb{1}_{\mathcal{L}(U)})(A \otimes B)) = \mathrm{Tr}((\mathbb{1}_{\mathcal{L}(V)} \otimes \mathrm{Tr})(A \otimes B)) \,. \tag{10}$$

5. *For $C : U \otimes V \to U \otimes V$,*

$$\mathrm{Tr}(C) = \mathrm{Tr}((\mathrm{Tr} \otimes \mathbb{1}_{\mathcal{L}(U)})(C)) = \mathrm{Tr}((\mathbb{1}_{\mathcal{L}(V)} \otimes \mathrm{Tr})(C)) \,. \tag{11}$$

6. *For $A : U \to V$,*

$$\|A\|_1 := \mathrm{Tr}(\sqrt{A^\dagger A}) = \sum_k |A_{kk}| \tag{12}$$

defines a norm.

7. *For $A, B : U \to V$,*

$$\mathrm{Tr}(A^\dagger B) = \sum_{kj} \overline{A}_{kj} B_{kj} \tag{13}$$

for any matrix representations $(A_{kj})_{kj}$ of A and $(B_{kj})_{kj}$ of B with respect to a common basis. This defines an inner product on $\mathcal{L}(U, V)$.

The norm $\|\cdot\|_1$ above is called the *trace norm*, and the corresponding metric when multiplied by $\frac{1}{2}$ is called the *trace distance* and is equal to the maximum probability of distinguishing the two quantum states (see Proposition 3.8.5), as represented by density operators (as defined in the next section).

Finally, normal operators on Hilbert spaces are diagonalizable by unitary operators. The result is one of the most important in linear algebra (and functional analysis).

Theorem 3.2.16 (Spectral theorem)**.** *Let A be a normal operator on an n-dimensional Hilbert space $\mathcal{H}$, where $n < \infty$. Then, the following hold:*

1. *There exists an othonormal basis for $\mathcal{H}$ of eigenvectors of $\mathcal{H}$*

2. $$A = \sum_{i=1}^{n} \lambda_i |\phi_i\rangle \langle\phi_i| \,, \tag{14}$$

where $|\phi_i\rangle$ is the i-th eigenvector from 1, with corresponding eigenvalue λ_i, and $|\phi_i\rangle \langle\phi_i|$ is the orthogonal projection onto the subspace spanned by $|\phi_i\rangle$.

3.3 Quantum States

We are now ready to describe quantum states, as both vectors (pure states) in a Hilbert space or density operators acting on them.

Definition 3.3.1 (Pure state)**.** Let $\mathcal{H}$ be a Hilbert space. Then a *pure state* is a vector $|\psi\rangle \in \mathcal{H}$ of norm 1 ($\langle\psi|\psi\rangle = 1$).
The coefficients of a pure state $|\psi\rangle \in \mathcal{H}$ with respect to an orthonormal basis are called *amplitudes* or *probability amplitudes*.
Note that if $|\psi\rangle = \sum_k \alpha_k |\phi_k\rangle$, where $(|\phi_k\rangle)_k$ is an orthonormal basis, then $\alpha_k = \langle\phi_k|\psi\rangle$.
The pure state $|\psi\rangle$ is said to be in a *superposition* of the states for which $\alpha_k \neq 0$.
If $|\psi\rangle \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ is equal to $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$ for some pure states $|\psi_i\rangle \in \mathcal{H}_i$, $1 \leq i \leq n$, then $|\psi\rangle$ is called *separable*. Otherwise, it is called *entangled*.

In fact, we only actually care about nonzero elements of $\mathcal{H}$ up to scalar multiples, so that a global phase does not matter, i.e. $\alpha|\psi\rangle$ and $|\psi\rangle$ are treated the same ($\alpha \neq 0$). This will become clear when density operators (Definition 3.3.2, next) and measurements (Definition 3.4.2) are defined.

Note that separability and entanglement are defined with respect to a particular decomposition of a Hilbert space into tensor products.

Definition 3.3.2 (Density operator)**.** A *density operator* (or *density matrix*) is a positive semidefinite operator A, such that $\mathrm{Tr}(A) = 1$. The set of all density operators on $\mathcal{H}$ is denoted by $\mathfrak{D}(\mathcal{H})$.

By convention, ρ, σ, with subscripts or superscripts are used to denote density operators.

Note that if $|\psi\rangle$ is a pure state, then $|\psi\rangle\langle\psi|$ is a density operator (and an orthogonal projection, more specifically). Furthermore, if $|\alpha| = 1$, then

$$(\alpha|\psi\rangle)(\alpha|\psi\rangle)^\dagger = \alpha|\psi\rangle\overline{\alpha}\langle\psi| = \alpha\overline{\alpha}|\psi\rangle\langle\psi| = 1|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi| \ . \tag{15}$$

Hence pure states that differ only by a global phase give rise to the same density operator.

Furthermore, all density operators decompose as convex combinations of density operators arising from orthogonal pure states:

Proposition 3.3.3 (Density operator spectral decomposition)**.** *Let $\rho \in \mathfrak{D}(\mathcal{H})$, where $dim(\mathcal{H}) = n < \infty$. Then*

$$\rho = \sum_{i=1}^{n} p_i |\psi_i\rangle\langle\psi_i| \,, \tag{16}$$

where the $|\psi_i\rangle$ are orthogonal pure states, $p_i \geq 0$ for each i and $\sum_{i=1}^{n} p_i = 1$.

Definition 3.3.4 (Pure and mixed states)**.** $\rho \in \mathfrak{D}(\mathcal{H})$ is called *pure* if $\rho = |\psi\rangle\langle\psi|$ for some pure state $|\psi\rangle$ on $\mathcal{H}$, and *mixed*, otherwise.

Definition 3.3.5 (Ensemble and mixture)**.** An *ensemble* is a finite set of indexed pairs (ρ_x, p_x) where $\rho_x \in \mathfrak{D}(\mathcal{H})$ and $p_x \geq 0$ for all x and $\sum_x p_x = 1$. Its *mixture* is the state $\sum_x p_x \rho_x$.
Alternatively, an *ensemble* is a $\mathfrak{D}(\mathcal{H})$-valued random variable ρ (with finite range), and its mixture is $\mathbb{E}[\rho]$.

The two definitions of ensembles and mixtures are equivalent, through $\rho = \rho_X$, where $\Pr[X = x] = p_x$, or $\Pr[\rho = \rho_x] = p_x$ assuming $x \neq y \implies \rho_x \neq \rho_y$.

The mixture, a fixed state, corresponds to the preparation of the state ρ_x with probability p_x when it is unknown which of the ρ_x is prepared.

The definition may be extended to ensembles with infinite range and arbitrary probability measures, but we focus on the finite discrete case here.

The state corresponding to a density operator $\rho \in \mathfrak{D}(\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n)$ is called *separable* if $\rho = \sum_k p_k \rho_1^k \otimes \ldots \rho_n^k$, and *entangled*, otherwise.

Finally, the qubit, the fundamental unit of quantum information, is defined:

Definition 3.3.6 (Qubit)**.** A *qubit* is any pure state in $\mathbb{C}^2$ or any density matrix in $\mathfrak{D}(\mathbb{C}^2)$. An *n-qubit state* is any pure state in $\mathbb{C}^{2^n} = (\mathbb{C}^2)^{\otimes n} = \bigotimes_{i=1}^{n} \mathbb{C}^2$ or any density matrix in $\mathfrak{D}(\mathbb{C}^{2^n})$.

Notation 3.3.7 (Standard states)**.** $|0\rangle = \binom{1}{0}$ *and* $|1\rangle = \binom{0}{1}$ *and tensor products of these states are the* computational basis states *(also the standard basis states for* $\mathbb{C}^{2^n}$*).* $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\binom{1}{1}$ *and* $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\binom{1}{-1}$ *and tensor products of these states are* Hadamard basis states*. The n-qubit* maximally mixed *(or* completely mixed*) state is the density matrix* $\frac{1}{2^n}\mathbb{1}_{\mathbb{C}^{2^n}} = \bigotimes_{i=1}^{n} \frac{1}{2}\mathbb{1}_{\mathbb{C}^2}$.

Note that $\frac{1}{d}\mathbb{1}_{\mathcal{H}} = \sum_{i=1}^{d} \frac{1}{d} |\psi_i\rangle \langle\psi_i|$, where $(|\psi_i\rangle)_{i=1}^{d}$ is *any* orthonormal basis for $\mathcal{H} = \mathbb{C}^d$, i.e. the maximally mixed state is the mixture of the states in any orthonormal basis with equal probability each.

3.4 Admissible Maps

This section describes admissible maps, but before they are defined in their generality, several elementary examples are introduced, from which are admissible maps can be constructed by tensor products and compositions.

An important restriction on the physically realizable operations on quantum systems is the no-cloning theorem, ruling out the admissibility of an operation:

Theorem 3.4.1 (No-cloning theorem)**.** *[WZ82, Die82, KLM07] There is no unitary $U : \mathcal{H} \otimes \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$ and pure state $|\phi\rangle \in \mathcal{H}$ such that for all pure states $|\psi\rangle \in \mathcal{H}$*

$$U(|\psi\rangle |\phi\rangle) = e^{i\alpha(\psi)} |\psi\rangle |\psi\rangle \tag{17}$$

for some $\alpha(\psi) \in \mathbb{R}$.

At the end of interactions with quantum data, when the information stored therin is to be accessed and classical information, readable to humans, extracted, a measurement must be performed:

Definition 3.4.2 (Single qubit computational basis measurement)**.**
Let $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ be a single-qubit pure state. Then, after performing a measurement on $|\psi\rangle$ in the computational basis, the resulting state is $|0\rangle$ with probability $\langle 0 |\psi\rangle \langle\psi| 0\rangle = |\langle 0|\psi\rangle|^2 = |\alpha|^2$, and $|1\rangle$, with probability $\langle 1 |\psi\rangle \langle\psi| 1\rangle = |\langle 1|\psi\rangle|^2 = |\beta|^2$.

Let ρ be a single-qubit density matrix. Then, after performing a measurement on ρ in the computational basis, the resulting state is $|0\rangle \langle 0|$ with probability $\mathrm{Tr}(|0\rangle \langle 0| \rho) = \langle 0| \rho |0\rangle$, and $|1\rangle \langle 1|$ with probability $\mathrm{Tr}(|1\rangle \langle 1| \rho) = \langle 1| \rho |1\rangle$

The definitions for pure states and density matrices agree when $\rho = |\psi\rangle \langle\psi|$.

Note that if $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, then

$$|\psi\rangle \langle\psi| = \overline{\alpha}\alpha |0\rangle \langle 0| + \overline{\alpha}\beta |0\rangle \langle 1| + \overline{\beta}\alpha |1\rangle \langle 0| + \alpha\overline{\beta}\beta |1\rangle \langle 1| \ . \tag{18}$$

On the other hand, the mixture of the states after measuring is $\overline{\alpha}\alpha \left|0\right\rangle \left\langle 0\right| + \overline{\beta}\beta \left|1\right\rangle \left\langle 1\right|$, with no mixed terms. Furthermore, the state after measurement is not this mixture, it is either $\left|0\right\rangle \left\langle 0\right|$ or $\left|1\right\rangle \left\langle 1\right|$: measurement is *not* a deterministic function $\mathfrak{D}(\mathcal{H}) \to \mathfrak{D}(\mathcal{H})$.

Definition 3.4.3 (Partial measurement in the computational basis)**.** Let $\left|\psi\right\rangle$ be an n-qubit pure state. Suppose the i-th qubit is measured in the computational basis, $1 \leq i \leq n$. Letting $b = 0$ or 1, and $P = P_1 \otimes P_2 \otimes \dots P_n$, where $P_k = \left|b\right\rangle \left\langle b\right|$ if $k = i$, and $P_k = \mathbb{1}_{\mathbb{C}^2}$, otherwise, then after performing the measurement, the resulting state is $\frac{1}{\|P\left|\psi\right\rangle\|} P \left|\psi\right\rangle$, with probability $\|P \left|\psi\right\rangle\|^2$.

If the state was instead given by the n-qubit density matrix ρ, the resulting state after measurement is $\frac{1}{\mathrm{Tr}(P\rho)} P\rho P$, with probability $\mathrm{Tr}(P\rho)$.

For single qubits, this reduces to the previous definition.

Again, the pure state and density matrix definitions agree, noting that each P is an orthogonal projection.

A partial measurement on n-qubits can be represented as a function from the pure states in $\mathbb{C}^{2^n}$ to the random variable pure states in $\mathbb{C}^{2^n}$, or from $\mathfrak{D}(\mathbb{C}^{2^n})$-valued random variables, and as such, can be composed with other functions, including other partial measurements.

Partial measurements in the computational basis commute, i.e. the order in which such successive measurements are applied does not matter.

Note that $\sum_P P = \mathbb{1}$.

Notation 3.4.4 (Standard unitaries)**.** *The following are standard unitary operators:*

1. *Hadamard* $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
   $H \left|0\right\rangle = \frac{1}{\sqrt{2}} \left|0\right\rangle + \frac{1}{\sqrt{2}} \left|1\right\rangle = \left|+\right\rangle$
   $H \left|1\right\rangle = \frac{1}{\sqrt{2}} \left|0\right\rangle - \frac{1}{\sqrt{2}} \left|1\right\rangle = \left|-\right\rangle$
   $H \left|b\right\rangle = \frac{1}{\sqrt{2}} \left|0\right\rangle + (-1)^b \frac{1}{\sqrt{2}} \left|1\right\rangle$

2. *Pauli-X (or NOT gate)* $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
   $X \left|0\right\rangle = \left|1\right\rangle$

$X|1\rangle = |0\rangle$
$X|b\rangle = |b \oplus 1\rangle$

3. *Paui-Y* $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
$Y|0\rangle = i|1\rangle$
$Y|1\rangle = -i|0\rangle$
$Y|b\rangle = (-1)^b i|b \oplus 1\rangle$

4. *Paui-Z* $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
$Z|0\rangle = |0\rangle$
$Z|1\rangle = -|1\rangle$
$Z|b\rangle = (-1)^b|b\rangle$

5. *Phase shift* ($\phi \in \mathbb{R}$) $R_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$
$Z|0\rangle = |0\rangle$
$Z|1\rangle = e^{i\phi}|1\rangle$
$Z|b\rangle = e^{ib\phi}|b\rangle$

6. *Controlled-NOT* $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
$CNOT|a\rangle|b\rangle = |a\rangle X^a|b\rangle = |a\rangle|a \oplus b\rangle$

7. *Controlled-U* $C(U) = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & 1 & 0 & \cdots & 0 \\ \vdots & & 0 & U_{11} & \cdots & U_{12^n} \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & U_{2^n 1} & \cdots & U_{2^n 2^n} \end{pmatrix}$
$C(U)|a\rangle|\psi\rangle = |a\rangle U^a|\psi\rangle$

(If U is $2^n \times 2^n$, then $C(U)$ is $2^{n+1} \times 2^{n+1}$)

8. *Toffoli* $T = C(CNOT) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$
$T |a\rangle |b\rangle |c\rangle = |a\rangle |b\rangle |ab \oplus c\rangle$

9. *Swap* $SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
$SWAP |\psi\rangle |\varphi\rangle = |\varphi\rangle |\psi\rangle$

Note that all of the above except for R_ϕ and $C(U)$ are self-adjoint, and so self-inverse.

Definition 3.4.5 (Unitary evolution for density operators)**.** Let $U : \mathcal{H} \to \mathcal{H}$ be unitary and $\rho \in \mathfrak{D}(\mathcal{H})$. Then the application of U to ρ results in the state $U\rho U^\dagger$.

Note that $U\rho U^\dagger \in \mathfrak{D}(\mathcal{H})$.

This corresponds to application of unitaries in the pure state formalism: if $\rho = |\psi\rangle \langle\psi|$, and U is applied to $|\psi\rangle$, then the corresponding density operator is $U |\psi\rangle (U |\psi\rangle)^\dagger = U |\psi\rangle \langle\psi| U^\dagger$. Furthermore, if $\rho = \sum_x \rho_x$, then

$$U\rho U^\dagger = U \sum_x p_x \rho_x U^\dagger = \sum_x p_x U \rho_x U^\dagger \,. \tag{19}$$

Hence, if ρ is the mixture of $(\rho_x, p_x)_x$, then $U\rho U^\dagger$ is the mixture of $(U\rho_x U^\dagger, p_x)_x$.

Definition 3.4.6 (Positive and completely positive maps)**.** A linear transformation $\Phi : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{K})$ is a *positive map* if $\Phi(A) \geq 0$ whenever $A \geq 0$, i.e. the image

of a positive semidefinite operator is positive semidefinite. Φ is *completely positive* if $\Phi \otimes \mathbb{1}_{\mathcal{L}(\mathbb{C}^k)}$ is positive for all $k \geq 1$.

Note that $\Phi \otimes \mathbb{1}_{\mathcal{L}(\mathbb{C})}$ is just Φ under a canonical isomorphism, since $\mathcal{L}(\mathbb{C}) \simeq \mathbb{C}$ and $\mathbb{1}_{\mathbb{C}} = 1$, multiplication by 1.

Definition 3.4.7 (Induced operator 1-norm)**.** For a linear transformation $\Phi : X \to Y$, where X and Y are normed vector spaces, with norms $\|\cdot\|_X$ and $\|\cdot\|_Y$, respectively, its *operator norm* is defined by

$$\|\Phi\| := \sup_{x \in X, x \neq 0} \frac{\|\Phi(x)\|_Y}{\|x\|_X} = \sup_{0 < \|x\|_X \leq 1} \|\Phi(x)\|_Y = \sup_{\|x\|_X = 1} \|\Phi(x)\|_Y \tag{20}$$

Positive maps are bounded in this norm (i.e. the operator norm is finite).

Furthermore, completely positive maps are *completely bounded*:

Definition 3.4.8 (Completely bounded)**.** A linear transformation $\Phi : X \to Y$ between normed vector spaces $(X, \|\cdot\|_X)$ and $(Y, \|\cdot\|_Y)$ is *completely bounded* if

$$\sup_k \|\Phi \otimes \mathbb{1}_{\mathcal{L}(\mathbb{C}^k)}\| < \infty \,. \tag{21}$$

Note that the norms on $X \otimes \mathcal{L}(\mathbb{C}^k)$ and $Y \otimes \mathcal{L}(\mathbb{C}^k)$ must first be chosen.

The completely bounded maps $X \to Y$ form a normed vector space, with the *diamond norm*, which is defined in the obvious way:

Definition 3.4.9 (Diamond norm)**.** The *diamond norm* (or *norm of complete boundedness* or *cb-norm*) of a completely bounded map $\Phi : X \to Y$ is defined by

$$\|\Phi\|_\diamond := \sup_k \|\Phi \otimes \mathbb{1}_{\mathcal{L}(\mathbb{C}^k)}\| \,. \tag{22}$$

The diamond norm is used because it gives the maximum probability of distinguishing between two quantum channels (see Proposition 3.8.5 and Definition 3.8.6 in Section 3.8), which we now define:

Definition 3.4.10 (Quantum channel)**.** A *quantum channel* is a completely positive trace-preserving (CPTP) linear transformation $\mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{K})$, i.e. it is completely positive and $\mathrm{Tr}(\Phi(A)) = \mathrm{Tr}(A)$ for all $A \in \mathcal{L}(\mathcal{H})$.

If one restricts the domain of a quantum channel $\mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{K})$ to $\mathfrak{D}(\mathcal{H})$, its range will be in $\mathfrak{D}(\mathcal{K})$. Hence, quantum channels send quantum states to quantum states.

Notation 3.4.11 (Subscript notation)**.** *Given a Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ where $\mathcal{H}_A$ and $\mathcal{H}_B$ are also Hilbert spaces (subsystems or registers of $\mathcal{H}$), the subscripts A, B will often be used on states and quantum channels (and admissible maps, defined shortly) to specify to which subsystem a channel applies. For example, if $|\psi\rangle \in \mathcal{H}$, then $|\psi\rangle_{AB}$ or $|\psi\rangle\langle\psi|_{AB}$ may be written, and if $\rho \in \mathfrak{D}(\mathcal{H})$, then ρ_{AB} may be written. Then, for quantum channels $\mathcal{F}$ and $\mathcal{G}$ with domains $\mathfrak{D}(\mathcal{H}_A)$ and $\mathfrak{D}(H_B)$, $(\mathcal{F}_A \otimes \mathcal{G}_B)\rho_{AB}$ may be written. Furthermore,* $\mathrm{Tr}_A := \mathrm{Tr} \otimes \mathbb{1}_{\mathcal{H}_B}, \rho_B := \mathrm{Tr}_A(\rho_{AB})$ *(called a* reduced density operator*) and $\mathbb{1}_B := \mathbb{1}_{\mathcal{H}_B}$. This notation will be used when the roles of A and B are switched or when more subsystems and subscripts are used.*

Examples of quantum channels include:

- $U(\cdot)U^\dagger$, where U is unitary, as above,
- Tr ,
- $\mathbb{C} \to \mathcal{L}(\mathcal{K})$ defined by $\alpha \mapsto \alpha\rho$, where $\rho \in \mathfrak{D}(\mathcal{K})$ is fixed, and
- tensor products and (well-defined) compositions of the above.

In fact, all quantum channels can be obtained this way, and in a particular factorized form:

Theorem 3.4.12 (Stinespring's dilation theorem)**.** *[Sti55]* $\Phi : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{K})$ *is a quantum channel if and only if*

$$\Phi(A) = \mathrm{Tr}_F(V(A \otimes |\phi\rangle\langle\phi|)V^\dagger), \tag{23}$$

for some unitary $V : \mathcal{H} \otimes \mathcal{H}_E \to \mathcal{K} \otimes \mathcal{H}_F$, for some pure state $|\phi\rangle \in \mathcal{H}_E$, for all $A \in \mathcal{L}(\mathcal{H})$.

Furthermore, for every pair of representations, one can be embedded isometrically into the other, so that minimal representations (those for which $\dim \mathcal{H}_E$ and $\dim \mathcal{H}_F$ are minimized) are unique up unitaries.

Like the no-cloning theorem for unitaries (3.4.1), there is also a no-cloning theorem for quantum channels:

Theorem 3.4.13 (No-cloning theorem (for quantum channels))**.** *[WZ82, Die82, KLM07] There is no quantum channel* $\Phi : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H} \otimes \mathcal{H})$*, where* $\dim \mathcal{H} \geq 2$*, such that for all* $\rho \in \mathfrak{D}(\mathcal{H})$*,*

$$\Phi(\rho) = \rho \otimes \rho \,. \tag{24}$$

Note that the above actually holds even for classical channels acting on density matrices representing classical (probabilistic) states, by considering, for example, the states $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$, and $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|0\rangle\langle 0|$ and using the linearity of the channel.

Next, we consider more general measurements.

Definition 3.4.14 (POVM and PVM measurements)**.** A (finite) *positive operator-valued measure* (*POVM*) is a (finite) set $(A_k)_k$ of positive semidefinite operators $A_k : \mathcal{H} \to \mathcal{H}, A_k$ such that $\sum_k A_k = \mathbb{1}_{\mathcal{H}}$ (so $A_k \leq \mathbb{1}_{\mathcal{H}}$ for all k).
A (finite) *projection-valued measure* (*PVM*) is a POVM such that each operator A_k, usually denoted instead by P_k, is an orthogonal projection.
A *von Neumann measurement* is a PVM such that $P_k = |\psi_k\rangle\langle\psi_k|$, where the $|\psi_k\rangle$ form an orthonormal basis for $\mathcal{H}$.
Given a pure state $|\psi\rangle \in \mathcal{H}$, measuring $|\psi\rangle$ with respect to the POVM $(A_k)_k$ results in the state $\frac{1}{\sqrt{\langle\psi|A_k|\psi\rangle}} B_k |\psi\rangle$ with probability $\langle\psi| A_k |\psi\rangle$, where B_k satisfies $B_k^\dagger B_k = A_k$.
Given $\rho \in \mathfrak{D}(\mathcal{H})$, measuring ρ with respect to the POVM $(A_k)_k$ results in the state $\frac{1}{\mathrm{Tr}(A_k\rho)} B_k \rho B_k^\dagger$ with probability $\mathrm{Tr}(A_k\rho)$.

In the case of PVMs, $B_k = P_k$ suffices, and in the case of von Neumann measurements, the state becomes $|\psi_k\rangle\langle\psi_k|$. PVM measurements are also called *projective measurements*.

These further generalize measurements in the computational basis. Note also that the tensor product of a POVM (PVM) with the identity on any other space is again

a POVM (PVM), and in the case of von Neumann measurements, this corresponds to partial measurements.

For general POVMs, $B_k := \sqrt{A_k}$'s can be computed by diagonalizing $A_k = SDS^\dagger$ where S is unitary (by the spectral theorem) and D is diagonal, and then setting $B_k = SD'S^\dagger$, where D' is obtained from D by taking the square root of each (diagonal) entry. These entries are nonnegative, since A_k is positive semidefinite. B_k as defined is positive semidefinite and

$$B_k^\dagger B_k = B_k B_k = (SD'S^\dagger)(SD'S^\dagger) = SD'D'S^\dagger = SDS^\dagger = A_k\,. \tag{25}$$

By the spectral theorem, to any self-adjoint operator is associated a von Neumann measurement, but, unless all eigenvalues have multiplicity 1, this measurement is not unique.

Again, a POVM can be represented as a function from $\mathfrak{D}(\mathcal{H})$ to $\mathfrak{D}(H)$-valued random variables, and as such, can be composed with other functions, including quantum channels and other POVMs.

By Naimark's dilation theorem [Nai40], every POVM can be represented as a PVM on a larger Hilbert space in the same way every quantum channel can be represented as a unitary on a larger Hilbert space (by Stinespring's dilation theorem). In general, all POVMs can be implemented through unitaries, ancillae, the trace and partial measurements in the computational basis (see [NC00, 2.2.8]).

Definition 3.4.15 (Admissible map)**.** An *admissible map* is the (well-defined) composition of a finite sequence of quantum channels and POVMs.

We consider only admissible maps whose domain and codomain are qubits, i.e. $\mathfrak{D}(\mathbb{C}^{2^n}) \to \mathfrak{D}(\mathbb{C}^{2^m})$.

Due to measurements, an admissible map's output on a fixed input is, in general, a random variable.

When admissible maps are composed only of by unitaries, $\alpha \mapsto \alpha\,|\psi\rangle$ and POVMs, it suffices to deal entirely with pure states. This is the pure state formalism. In this thesis, the more general density matrix formalism is used.

3.5 Quantum Circuits

Quantum circuits are admissible maps constructed from fixed set of admissible maps, called a *gate set*.

Definition 3.5.1 (Gate set)**.** A *gate set* is a set of admissible maps.

Definition 3.5.2 (Standard gate set)**.** The *standard gate set* consists of the standard unitaries (except $SWAP$ and general $C(U)$), $\mathrm{Tr} : \mathbb{C}^2 \to \mathbb{C}$, ancilla qubits $\mathbb{C} \to \mathbb{C}^2$ defined by $\alpha \mapsto \alpha |0\rangle \langle 0|$ and single-qubit partial measurements in the computational basis.

Measurement gate will be used to refer only to single-qubit partial measurements in the computational basis.

Definition 3.5.3 (Quantum circuit)**.** A *quantum circuit* is a directed acyclic graph in which

- each edge is called a *wire*, representing a single qubit;
- each vertex which has no wires into it is labelled as one or multiple input or ancilla qubits;
- each vertex which has no wires out of it is labelled as one or multiple output qubits, or by one or multiple trace gates;
- every other vertex is labelled by a gate from a gate set representing an admissible map $\mathcal{L}(\mathbb{C}^{2^n}) \to \mathcal{L}(\mathbb{C}^{2^m})$, with n wires in and m wires out (if $n = 0$, there are no wires in, and if $m = 0$, there are no wires out), and measurement gates, specifically, have exactly the wires being measured in and out; and
- at the vertex, the wires into it are ordered (1 to n), and the wires out of it are ordered (1 to m).

Single-qubit measurement gates correspond to partial measurements, and for other gates with wires into them, the admissible map applied is actually the tensor product

of the admissible map the gate represents with the identity on the subsystem corresponding to the wires to which the gate does not apply and that are parallel to (that have not ended in trace gates before) the gate. Wires crossing correspond to the application of the SWAP gate (so the explicit use of the SWAP gate is unnecessary). In circuit diagrams, the wires into a gate are ordered from top to bottom. Figure 1 is an example of a quantum circuit; it implements the quantum teleportation of a single qubit.

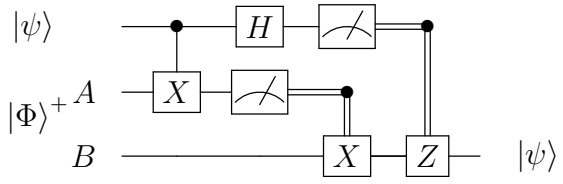

Figure 1: Circuit for quantum teleportation.

In Figure 1,

- single lines represent qubits while double lines represent classical bits;
- $|\Phi\rangle^+ = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, a Bell state, which is maximally entangled;
- the lines extending down from dots represent controlled operations; and
- the meter gates represent measurements in the computational basis.

For more complex circuits than that pictured in Figure 1, to condense pictorial representations, multiple wires may be drawn as a single wire, labelling it instead by the subsystem the wires represent, e.g. A and B, where the state is over $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A = \mathbb{C}^{2^n}$ and $\mathcal{H}_B = \mathbb{C}^{2^m}$. Multiple ancilla qubit gates may be combined, and similarly, multiple trace gates may be combined. Whole circuits, used as subcircuits, may be treated as gates.

Definition 3.5.4 (Universal gate set)**.** A gate set is called *universal* if every unitary operator can be approximated arbitrarily (in any norm) by quantum circuits using gates from the gate set.

The standard gate set is one such universal gate set. In fact, just the Toffoli and the Hadamard (or any other gate which does not preserve the computational basis, up to global phases) together form a universal gate set, noting that complex numbers can be simulated with more qubits.

Definition 3.5.5 (Purification of a quantum circuit)**.** Let A be a quantum circuit composed only of ancilla qubit, trace and unitary gates (no measurement or more general admissible maps). Then the purification of A is the circuit obtained by replacing in A the ancilla gates with input and the trace gates with output.

The purification of a circuit implements a unitary operator.

3.6 Efficient Classical and Quantum Computations

This section is based on the section of the same name from the joint paper [ABF+16], athough it largely rewritten for consistency with the rest of the preliminaries.

Turing machines are left formally undefined. It suffices to think of them as algorithms or computer programs.

Note that classical Boolean circuits are analogous to quantum circuits; they are instead (usually) composed of the standard AND, OR and NOT gates.

We will refer to several different notions of efficient algorithms. The most basic of these is a deterministic polynomial-time algorithm (or PT).

Definition 3.6.1 (Polynomial-time algorithm (PT))**.** A *polynomial-time algorithm* (or *PT*) is a deterministic polynomial-time Turing machine $\mathcal{A}$ that on input n in unary, prints a description of a classical Boolean circuit $\mathcal{A}_n$ that itself receives n bits. For a binary string x, $\mathcal{A}(x) := \mathcal{A}_{|x|}(x)$ (overloading the notation).
A function family $f : \{0,1\}^n \to \{0,1\}^m$ is *PT-computable* if there exists a PT $\mathcal{A}$ such that $\mathcal{A}(x) = f(x)$ for all x; it is implicit that m is a function of n which is bounded by some polynomial, e.g., the same one that bounds the running time of $\mathcal{A}$.

Definition 3.6.2 (Probabilistic polynomial-time algorithm (PPT))**.** A *probabilistic polynomial-time algorithm* (or *PPT*) is a deterministic polynomial-time Turing machine $\mathcal{A}$ that on input n in unary, prints a description of a classical Boolean circuit $\mathcal{A}_n$ that itself receives n bits of input, as well as an additional $p(n)$ random bits. For a PPT $\mathcal{A}$, n-bit input x and $p(n)$-bit coin string r, $\mathcal{A}(x;r) := \mathcal{A}_n(x;r)$. $\mathcal{A}(x)$ refers to the random variable $\mathcal{A}(x;r)$ where $r \xleftarrow{\$} \{0,1\}^{p(n)}$ and the corresponding probability distribution.

Note that uniformity enforces that the function p is bounded by some polynomial.

Definition 3.6.3 (Quantum polynomial-time algorithm (QPT))**.** A *quantum polynomial-time algorithm* (or *QPT*) is a deterministic polynomial-time Turing machine $\mathcal{A}$ that on input n in unary, prints a description of a quantum circuit $\mathcal{A}_n$, composed of gates from a fixed finite (and usually universal) gate set, that itself receives n qubits. When ρ is an n-qubit state, $\mathcal{A}(\rho)$ denotes the corresponding output state or the random variable over the possible output states. For n-bit strings x, $\mathcal{A}(x) := \mathcal{A}(|x\rangle\langle x|)$. The expression $\mathcal{A}(x) = y$ for classical y is taken to evaluate to true if the output register of the circuit contains the state $|y\rangle\langle y|$ exactly.

A commonly-used alternative is to specify that the elements of the gate set are unitary. In terms of computational power, the models are the same [AKN98], however using admissible operations (versus unitary ones only) allows us to formalize a wider range of oracle-enabled QPT machines (see Subsection 3.6.1). In general, a QPT $\mathcal{A}$ defines a family of admissible maps from input registers to output registers.Unless explicitly stated, any statements about the probability of an event involving a QPT are taken over the measurements of the QPT, in addition to any indicated random variables. For instance, the expression $\Pr_{x \in_R \{0,1\}^n}[\mathcal{A}(x) = y]$ means the probability that, given a uniformly random input string x, the output register of the nth circuit of the QPT $\mathcal{A}$ executed on $|x\rangle\langle x|$, after all gates and measurements have been applied, is in the state $|y\rangle\langle y|$.

At times, we will define QPTs with many input and output quantum registers. In these cases, some straightforward bookkeeping (e.g., via an additional classical

register) may be required; for the sake of clarity, we will simply assume that this has been handled.

Throughout this work, we are concerned only with polynomial-time *uniform* computation. That is to say, the circuit families that describe any PT, PPT, or QPT will always be both of polynomial length *and* generatable by some fixed (classical) deterministic polynomial-time Turing machine. In particular, we consider uniform adversaries only—although all of our results carry over appropriately to the non-uniform setting as well.

3.6.1 Oracles

Definition 3.6.4 (Oracles)**.** For a function family f on binary strings (whose output lengths depend only the input lengths, and one function f_n for each n), $\mathcal{A}^f$ denotes an oracle PT, PPT or QPT whose gates come from a finite fixed set as well as gates evaluating f_n for the circuit $\mathcal{A}_n$. In the case of QPTs, f may only be applied to classical strings.
Also for QPTs, any family of admissible maps $\mathcal{C}$ is further allowed, denoted by, e.g. $\mathcal{A}^{\mathcal{C}}$.
The algorithms are said to have *oracle access* to f or $\mathcal{C}$.
Furthermore, the oracles may be indexed by strings rather than simply n to be used in $\mathcal{A}_n$. In this case, the particular gate $\mathcal{A}_n$ uses from the family will depend on an external event, e.g. the generation of a key k, and the index will also be used to denote the algorithm, so $\mathcal{A}^{f_k}$ or $\mathcal{A}^{\mathcal{C}_k}$ will be written in this example.

The second definition for QPTs generalizes the first with a classical oracle, if it is assumed that the queries are measured before the oracle is applied (this is sometimes referred to as "standard-security" [Zha12]). We emphasize that we do not require that the oracle is made reversible, nor do we allow the QPT to input superpositions. While it might seem that disallowing superposition inputs is an artificial and unrealistic restriction, in our case it actually strengthens results. For instance, we will show that secure quantum encryption can be achieved using pseudorandom functions which are secure only against quantum adversaries possessing just classical oracle access. One can of course also ask for *more powerful* functions (which are secure

against superposition access, or "quantum-secure" [Zha12]) but this turns out to be unnecessary in our case.

In any case, each use of an oracle gate counts towards the circuit length, and hence also towards the total computation time of the algorithm. In particular, no PT, PPT or QPT algorithm may make more than a polynomial number of oracle calls.

3.7 Negligible Functions

It is the norm in cryptography to allow small probabilities of "failure" that converge quickly to 0 in a security parameter 1^n, so that this probability can easily be made arbitrarily small. This is captured by *negligible functions*. For references, see [Gol06, KL07].

Definition 3.7.1 (Negligible Function)**.** A function $f : \mathbb{N} \to \mathbb{R}$ is called *negligible* if for every positive polynomial p, there exists an $N \in \mathbb{N}$ such that for all $n > N$ (or for sufficiently large n),

$$f(n) < \frac{1}{p(n)}\,. \tag{26}$$

Note that we allow f to take on negative values in this definition, although it will only be used for non-negative functions in this thesis.

Some examples of negligible functions are: $0, \frac{1}{2^n}, -1, -2^n, \frac{1}{(1.0000001)^{(\log(n))^2}}$, and $\begin{cases} 2^n, & \text{if } n<10^{100} \\ 2^{-n}, & \text{otherwise} \end{cases}$.

We will often write $\mathrm{negl}(\cdot)$ to denote a negligible function.

The following results are immediate from the definition:

Proposition 3.7.2 (Equivalent Definitions of Negligible Function)**.**

1. *f is negligible if and only if $f(n)$ is $O(n^{-c})$ for all $c \geq 0$.*
2. *If f is positive for all sufficiently large n, then it is negligible if and only if $\frac{1}{f(n)}$ grows faster than any polynomial (i.e. $\frac{1}{f(n)}$ is $\Omega(n^c)$ for all $c > 0$).*

3. *f is not negligible if and only if there exists a polynomial p such that $f(n) \geq \frac{1}{p(n)}$ for infinitely many n.*

Proposition 3.7.3 (Properties of Negligible Functions)**.**

1. *f negligible and non-negative (for all sufficiently large n) $\Rightarrow \lim_{n\to\infty} f(n) = 0$.*
2. *f negligible $\Rightarrow \limsup_n f(n) \leq 0$.*
3. *$f(n) \leq g(n)$ for all (sufficiently large) n, and g negligible $\Rightarrow$ f negligible. In particular, $f = \min\{g, h\}$ is negligible, for any $h : \mathbb{N} \to \mathbb{R}$.*
4. *f and g negligible $\Rightarrow \max\{f, g\}$ and $f + g$ negligible.*
5. *f negligible and g non-negative (for all sufficiently large n) and polynomially bounded (e.g. constant) $\Rightarrow g \times f$ negligible.*

Furthermore, since the product of a polynomially bounded function and a negligible function is again negligible, any event that occurs with negligible probability, even if repeated in polynomially many independent trials, will remain negligible:

Proposition 3.7.4. *Let t be a positive and polynomially bounded integer-valued function, $X_i^n, 1 \leq i \leq t(n)$ be independent events such that $\Pr[X_i^n] = \mathrm{negl}(n)$. Then $\Pr[\bigcup_{i=1}^{t(n)} X_i^n]$ is negligible.*

Proof.

$$\Pr[\bigcup_{i=1}^{t(n)} X_i^n] \leq \sum_{i=1}^{t(n)} \Pr[X_i^n] = t(n)\,\mathrm{negl}(n)\,, \tag{27}$$

which is, again, negligible. □

3.8 Distinguishing Between States and Channels

In this section, we consider quantum circuits whose measurements are all in the computational basis, and the probability that they can distinguish between distinct quantum states.

First, a useful result that allows quantum circuits with measurements to be represented as they were initially developed, as unitaries with all measurement occuring at the end, is the *principle of deferred measurement*:

Proposition 3.8.1 (Principle of deferred measurement [NC00])**.** *Every quantum circuit with measurement gates is equivalent to a quantum circuit in which all of the measurement gates appear at the end of the circuit (possibly followed by trace gates). Furthermore, every quantum algorithm is equivalent to a quantum algorithm in which the measurements are at the end of each circuit.*

Using this principle, quantum circuits whose wires all end in measurements gates, correspond to POVMs:

Proposition 3.8.2 (Measurement circuits as POVMs)**.** *Consider a quantum circuit $\mathcal{A}$ with input from $\mathcal{H}$, all of whose output is classical (so, without loss of generality, all wires end in either trace or measurement gates). Then there exists a POVM $(A_x)_{x\in\{0,1\}^m}$ over $\mathcal{H}$, where m is the number of output wires, such that for all $\rho \in \mathfrak{D}(\mathcal{H})$, and all $x \in \{0,1\}^m$,*

$$\Pr[\mathcal{A}(\rho) = x] = \mathrm{Tr}[A_x \rho]\,. \tag{28}$$

Proof. By the principle of deferred measurement, without loss of generality, all measurement gates appear at the end of the circuit, whether followed by trace gates or not. Since all wires end in either measurement gates or trace gates, any measurement gates that are followed by trace gates can be omitted. To see why, consider the state $|\psi\rangle = \sum_{x,y} \alpha_{xy} |x\rangle |y\rangle$, which is the state of the system before any measurement or trace gates are applied, where the x subsystem is to be measured and kept, and the y subsystem is to be traced out, and either (1) measured or (2) not measured before the trace is applied.

In (1), after measuring the entire state, but before applying the trace, the state becomes $|x\rangle |y\rangle$ with probability $|\alpha_{xy}|^2$, and then after applying the trace, it becomes $|x\rangle$. The probability that $|x\rangle$ is obtained is the sum over the y's of the probability of measuring $|x\rangle |y\rangle$, i.e. $\sum_y |\alpha_{xy}|^2$.

In (2), after measuring only the x subsystem, the state becomes $\sum_y \alpha_{xy} |x\rangle |y\rangle$ (normalized) with probability $\sum_y |\alpha_{xy}|^2$. Applying the trace to the y subsystem, the state becomes just $|x\rangle$, and again, the probability that $|x\rangle$ is obtained is $\sum_y |\alpha_{xy}|^2$. Or, we could apply the partial trace first, obtaining the mixed state $\sum_{x,y} |\alpha_{xy}|^2 |x\rangle \langle x|$, and $|x\rangle$ is again obtained by measurement with probability $\sum_y |\alpha_{xy}|^2$.

Similarly, measurements of subsystems of the y subsystem are also equivalent.

Now, consider a purification A of $\mathcal{A}$.

Let $B_x = (\langle x| \otimes \mathbb{1})A(\mathbb{1} \otimes |0\rangle)$, where $|0\rangle$ is the ancillary qubits in $\mathcal{A}$.

Then, let

$$\begin{aligned} A_x &= B_x^\dagger B_x \\ &= (\mathbb{1} \otimes \langle 0|)A^\dagger(|x\rangle \otimes \mathbb{1})(\langle x| \otimes \mathbb{1})A(\mathbb{1} \otimes |0\rangle) \\ &= (\mathbb{1} \otimes \langle 0|)A^\dagger(|x\rangle \langle x| \otimes \mathbb{1})A(\mathbb{1} \otimes |0\rangle), \end{aligned} \tag{29}$$

so that A_x is positive semidefinite for each x, and

$$\begin{aligned}
\sum_x A_x &= \sum_x (\mathbb{1} \otimes \langle 0|) A^\dagger (|x\rangle \langle x| \otimes \mathbb{1}) A (\mathbb{1} \otimes |0\rangle) \\
&= (\mathbb{1} \otimes \langle 0|) A^\dagger \sum_x (|x\rangle \langle x| \otimes \mathbb{1}) A (\mathbb{1} \otimes |0\rangle) \\
&= (\mathbb{1} \otimes \langle 0|) A^\dagger (\sum_x |x\rangle \langle x| \otimes \mathbb{1}) A (\mathbb{1} \otimes |0\rangle) \\
&= (\mathbb{1} \otimes \langle 0|) A^\dagger (\mathbb{1} \otimes \mathbb{1}) A (\mathbb{1} \otimes |0\rangle) \\
&= (\mathbb{1} \otimes \langle 0|) A^\dagger \mathbb{1} A (\mathbb{1} \otimes |0\rangle) \\
&= (\mathbb{1} \otimes \langle 0|) A^\dagger A (\mathbb{1} \otimes |0\rangle) \\
&= (\mathbb{1} \otimes \langle 0|) \mathbb{1} (\mathbb{1} \otimes |0\rangle) \\
&= (\mathbb{1} \otimes \langle 0|) (\mathbb{1} \otimes |0\rangle) \\
&= \mathbb{1} \otimes \langle 0|0\rangle \\
&= \mathbb{1} \otimes 1 \\
&= \mathbb{1}
\end{aligned} \tag{30}$$

Hence $(A_x)_x$ is a POVM. Finally,

$$\begin{aligned}
\Pr[\mathcal{A}(\rho) = x] &= \langle x| (\mathbb{1} \otimes \mathrm{Tr})(A(\rho \otimes |0\rangle \langle 0|) A^\dagger) |x\rangle \ \text{(trace before measurement)} \\
&= \mathrm{Tr}(\langle x| (\mathbb{1} \otimes \mathrm{Tr})(A(\rho \otimes |0\rangle \langle 0|) A^\dagger) |x\rangle) \\
&= \mathrm{Tr}((\mathbb{1} \otimes \mathrm{Tr})(A(\rho \otimes |0\rangle \langle 0|) A^\dagger) |x\rangle \langle x|) \\
&= \mathrm{Tr}(A(\rho \otimes |0\rangle \langle 0|) A^\dagger) |x\rangle \langle x|) \\
&= \mathrm{Tr}(A^\dagger |x\rangle \langle x| A(\rho \otimes |0\rangle \langle 0|) \\
&= \mathrm{Tr}(A^\dagger |x\rangle \langle x| A(\mathbb{1} \otimes |0\rangle) \rho (\mathbb{1} \otimes \langle 0|)) \\
&= \mathrm{Tr}((\mathbb{1} \otimes \langle 0|) A^\dagger |x\rangle \langle x| A(\mathbb{1} \otimes |0\rangle) \rho) \\
&= \mathrm{Tr}[A_x \rho]
\end{aligned} \tag{31}$$

□

As POVMs, measurement statistics from quantum circuits depend only on the mixture of an ensemble of quantum states, not the states individually:

Proposition 3.8.3. *Let $(\rho_x, p_x)_x$ be an ensemble and $\rho = \sum_x p_x \rho_x$ be its mixture. Let X be a random variable defined by $Pr[X = x] = p_x$. Then, for any quantum circuit $\mathcal{A}$ with classical output, written as a POVM $(A_i)_i$ with A_1 corresponding to an output of 1,*

$$\Pr[\ \mathcal{A}(\rho_X) = 1\ ] = \mathrm{Tr}[A_1\rho] = \Pr[\ \mathcal{A}(\rho) = 1\ ], \tag{32}$$

where the first probability is taken over X, and both probabilities are also taken over any internal randomness in $\mathcal{D}$.

Proof.

$$\begin{aligned}
\Pr[\ \mathcal{A}(\rho_X) = 1\ ] &= \sum_x \Pr[\ \mathcal{A}(\rho_X) = 1|\ X = x\ ] Pr[X = x] \\
&= \sum_x \mathrm{Tr}[A_1\rho_x] p_x \\
&= \mathrm{Tr}[A_1 \sum_x p_x \rho_x] \text{ by linearity of Tr and } A_1 \\
&= \mathrm{Tr}[A_1\rho]
\end{aligned} \tag{33}$$

□

Although in this thesis we are only concerned with ensembles over *finite* index sets of x with probabilities p_x, the above can be extended to arbitrary (ρ, P_X) where P_X is a measure defined on a sigma algebra on X and $\rho : X \to \mathfrak{D}(\mathcal{H})$ is P_X-integrable, replacing the convex combinations with integrals.

Corollary 3.8.4. *Ensembles with identical mixtures are indistinguishable.*

Proof.

$$\big|\Pr[\ \mathcal{A}(\rho_X) = 1\ ] - \Pr[\ \mathcal{A}(\sigma_Y) = 1\ ]\big| = \big|\mathrm{Tr}[A_1\rho] - \mathrm{Tr}[A_1\sigma]\big| = \big|\mathrm{Tr}[A_1(\rho - \sigma)]\big| = 0\,. \tag{34}$$

□

It is worth noting that the maximum difference in probability of distinguishing between any pair of states (and hence pairs of ensembles, by linearity) is half of the distance between them, in the 1-norm (see [NC00, Chapter 9]):

Proposition 3.8.5. *Let $\rho, \sigma \in \mathfrak{D}(\mathcal{H})$, then*

$$\max_{0 \leq A \leq \mathbb{1}_{\mathcal{H}}} \mathrm{Tr}[A(\rho - \sigma)] = \tfrac{1}{2}\|\rho - \sigma\|_1 \,. \tag{35}$$

The maximization can equivalently be taken over orthogonal projections only. The maximum is achieved by some orthogonal projection P in either case.

Since quantum circuits built from a universal gate set and computational basis measurements can approximate any unitary, they can approximate optimal measurements. However, the size of the circuit may grow exponentially in the number of qubits in the states.

Related to this is the *diamond norm* (Definition 3.4.9), which we extend here to a metric between admissible maps. Following this proposition, it measures the maximum probability of distinguishing between a pair of them (multiplied by 2).

Definition 3.8.6 (Diamond metric)**.** The *diamond metric*, $D(\cdot,\cdot)_\diamond$, is defined by, for admissible maps $\Phi_1, \Phi_2 : \mathfrak{D}(\mathcal{H}_M) \to \mathfrak{D}(\mathcal{H}_N)$, by

$$D(\Phi_1, \Phi_2)_\diamond := \sup_{\mathcal{H}_E, \rho_{ME} \in \mathfrak{D}(\mathcal{H}_M \otimes \mathcal{H}_E)} \mathbb{E}[\|(\Phi_1 \otimes \mathbb{1}_E)\rho_{ME} - (\Phi_2 \otimes \mathbb{1}_E)\rho_{ME}\|_1] \,, \tag{36}$$

where the expected value is taken over the internal randomness of Φ_1 and Φ_2 (and is equivalent to taking the 1-norm of the difference of mixtures of their outputs).

Note that the supremum is taken over density operators only.

3.8.1 The Quantum One-time Pad

This subsection is from the joint paper [ABF+16].

It is easy to check that applying a uniformly random Pauli operator to any single-qubit density operator results in the maximally mixed state:

$$\frac{1}{4}\left(\rho + X\rho X + Y\rho Y + Z\rho Z\right) = \frac{\mathbb{1}_1}{2} \,, \qquad \text{for all } \rho \in \mathfrak{D}(\mathcal{H}_1) \,. \tag{37}$$

Since the Pauli operators are self-adjoint, we may implement the above map by choosing two bits s and t uniformly at random and then applying

$$\rho \mapsto X^s Z^t \rho Z^t X^s \,.$$

To observers with no knowledge of s and t, the resulting state is information-theoretically indistinguishable from $\mathbb{1}_1/2$. Of course, if we know s and t, we can invert the above map and recover ρ completely.

The above map can be straightforwardly extended to the n-qubit case in order to obtain an elementary *quantum encryption scheme* called the *quantum one-time pad*. We first set $X_j = \mathbb{1}^{\otimes j-1} \otimes X \otimes \mathbb{1}^{\otimes n-j}$ and likewise for Y_j and Z_j. We define the n-qubit Pauli group $\mathcal{P}_n$ to be the subgroup of $\mathrm{SU}(\mathbb{C}^{2^n})$ generated by $\{X_j, Y_j, Z_j : j = 1, \ldots, n\}$. Note that Hermiticity is inherited from the single-qubit case, i.e. $P^\dagger = P$ for every $P \in \mathcal{P}_n$.

Definition 3.8.7. [Quantum one-time pad] For $r \in \{0,1\}^{2n}$, we define the *quantum one-time pad (QOTP)* on n qubits with classical key r to be the map:

$$P_r := \prod_{j=1}^{n} X_j^{r_{2j-1}} Z_j^{r_{2j}} \in \mathcal{P}_n \,.$$

The effect of P_r on any quantum state $\rho \in \mathfrak{D}(\mathbb{C}^{2^n})$ is simply

$$\frac{1}{2^{2n}} \sum_{r \in \{0,1\}^{2n}} P_r \rho P_r = \frac{\mathbb{1}_n}{2^n} \,. \tag{38}$$

As before, the map $\rho \mapsto P_r \rho P_r$ (for uniformly random key r) is an information-theoretically secure symmetric-key encryption scheme for quantum states.

Just as in the classical case [Sha49], any reduction in key length is not possible without compromising information-theoretic security [AMTdW00, BR03]. Of course, in practice the key length of the one-time pad (quantumly or classically) is highly impractical. This is a crucial reason to consider—as we do in this work—encryption schemes which are secure only against computationally bounded adversaries.

3.8.2 Computational Indistinguishability

An important notion in modern cryptography is that of computational indistinguishability. Ciphertext indistinguishability (see Definition 3.9.4 and Definition 4.1.3), defining the security of encryption, is a special case. Computational indistinguishability applies to sequential ensembles:

Definition 3.8.8 (Sequential ensemble)**.** A *sequential ensemble* is a sequence of ensembles of quantum states, $(\rho_n)_{n=1}^{\infty}$ (where ρ_n is taken to be a random variable). Often, such a sequential ensemble will simply be referred to as an *ensemble*, and denoted by $(\rho_n)_n$ or simply ρ_n.

Definition 3.8.9 (Computational indistinguishability)**.** Two sequential ensembles $(\rho_n)_n$ and $(\sigma_n)_n$ are *computationally indistinguishable* if for every QPT $\mathcal{D}$,

$$|Pr[\mathcal{D}(\rho_n) = 1] - Pr[\mathcal{D}(\sigma_n) = 1]| \leq \text{negl}(n)\,, \tag{39}$$

where the probabilities are taken over the randomness inherent in ρ_n and σ_n as ensembles as well as any internal randomness in $\mathcal{D}$.

Typically, the number of registers (size or length) in the ensembles making up a sequential ensemble is polynomially bounded in n, and we assume that their sizes are also at least linear in n, since otherwise we include 1^n as input to $\mathcal{D}$. This ensures that $\mathcal{D}$'s running time is polynomial in n, not the sizes of the states. Usually, also, the ensembles will be generated by a QPTs.

By Proposition 3.8.3, it suffices to consider the mixtures of the ensembles instead of the ensembles themselves.

Note also that computational indistinguishability forms an equivalence relation, i.e. each ensemble is computationally indistinguishable from itself (reflexivity), computational indistinguishability is symmetric, and it is transitive (by the triangle inequality and since the sum of two negligible functions is negligible). Furthermore, the resulting ensembles from the application of a QPT to a pair of computationally indistinguishable ensembles are again computationally indistinguishable, since the composition of the QPT and any QPT distinguisher is a QPT distinguisher acting on the original pair.

3.9 Modern Cryptography

The modern cryptography definitions and results whose quantum analogues are contained in this thesis are given in this section. See [Gol04] for a reference, although the definition of semantic security has been simplified here.

First, we define encryption schemes, both in the private- and public-key settings. These definitions can be relaxed in various ways.

Definition 3.9.1. A *symmetric-key encryption scheme* or *private-key encryption scheme* or *SKE* is a triple of PPTs $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ such that $\mathsf{Dec}(k, (\mathsf{Enc}(k, m)) = m$ for all *keys* $k \in \mathbf{supp}\, \mathsf{KeyGen}(1^n)$ and messages $m \in \{0,1\}^*$. We write $\mathsf{Enc}_k = \mathsf{Enc}(k, \cdot)$ and $\mathsf{Dec}_k = \mathsf{Dec}(k, \cdot)$. $c = Enc_k(m)$ is called a ciphertext (corresponding to m)

Definition 3.9.2. A *public-key encryption scheme* or *PKE* is a triple of PPTs $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ such that $\mathsf{Dec}(sk, (\mathsf{Enc}(pk, m)) = m$ for all $(pk, sk) \in \mathbf{supp}\, \mathsf{KeyGen}(1^n)$ and $m \in \{0,1\}^*$. We write $\mathsf{Enc}_{pk} = \mathsf{Enc}(pk, \cdot)$ and $\mathsf{Dec}_{sk} = \mathsf{Dec}(sk, \cdot)$. pk is called the *public key* and sk, the *secret key* (or *private key*).

The security of an encryption scheme is captured by the equivalent definitions of semantic security and ciphertext indistinguishability. It may also be defined under chosen plaintext attack (CPA), non-adaptive chosen ciphertext attack (CPA1) or adaptive chosen ciphertext attack (CPA2)

Definition 3.9.3 (Semantic Security)**.** A public-key encryption scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is *semantically secure* if for any PPT adversary $\mathcal{A}$, there exists a PPT simulator $\mathcal{S}$ such that for any PPT $\mathcal{M}$ and PT f [1],

$$\Pr\left[\, \mathcal{A}(\mathsf{Enc}_{pk}(m), \sigma) = f_{pk}(m) \,\right] - \Pr\left[\, \mathcal{S}(\sigma) = f_{pk}(m) \,\right] \leq \mathrm{negl}(n)\,, \tag{40}$$

where $(m, \sigma) \leftarrow \mathcal{M}(pk)$,[2] and the probabilities are taken over $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$ and the internal randomness of Enc, $\mathcal{A}$ and $\mathcal{S}$.

[1] Originally, f was any family of functions, not just PT [GM84].
[2] Originally, there was no σ [GM84].

- ***SEM-CPA:*** In addition to the above, $\mathcal{M}, \mathcal{A}$ and $\mathcal{S}$ have oracle access to Enc_{pk}.
- ***SEM-CCA1:*** In addition to SEM-CPA, $\mathcal{M}$ has oracle access to Dec_{sk}.
- ***SEM-CCA2:*** In addition to SEM-CCA1, $\mathcal{A}$ and $\mathcal{S}$ have oracle access to Dec_{sk} but cannot apply it to the challenge ciphertext $\mathsf{Enc}_{pk}(m)$.

In [Gol04], $\mathcal{A}$ and $\mathcal{S}$ are also given access to $h_{pk}(m)$, for some efficiently computable h, representing partial side information, and security must hold for all such h, but this can simply be captured with σ.

Definition 3.9.4 (Ciphertext Indistinguishability)**.** A public-key encryption scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ has *indistinguishable encryptions* if for every PPT adversary $\mathcal{A} = (\mathcal{M}, \mathcal{D})$ we have:

$$\left|\Pr\left[\, \mathcal{D}(\mathsf{Enc}_{pk}(m), \sigma) = 1 \,\right] - \Pr\left[\, \mathcal{D}(\mathsf{Enc}_{pk}(0^{|m|}), \sigma) = 1 \,\right]\right| \leq \mathrm{negl}(n)\,, \tag{41}$$

where $(m, \sigma) \leftarrow \mathcal{M}(pk)$,[2] and the probabilities are taken over $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$ and the internal randomness of Enc, $\mathcal{M}$, and $\mathcal{D}$.

- ***IND-CPA:*** In addition to the above, $\mathcal{M}$ and $\mathcal{D}$ have oracle access to Enc_{pk}.
- ***IND-CCA1:*** In addition to IND-CPA, $\mathcal{M}$ has oracle access to Dec_{sk}.
- ***IND-CCA2:*** In addition to IND-CCA1, $\mathcal{D}$ has oracle access to Dec_{sk} but cannot apply it to the challenge ciphertext $\mathsf{Enc}_{pk}(m)$.

Note that a secure public-key encryption scheme must be CPA-secure, as oracle calls can be implemented directly with access to Enc and pk. Security in the private-key setting is defined similarly, but with $\mathcal{M}$ receiving the security parameter 1^n instead of pk.

Goldwasser and Micali famously proved in [GM84] that indistinguishability implied semantic security (the converse, which is relatively easy to show, was left out):

Theorem 3.9.5. *An encryption scheme is semantically secure if and only if it has indistinguishable encryptions.*

Their equivalence holds for corresponding scenarios only, i.e. in the private- or public-key setting, and under regular attacks, CPA, CCA1 or CCA2. The security definitions can also be extended to the encryption of multiple messages with the same key, so that multiple-message SEM and IND are equivalent to one another. Furthermore, IND-CPA implies multiple message IND-CPA.

Secure encryption schemes are often constructed using cryptographic primitives, in particular, one-way functions, trapdoor one-way permutations, pseudorandom generators and pseudorandom functions.

First, a one-way function is an efficiently computable function that is difficult for PPTs to invert on random inputs.

Definition 3.9.6. A PT-computable function $f : \{0,1\}^* \to \{0,1\}^*$ is a *one-way function (OWF)* if for every PPT $\mathcal{A}$,

$$\Pr_{x \xleftarrow{\$} \{0,1\}^n} [\mathcal{A}(f(x), 1^n) \in f^{-1}(f(x))] \leq \mathrm{negl}(n)\,. \tag{42}$$

A trapdoor one-way permutation is an (efficiently) indexed family of one-way permutations (injective one-way functions that preserve the lengths of their inputs) that are easy to invert given a string, called the trapdoor.

Definition 3.9.7. A *trapdoor one-way permutation (TOWP)* is a PT-computable collection

$$f = \{f_i : D_i \to D_i\}_{i \in I}$$

of permutations on sets $D_i \subseteq \{0,1\}^{l(i)}, i \in I$, for some (infinite) set I of strings, and a PT-computable function $l : \mathbb{N} \to \mathbb{N}$, together with a triple of PPTs $(\mathcal{G}, \mathcal{S}, \mathcal{I})$ which

1. (generate (index, trapdoor) pair) $\mathbf{supp}\, \mathcal{G}(1^n) \subseteq (I \cap \{0,1\}^n) \times \{0,1\}^n$;
2. (sample from domain) for all $i \in I$, $\mathbf{supp}\, \mathcal{S}(i) = D_i$;
3. (invert using trapdoor) for all $(i,t) \in \mathbf{supp}\, \mathcal{G}(1^n)$ and all $x \in D_i$, $\mathcal{I}(f_i(x), t) = x$,

such that for every PPT $\mathcal{A}$,

$$\Pr_{(i,t) \leftarrow \mathcal{G}(1^n), x \leftarrow S(i)} [\mathcal{A}(f_i(x), i) = x] \leq \mathrm{negl}(n)\,. \tag{43}$$

A hard-core of a one-way function f is a predicate whose value on a random x is infeasible to guess with probability non-negligibly better than $\frac{1}{2}$, even given access to $f(x)$:

Definition 3.9.8. A PT-computable $b : \{0,1\}^* \to \{0,1\}$ is a *hard-core* of a OWF f if for every PPT $\mathcal{A}$,

$$\Pr_{x \xleftarrow{\$} \{0,1\}^n} [\mathcal{A}(f(x), 1^n) = b(x)] \leq \frac{1}{2} + \mathrm{negl}(n)\,. \tag{44}$$

The definition of hard-core may also be modified in the case of trapdoor one-way functions or permutations in the obvious way, by indexing f and b by i, generating $x \leftarrow S(i)$, where $(i,t) \leftarrow \mathcal{G}(1^n)$, and giving $\mathcal{A}$ access to i in place of 1^n.

Definition 3.9.9. A *hard-core* of a TOWP $(f, \mathcal{G}, \mathcal{S}, \mathcal{I})$ is a PT-computable collection $b = \{b_i : D_i \to \{0,1\}\}_{i \in I}$ such that for every PPT $\mathcal{A}$,

$$\Pr_{(i,t) \leftarrow \mathcal{G}(1^n), x \leftarrow S(i)} [\mathcal{A}(f_i(x), i) = b_i(x)] \leq \frac{1}{2} + \mathrm{negl}(n)\,. \tag{45}$$

Theorem 3.9.10 (Goldreich-Levin Theorem)**.** *[Gol06] If OWFs (or TOWPs) exist, then OWFs (or TOWPs, respectively) with hard-cores exist.*

Next is the pseudorandom generator, which expands a uniformly random seed to an output that is computationally indistinguishable from a longer uniformly random string, hence "pseudorandom".

Definition 3.9.11. A PT-computable function $G : \{0,1\}^* \to \{0,1\}^*$ is a *pseudorandom generator (PRG)* if $|G(s)| = p(|s|)$ for all $s \in \{0,1\}^*$ and for every PPT $\mathcal{D}$,

$$\left| \Pr_{s \xleftarrow{\$} \{0,1\}^n} [\mathcal{D}(G(s)) = 1] \quad - \Pr_{y \xleftarrow{\$} \{0,1\}^{p(n)}} [\mathcal{D}(y) = 1] \right| \leq \mathrm{negl}(n)\,. \tag{46}$$

Note that p must necessarily itself be PT-computable, and hence polynomially bounded.

Pseudorandom generators can be constructed from one-way functions [HILL99] or more easily from trapdoor one-way permutations with hard-cores [Gol06].

A pseudorandom function is an efficiently computable family of functions which are indistinguishable from perfectly random functions, even when allowed to query an oracle for the given function polynomially many times.

Definition 3.9.12. A PT-computable function family

$$f = \{f^{(n)} : \{0,1\}^n \times \{0,1\}^{p(n)} \to \{0,1\}^{\ell(n)}\}_{n\in\mathbb{N}}\,,$$

with $p, \ell : \mathbb{N} \to \mathbb{N}$ PT-computable, is a *pseudorandom function (PRF)* if for every PPT $\mathcal{D}$ equipped with an oracle,

$$\left| \Pr_{k \xleftarrow{\$} \{0,1\}^n} [\mathcal{D}^{f_k}(1^n) = 1] \quad - \Pr_{g \xleftarrow{\$} \{\{0,1\}^{p(n)} \to \{0,1\}^{\ell(n)}\}} [\mathcal{D}^{g}(1^n) = 1] \right| \leq \mathrm{negl}(n)\,, \tag{47}$$

where $f_k := f^{(n)}(k, \cdot) : \{0,1\}^{p(n)} \to \{0,1\}^{\ell(n)}$ for $k \in \{0,1\}^n$.

Pseudorandom functions can be constructed from pseudorandom generators [GGM86]. Hence, combining the two results,

Theorem 3.9.13. *If one-way functions exist, then pseudorandom functions exist.*

Finally, pseudorandom functions and trapdoor one-way permutations with hard-cores can be used to construct secure private-key and public-key encryption schemes, respectively. Hence,

Theorem 3.9.14. *If one-way functions exist, then so do IND-CCA1-secure private-key encryption schemes.*

Theorem 3.9.15. *If trapdoor one-way permutations exist, then so do semantically secure public-key quantum encryption schemes.*

Chapter 4

Computational Security of Quantum Encryption

This chapter is taken from the joint paper [ABF+16].

4.1 Quantum Encryption and Indistinguishability

In this section, we give general definitions of encryption schemes for quantum data (Section 4.1.1) and a corresponding notion of indistinguishability, including IND-CPA and IND-CCA1 (Section 4.1.2.)

The definitions of quantum encryption schemes Definitions 4.1.1 and 4.1.2 in Subsection 4.1.1, have been modified slightly from the original paper [ABF+16] for this thesis.

4.1.1 Quantum Encryption Schemes

We start by defining *symmetric-key encryption for quantum data*. In the following we assume that the secret key is a classical bitstring, while the plaintext and the ciphertext can be arbitrary quantum states.

We refer to $\mathcal{K}$ as the key space and we assume that $\mathcal{K} := \{0,1\}^*$. The key-generation algorithm, KeyGen, accepts a description of the security parameter n in

unary (i.e. 1^n) and outputs a classical key of length n. We let $\mathcal{H}_{M,n}$ and $\mathcal{H}_{C,n}$ denote the message (or plaintext) and ciphertext spaces for the security parameter 1^n, respectively. We remark that these are potentially infinite families of spaces, i.e. $\mathcal{H}_{M,n} = \{\mathcal{H}_{M,n}^{(i)}\}_i$ and $\mathcal{H}_{C,n} = \{\mathcal{H}_{C,n}^{(i)}\}_i$, and we thus define $\mathfrak{D}(\mathcal{H}_{M,n}) = \bigcup_i \mathfrak{D}(\mathcal{H}_{M,n}^{(i)})$ and $\mathfrak{D}(\mathcal{H}_{C,n}) = \bigcup_i \mathfrak{D}(\mathcal{H}_{C,n}^{(i)})$

Encryption, Enc, accepts a classical key and a plaintext, and outputs a ciphertext; decryption, Dec, accepts a classical key and a ciphertext, and outputs a plaintext. We assume that the encryption and decryption algorithms output a fixed state denoting failure on input states not from the correct plaintext or ciphertext spaces, respectively. The correctness guarantee is that plaintexts are preserved under encryption followed by decryption under the same key.

Definition 4.1.1. A *quantum symmetric-key encryption scheme* or *quantum private-key encryption scheme* or *qSKE* is a triple of QPTs:

1. (key generation) $\mathsf{KeyGen} : 1^n \mapsto k \in \mathcal{K}$
2. (encryption with $k \in \mathbf{supp}\, \mathsf{KeyGen}(1^n)$)
$$\mathsf{Enc}_k := \mathsf{Enc}(k, \cdot) : \mathfrak{D}(\mathcal{H}_{M,n}) \to \mathfrak{D}(\mathcal{H}_{C,n})$$
3. (decryption with $k \in \mathbf{supp}\, \mathsf{KeyGen}(1^n)$)
$$\mathsf{Dec}_k := \mathsf{Dec}(k, \cdot) : \mathfrak{D}(\mathcal{H}_{C,n}) \to \mathfrak{D}(\mathcal{H}_{M,n})$$

such that for all $k \in \mathbf{supp}\, \mathsf{KeyGen}(1^n)$,

$$\mathsf{Dec}_k \circ \mathsf{Enc}_k = \mathbb{1}_{M,n} \tag{48}$$

In order to further simplify notation, the subscript n will be dropped from the spaces, i.e. we write $\mathcal{H}_M$ instead of $\mathcal{H}_{M,n}$, $\mathbb{1}_M$ instead of $\mathbb{1}_{M,n}$, and $\mathcal{C}_M$ instead of $\mathcal{C}_{M,n}$. Later, we will define additional Hilbert spaces (or families of Hilbert spaces) $\mathcal{H}_E$ and $\mathcal{H}_F$ in order to model auxiliary information used by some adversary, and again these implicitly depend on the input the adversaries receive.

Next, we define a notion of *public-key encryption for quantum data*. In addition to the usual spaces from the symmetric-key setting above, we now also have a public key of polynomially bounded length. We define the related public-key space as $\mathcal{K}_{pub} \subseteq \{0,1\}^*$ and reuse $\mathcal{K}$ for the corresponding private-key space, whose length is also polynomially bounded, noting that in this case, neither need be the entirety of $\{0,1\}^*$. Furthermore, rather than depending simply on n, the message (or plaintext) and ciphertext spaces may in general depend upon the public key pk, i.e. we write $\mathcal{H}_{M,pk}$ and $\mathcal{H}_{C,pk}$. Again, we will later drop the pk subscripts, but the definition is presented below with it for clarity.

Definition 4.1.2. A *quantum public-key encryption scheme* or *qPKE* is a triple of QPTs:

1. (key-pair generation) $\mathsf{KeyGen} : 1^n \mapsto (pk, sk) \in \mathcal{K}_{pub} \times \mathcal{K}$
2. (encryption with public key $pk \in \mathcal{K}_{pub}, (pk, sk) \in \mathbf{supp}\, \mathsf{KeyGen}(1^n)$)
$$\mathsf{Enc}_{pk} := \mathsf{Enc}(pk, \cdot) : \mathfrak{D}(\mathcal{H}_{M,pk}) \to \mathfrak{D}(\mathcal{H}_{C,pk})$$
3. (decryption with private key $sk \in \mathcal{K}, (pk, sk) \in \mathbf{supp}\, \mathsf{KeyGen}(1^n)$)
$$\mathsf{Dec}_{sk} := \mathsf{Dec}(sk, \cdot) : \mathfrak{D}(\mathcal{H}_{C,pk}) \to \mathfrak{D}(\mathcal{H}_{M,pk})$$

such that for all $(pk, sk) \in \mathbf{supp}\, \mathsf{KeyGen}(1^n)$,

$$\mathsf{Dec}_{sk} \circ \mathsf{Enc}_{pk} = \mathbb{1}_{M,pk} \tag{49}$$

Remarks Some variations on the above two definitions are also possible. For instance, one could restrict the messages spaces to particular subsets of the density operators on Hilbert spaces. In the paper [ABF+16], a uniform diamond metric (Definition 3.8.6) relaxation is used in both definitions for (48) and (49), and only exact decryption was noted as an alternative. That is, we would only require

$$D(\mathsf{Dec}_{sk} \circ \mathsf{Enc}_{pk}, \mathbb{1}_M)_\diamond \leq \mathrm{negl}(n), \tag{50}$$

uniformly in the key-pairs $(pk, sk) \in \mathbf{supp}\,\mathsf{KeyGen}(1^n)$. This allows errors in encryption and decryption with negligible probability for each pair of keys. One can weaken the condition further to

$$\mathbb{E}[\|(\mathsf{Dec}_k \circ \mathsf{Enc}_k \otimes \mathbb{1}_E)(\rho_{ME}) - \rho_{ME}\|_1] \leq \mathrm{negl}(n)\,, \tag{51}$$

for all $\mathcal{H}_E$ and $\rho_{ME} \in \mathcal{H}_M \otimes \mathcal{H}_E$, where the expected value is taken over $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$ and the internal randomness of Enc_{pk} and Dec_{sk}. This even allows a negligible probability of choosing keys for which large errors are consistently obtained. An even weaker constraint could be a computational one, along the lines of computational indistinguishability.

4.1.2 Indistinguishability of Encryptions

Following the classical definition, the security notion of *quantum indistinguishability under chosen plaintext attacks* has been considered previously for the case of quantum encryption schemes in [BJ15] and for classical encryption schemes in [GHS15]. Here, we extend the definition of [BJ15] to the CCA1 (chosen ciphertext attack) setting. The security definitions are formulated with the public-key (or asymmetric-key) setting in mind, and we clarify when meaningful differences in the symmetric-key setting arise.

Our definition models a situation in which an honest user encrypts messages of the adversary's choice; the adversary then attempts to match the ciphertexts to the plaintexts. In our formulation, an IND adversary $\mathcal{A} = (\mathcal{M}, \mathcal{D})$ consists of two QPTs: the *message generator*, $\mathcal{M}$, and the *distinguisher*, $\mathcal{D}$. The message generator takes as input the security parameter and a public key, and outputs a challenge state consisting of a plaintext and some auxiliary information. The auxiliary information models, for instance, the fact that the output state might be entangled with some internal state of the adversary itself. Then the distinguisher receives this auxiliary information, and a state which might be either the encryption of the original challenge state or the encryption of the zero state. The distinguisher's goal is to decide which of the two is the case.

Security in this model requires that the adversary does not succeed with probability significantly better than guessing. We also define two standard variants: indistinguishability under chosen plaintext attack (IND-CPA) and indistinguishability under chosen ciphertext attack (IND-CCA1). We leave the definition of CCA2 (adaptive chosen ciphertext attack) security as an interesting open problem. As before, all circuits are indexed by the security parameter.

Definition 4.1.3 (IND)**.** A qPKE scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ has *indistinguishable encryptions* (or is *IND secure*) if for every QPT adversary $\mathcal{A} = (\mathcal{M}, \mathcal{D})$ we have:

$$\begin{aligned} &\big|\Pr\big[\, \mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho_{ME} = 1 \,\big] \\ &- \Pr\big[\, \mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)(|0\rangle\langle 0|_M \otimes \rho_E) = 1 \,\big]\big| \leq \mathrm{negl}(n)\,, \end{aligned} \tag{52}$$

where $\rho_{ME} \leftarrow \mathcal{M}(pk)$, $\rho_E = \mathrm{Tr}_M(\rho_{ME})$, and the probabilities are taken over $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$ and the internal randomness of Enc, $\mathcal{M}$, and $\mathcal{D}$.

- ***IND-CPA:*** In addition to the above, $\mathcal{M}$ and $\mathcal{D}$ have oracle access to Enc_{pk}.
- ***IND-CCA1:*** In addition to IND-CPA, $\mathcal{M}$ has oracle access to Dec_{sk}.

Here we use $|0\rangle\langle 0|_M$ to denote $|0^m\rangle\langle 0^m|$, where m is the number of qubits in the M register.

The definition is illustrated in Figure 2. The symmetric-key scenario is the same, except $pk = sk$, and $\mathcal{M}$ receives only a blank input. We remark that in the public-key setting, IND implies IND-CPA: an adversary with knowledge of pk can easily simulate the Enc_{pk} oracle. Note that, under CPA, the IND definition is known to be equivalent to IND in the *multiple-message* scenario [BJ15]. Section 6.2 contains the details.

4.2 Quantum Semantic Security

This section is devoted to defining quantum semantic security (Section 4.2.2), and showing its equivalence with quantum indistinguishability (Section 4.2.3).

Following the classical definition, the security notion of *quantum semantic security under chosen plaintext attacks* has been given previously in [GHS15] for the case

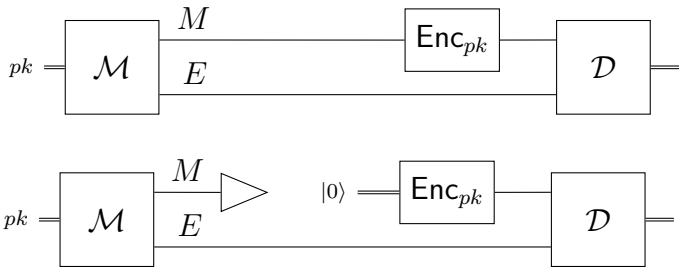

Figure 2: IND posits that a QPT $(\mathcal{M}, \mathcal{D})$ cannot distinguish between these two scenarios.

of a special class of quantum states arising when considering quantum access to classical encryption schemes. Here, we give a more general definition for arbitrary quantum plaintexts. As we outlined the classical situation with semantic security in Section 1.2.1, we start with a discussion of some difficulties in transitioning to the quantum setting. A similar discussion can be found in [GHS15] and we explain below where and why we make different choices.

4.2.1 Difficulties in the Quantum Setting

When attempting to transfer the definition of semantic security to the quantum world, the main question one encounters is to determine the quantum equivalents of σ and $f(m)$ (as it is relatively clear that the plaintext m would have as quantum equivalent a quantum state ρ_M, in a *message register*, M).

For the case of the side-information, σ, one might attempt to postulate that this side information is available via the output of a quantum map Φ_h, evaluated on ρ_M. There are, however, two obvious problems with this approach: firstly, it is unclear how to *simultaneously* generate both ρ_M and $\Phi_h(\rho_M)$ (the main obstacle stemming from the quantum *no-cloning* theorem [WZ82], according to which it is not possible to perfectly copy an unknown quantum state)[1]. Secondly, it is well-established that

[1] [GHS15] solves the issue by essentially requiring that the quantum circuits generating messages use no measurement gates, but instead output random states by taking random classical strings as input. Hence, multiple plaintext states can be generated by using the same string.

the most general type of quantum side-information includes entanglement (contrary to the scenario studied in [GHS15]). We therefore conclude that side information should be modelled simply as an extra register (called E) such that ρ_{ME} are in an arbitrary quantum state (as generated by some process—for a formal description, see Definition 4.2.1).

For the case of the target function f, one might also postulate a quantum map Φ_f, the goal then (for both the adversary and simulator), being to output $\Phi_f(\rho_M)$. However, given that quantum states and maps form a continuum, one must exercise care in quantifying when a simulator has successfully simulated the adversary. We propose three possible tests for quantifying "success" in the semantic security game, each leading to its own definition. Since we show that all three definitions are equivalent, we conclude that it is a matter of taste (or context) which definition to label as *the* definition of quantum semantic security. We focus in this section on the first one, which we called SEM, because we find it the most natural. We give formal definitions and proofs of equivalence for all three definitions in Appendix 4.4. Here is an overview of the three different notions:

- **SEM.** In Definition 4.2.1, a state ρ_{MEF} is generated; intuitively, the contents of register F can be seen as a "target" output that the adversary tries to achieve (however, this is not quite the case as we point out shortly). We then postulate a quantum polynomial time *distinguisher* who is given the F register and charged with distinguishing the output of the adversary from the output of the simulator, with security being associated with the inability of the distinguisher in telling the two situations apart. We thus see that the role of register F is actually to assist the distinguisher: semantic security corresponds to the situation where the distinguisher essentially cannot tell the real from ideal apart, *even with access to the F system*.

- **SEM2**. In Definition 4.4.2, we specify instead that the state ρ_{MEF} be a *classical-quantum state*. That is, ρ_{ME} is quantum, but the register F contains a classical pure state, and hence $\rho_{MEF} = \rho_{ME} \otimes \rho_F$, with ρ_F corresponding to a binary string. The requirement for security is that the simulator should provide

a classical output that equals the contents of F, essentially just as well as the adversary can.

- **SEM3**. In Definition 4.4.5, we introduce a classical function f, thus closely mimicking the classical definition. Here, there is no subsystem F, but the target $f(x)$ takes its place, where x is precisely the results of any measurements used to generate ρ_{ME} (thus, x is, in a sense, a full "classical description" of ρ_{ME}). The requirement for security is that the simulator is able to output $f(x)$ (for any f) with essentially the same probability as the adversary.

4.2.2 Definition of Semantic Security

As before, we work primarily in the public-key setting; adaptation to the private-key setting is again straightforward. In our concrete formulation of SEM (Definition 4.2.1), we define the following QPT machines: the *message generator* $\mathcal{M}$ (which generates ρ_{MEF}), the *adversary* $\mathcal{A}$, the *simulator* $\mathcal{S}$ and the *distinguisher* $\mathcal{D}$.

Definition 4.2.1. [SEM] A qPKE scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is *semantically secure* if for any QPT adversary $\mathcal{A}$, there exists a QPT simulator $\mathcal{S}$ such that for all QPTs $\mathcal{M}$ and $\mathcal{D}$,

$$\begin{aligned}\Big|\Pr\big[\,\mathcal{D}(\mathcal{A}\otimes \mathbb{1}_F)(\mathsf{Enc}_{pk}\otimes \mathbb{1}_{EF})\rho_{MEF}=1\,\big] \\ -\Pr\big[\,\mathcal{D}(\mathcal{S}\otimes \mathbb{1}_F)\rho_{EF}=1\,\big]\Big| \le \mathrm{negl}(n)\,,\end{aligned} \tag{53}$$

where $\rho_{MEF} \leftarrow \mathcal{M}(pk)$, $\rho_{EF} = \mathrm{Tr}_M(\rho_{MEF})$, and the probabilities are taken over $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$ and the internal randomness of Enc, $\mathcal{A}, \mathcal{S}, \mathcal{M}$ and $\mathcal{D}$.

- ***SEM-CPA:*** In addition to the above, all QPTs have oracle access to Enc_{pk}.
- ***SEM-CCA1:*** In addition to SEM-CPA, $\mathcal{M}$ has oracle access to Dec_{sk}.

The interactions among the QPTs are illustrated in Figure 3. A few remarks are in order. First, all the registers above are uniformly of size polynomial in n. Second, the input and output registers of the relevant QPTs are understood from context, e.g., the expression $(\mathcal{S}\otimes \mathbb{1}_F)\rho_{EF}$ makes clear that the input register of $\mathcal{S}$ is E. Third, we

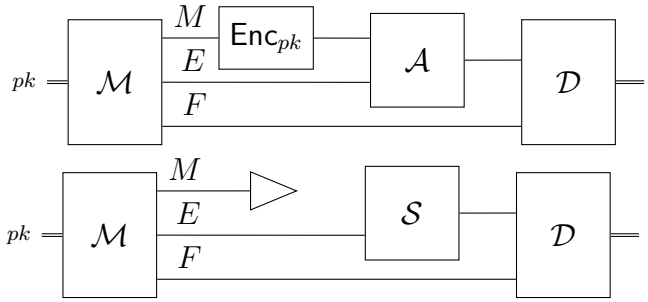

Figure 3: SEM: for all adversaries $\mathcal{A}$ there exists a simulator $\mathcal{S}$ such that these two scenarios are indistinguishable.

note that SEM implies SEM-CPA in the public-key setting, since access to the public key implies simulatability of Enc_{pk}. Finally, just as in the case of IND, adapting to the symmetric-key setting is simply a matter of setting $pk = sk$ and positing that $\mathcal{M}$ receives only a blank input.

The classical (uniform) definition of semantic security (Definition 3.9.3) is recovered as a special case, as follows. All of the QPTs are PPTs, and the message generator $\mathcal{M}$ outputs classical plaintext m, side information σ and target function $f(m)$ on top of σ. The distinguisher $\mathcal{D}$ simply checks whether the adversary's (or simulator's) output is equal to the contents of the F register.

4.2.3 Semantic Security Is Equivalent to Indistinguishability

While semantic security gives a strong and intuitively meaningful definition of security, indistinguishability is typically easier to prove and work with. In this section we show that—just as in the classical setting—the two notions are equivalent. This proves Theorem 1.2.1. The equivalence holds for all of the variants of Definition 4.1.3 and Definition 4.2.1: under either public or private-key, we have equivalence of IND with SEM, IND-CPA with SEM-CPA, and IND-CCA1 with SEM-CCA1. Here, we focus on the SEM definition; see Appendix 4.4 for the equivalence with the SEM2 and SEM3 definitions.

Theorem 4.2.2 (IND $\implies$ SEM)**.** *If a quantum encryption scheme*

$(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *has indistinguishable encryptions (IND), then it is semantically secure (SEM).*

Proof. Suppose that an encryption scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ has indistinguishable encryptions. Let $\mathcal{A}$ be QPT SEM attacker against semantic security as in Definition 4.2.1. We define the QPT SEM simulator $\mathcal{S}$ as follows: $\mathcal{S}$ does not receive $\mathsf{Enc}_{pk}(\rho_M)$, but instead runs $\mathcal{A}$ on input $(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)(|0\rangle\langle 0| \otimes \rho_E)$ and outputs whatever $\mathcal{A}$ outputs. Let $\mathcal{M}$ be a QPT SEM message generator that outputs ρ_{MEF}.

Assume for a contradiction the existence of a QPT SEM distinguisher $\mathcal{D}$ which successfully distinguishes the output of $\mathcal{A}$ from the output of $\mathcal{S}$ (with the help of register F), then the combination of $\mathcal{A}$ and $\mathcal{D}$ successfully distinguishes $(\mathsf{Enc}_{pk} \otimes I_{EF})\rho_{MEF}$ from $(\mathsf{Enc}_{pk} \otimes I_{EF})(|0\rangle\langle 0| \otimes \rho_{EF})$, hence contradicting the indistinguishability. □

In the private-key setting without CPA oracle access, $\mathcal{S}$ runs $\mathsf{KeyGen}(1^n)$ to generate his own secret key k', and then encrypts $|0^n\rangle\langle 0^n|$ using k' instead of k. The challenges $(\mathsf{Enc}_k \otimes \mathbb{1}_E)(|0\rangle\langle 0| \otimes \rho_E)$ and $(\mathsf{Enc}_{k'} \otimes \mathbb{1}_E)(|0\rangle\langle 0| \otimes \rho_E)$ will be distributed identically since k and k' are and ρ_E doesn't depend on the key. Hence, the success probability of the SEM simulator $\mathcal{S}$ does not change.

In case of CPA and CCA1 oracles, both for the public- and private-key setting, the simulator $\mathcal{S}$ forwards $\mathcal{A}$'s oracle queries to his own oracle(s), and $\mathcal{S}$ obtains $\mathcal{A}$'s input state by a call to his encryption oracle on state $|0\rangle\langle 0|$, joined with his auxiliary information ρ_E.

Note that we defined semantic security with quantifiers as $\forall\mathcal{A}\exists\mathcal{S}\forall\mathcal{M}\forall\mathcal{D}$, but the above proof actually yields $\exists\mathcal{S}\forall\mathcal{A}\forall\mathcal{M}\forall\mathcal{D}$, where $\mathcal{S}$ is an oracle algorithm with oracle access to $\mathcal{A}$, i.e. $\mathcal{S}$'s strategy is essentially the same no matter the adversary $\mathcal{A}$.

Theorem 4.2.3 (SEM $\implies$ IND)**.** *If a quantum encryption scheme* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *is semantically secure (SEM), then it has indistinguishable encryptions (IND).*

Proof. Let $(\mathcal{M}, \mathcal{D})$ be an IND adversary such that $\mathcal{D}$ distinguishes $(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho_{ME}$ from $(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)(|0\rangle\langle 0| \otimes \rho_E)$ with advantage $\varepsilon(n)$ if $\rho_{ME} \leftarrow \mathcal{M}$. Let us consider the SEM message generator $\mathcal{M}'$ which runs $\rho_{ME} \leftarrow \mathcal{M}$ and outputs (with probability

$\frac{1}{2}$ each) either the state $\rho_{ME} \otimes |1\rangle\langle 1|_F$ or the state $|0\rangle\langle 0|_M \otimes \rho_E \otimes |0\rangle\langle 0|_F$. Next we consider the SEM attacker $\mathcal{A}$ which runs $\mathcal{D}$ and outputs the classical bit that $\mathcal{D}$ outputs. We also consider the SEM attacker $\mathcal{A} \oplus 1$, which outputs the opposite bit. As SEM distinguisher, let us consider the procedure which compares $\mathcal{A}$'s output bit to a measurement (in the computational basis) of the qubit in register F. Any SEM simulator $\mathcal{S}$ that does not have access to the encrypted M-register has to guess the state of the random bit in F and will be correct with probability $1/2$. Then $\varepsilon(n)$ is twice the maximum of the advantages that $\mathcal{A}$ and $\mathcal{A} \oplus 1$ have in successfully predicting F over $1/2$, the probability of success of any simulator. By SEM, both of these advantages are negligible, and hence so is $\varepsilon(n)$. □

4.3 Quantum Encryption Schemes

We now turn to the question of existence for encryption schemes for quantum data. We present two schemes based on the existence of classical functions which are difficult to invert for quantum computers. The first scheme (Section 4.3.1) is symmetric-key and IND-CCA1-secure; the second scheme (Section 4.3.2) is public-key and IND-CPA-secure, and hence, by Theorem 4.2.3, also semantically secure. The cryptographic primitives in this section are quantum-secure versions of those in Section 3.9.

4.3.1 Quantum Symmetric-Key Encryption from One-Way Functions

In this section, we prove Theorem 1.2.2: *If quantum-secure one-way functions exist, then so do IND-CCA1-secure private-key quantum encryption schemes.*

The proof proceeds in two steps. First, we define quantum-secure one-way functions (qOWFs) and quantum-secure pseudorandom functions (qPRFs); we can argue as in the classical world that qPRFs exist if qOWFs do (Theorem 4.3.3.) Second, we show that any qPRF can be used to construct an explicit IND-CCA1-secure symmetric-key scheme for quantum data.

We begin with the formal definitions of qOWFs and qPRFs, and a statement of

the result connecting the two.

First, a quantum-secure one-way function is an efficiently computable function that is difficult for QPTs to invert on random inputs.

Definition 4.3.1. A PT-computable function $f : \{0,1\}^* \to \{0,1\}^*$ is a *quantum-secure one-way function (qOWF)* if for every QPT $\mathcal{A}$,

$$\Pr_{x \xleftarrow{\$} \{0,1\}^n} [\mathcal{A}(f(x), 1^n) \in f^{-1}(f(x))] \leq \mathrm{negl}(n)\,. \tag{54}$$

Next, a quantum-secure pseudorandom function is an efficiently computable family of functions which are indistinguishable to QPTs from perfectly random functions, even when allowed to query an oracle for the given function polynomially many times.

Definition 4.3.2. A PT-computable function family

$$f = \{f^{(n)} : \{0,1\}^n \times \{0,1\}^{p(n)} \to \{0,1\}^{\ell(n)}\}_{n \in \mathbb{N}}\,,$$

with $p, \ell : \mathbb{N} \to \mathbb{N}$ PT-computable, is a *quantum-secure pseudorandom function (qPRF)* if for every QPT $\mathcal{D}$ equipped with a classical oracle,

$$\left| \Pr_{k \xleftarrow{\$} \{0,1\}^n} [\mathcal{D}^{f_k}(1^n) = 1] \quad - \Pr_{g \xleftarrow{\$} \{\{0,1\}^{p(n)} \to \{0,1\}^{\ell(n)}\}} [\mathcal{D}^{g}(1^n) = 1] \right| \leq \mathrm{negl}(n)\,, \tag{55}$$

where $f_k := f^{(n)}(k, \cdot) : \{0,1\}^{p(n)} \to \{0,1\}^{\ell(n)}$ for $k \in \{0,1\}^n$.

We remark that, to some readers, the restriction to classical oracles might seem artificial. While one can certainly consider functions with the *stronger* guarantee of resistance to quantum adversaries with quantum oracle access, stronger functions are not necessary to establish our results. We thus opt for the weaker primitive. In either case, the following holds.

Theorem 4.3.3. *If qOWFs exist, then qPRFs exist.*

Since our definitions are in terms of *classical* oracles, the classical proof that shows that qOWFs imply qPRFs carries through [HILL99, GGM86]. We remark that Zhandry [Zha12] extended this result to the case of functions secure against

quantum superposition queries, what he calls "quantum-secure PRFs." It should be noted that the proof of the Theorem 4.3.3 actually implies the existence of a qPRF for any PT-computable choice of the parameters p and ℓ in Definition 4.3.2.

We are now ready to proceed with the second part of the proof of Theorem 1.2.2, namely the construction of an encryption scheme from a given qPRF. Essentially, this scheme encrypts a quantum state ρ by first selecting a random string r, then inputting r into a qPRF; the output $f_k(r)$ is then used as an encryption key for the quantum one-time pad, $P_{f_k(r)}$ (see Subsection 3.8.1).

Scheme 1. If $f = \{f^{(n)} : \{0,1\}^n \times \{0,1\}^{2n} \to \{0,1\}^{2n}\}_{n\in\mathbb{N}}$ is a qPRF, then let qPRF-SKE be the following triple of QPT algorithms:

1. (key generation) $\mathsf{KeyGen}(1^n)$: output $k \xleftarrow{\$} \{0,1\}^n$;
2. (encryption) $\mathsf{Enc}_k(\rho)$, for $\rho \in \mathfrak{D}(\mathbb{C}^{2^n})$, an n-qubit state: choose $r \xleftarrow{\$} \{0,1\}^{2n}$ and output $|r\rangle\langle r| \otimes P_{f_k(r)}\rho P_{f_k(r)}$,
3. (decryption) $\mathsf{Dec}_k(\sigma)$, for $\sigma \in \mathfrak{D}(\mathbb{C}^{2^{3n}})$, a $3n$-qubit state: measure the first $2n$ qubits in the computational basis to obtain $r' \in \{0,1\}^{2n}$; apply $P_{f_k(r')}$ to the remaining n qubits and output the result.

For simplicity, we chose $\mathfrak{D}(\mathbb{C}^{2^n})$ for the plaintext space, and $\mathfrak{D}(\mathbb{C}^{2^{3n}})$ for the ciphertext space; we can easily adapt the above to other polynomially related cases by selecting a qPRF with different parameters. The correctness of Scheme 1 is easily verified:

$$\mathsf{Dec}_k(\mathsf{Enc}_k(\rho)) = \mathsf{Dec}_k\big(|r\rangle\langle r| \otimes P_{f_k(r)}\rho P_{f_k(r)}\big) = P_{f_k(r)}P_{f_k(r)}\rho P_{f_k(r)}P_{f_k(r)} = \rho\,, \quad (56)$$

where the second equality follows from the definition of the decryption function and the last step is due to the fact that the Pauli operators are self-inverse. Next, we show that the scheme is secure against non-adaptive chosen ciphertext attacks. The classical version of this result is standard, and we use essentially the same proof; see, e.g., Proposition 5.4.18 in Goldreich's textbook [Gol04].

Lemma 4.3.4. *If f is a qPRF, then Scheme 1 is an IND-CCA1-secure symmetric-key quantum encryption scheme as defined in Definition 4.1.3.*

Proof. First, we analyse the security of the scheme in an idealized scenario where f is a truly random function. We claim that in this case, $\mathcal{A}$ correctly guesses the challenge with probability at most $1/2 + \mathrm{negl}(n)$(see Definition 4.4.7). In fact, this bound holds for a stronger adversary $\mathcal{A}'$, who has access to a classical oracle for f prior to the challenge, and access to polynomially many pairs $(r_i, f(r_i))$ for random $r_i, 1 \leq i \leq q$, after the challenge. This adversary is stronger than $\mathcal{A}$ since it can simulate $\mathcal{A}$ by implementing Enc_f and Dec_f oracles using its f oracles. Since the input r into f in the challenge ciphertext is uniformly random, the probability that any of the polynomially many oracle calls of $\mathcal{A}'$ uses the same r is negligible. In the case that no oracle calls use r, the mixtures of the inputs to $\mathcal{A}'$ (including the pairs $(r_i, f(r_i))$) are the same for the original challenge and the zero challenge. This fact can be verified by first averaging over the values of $f(r)$: since f is uniformly random, $f(r)$ is also uniformly random as well as independent of the other values of f (and hence ρ_{ME}). In both cases, applying the quantum one-time pad results in the state:

$$|r\rangle\langle r| \otimes \frac{1}{2^n}\mathbb{1} \otimes \rho_E \otimes |r_1\rangle\langle r_1| \otimes |f(r_1)\rangle\langle f(r_1)| \otimes \cdots \otimes |r_q\rangle\langle r_q| \otimes |f(r_q)\rangle\langle f(r_q)|\,, \quad (57)$$

and indistinguishability follows.

Next, we consider the case that f is a pseudorandom function. We show that a successful IND-CCA1 adversary $\mathcal{A}$ (i.e., one that distinguishes challenges with better than negligible probability) can be used to construct a successful f-adversary $\mathcal{A}_0$ (i.e., one that distinguishes f from random with non-negligible probability.) The adversary $\mathcal{A}_0$ is a QPT with classical oracle access to a function $\varphi : \{0,1\}^{2n} \to \{0,1\}^{2n}$, and aims to output 0 if φ is perfectly random and 1 if $\varphi = f_k$ for some k. Define the simulated oracles

$$\mathsf{Enc}_\varphi : \rho \mapsto \left(r,\, P_{\varphi(r)}\rho P_{\varphi(r)}\right) \text{ for } r \xleftarrow{\$} \{0,1\}^{2n}, \quad \text{and}$$

$$\mathsf{Dec}_\varphi : |r'\rangle\langle r'| \otimes \rho \mapsto P_{\varphi(r')}\rho P_{\varphi(r')}\,,$$

where, as before, we assume that Dec_φ measures the first register before decrypting the second. Note that if $\varphi = f_k$ then these are exactly the encryption and decryption oracles (with key k) of the qPRF-SKE scheme.

The QPT $\mathcal{A}_0^\varphi$ proceeds as follows. First, it simulates $\mathcal{A}$, and replies to its queries to the encryption oracle with Enc_φ and its queries to the decryption oracle with

Dec_φ. When it transmits the challenge, $\mathcal{A}_0^\varphi$ replies with either the encryption of the challenge, or the encryption of $|0^n\rangle\langle 0^n|$, each with probability $1/2$. If $\mathcal{A}$ responds correctly, $\mathcal{A}_0^\varphi$ outputs 1; otherwise it outputs 0. If $\varphi = f_k$ then we have exactly simulated the IND-CCA1 game with adversary $\mathcal{A}$; in that case, since $\mathcal{A}$ is IND-CCA1-breaking, $\mathcal{A}_0^\varphi$ outputs 1 with probability at least $1/2 + 1/t(n)$ for some polynomial t, for infinitely many n.

We conclude that

$$\left| \Pr_{k \xleftarrow{\$} \{0,1\}^n} [\mathcal{A}_0^{f_k}(1^n) = 1] \quad - \Pr_{\varphi \xleftarrow{\$} \{\{0,1\}^{2n} \to \{0,1\}^{2n}\}} [\mathcal{A}_0^{\varphi}(1^n) = 1] \right| \geq \frac{1}{t(n)} - \mathrm{negl}(n)\,, \quad (58)$$

for infinitely many n, i.e., f is not a qPRF. □

The proof of Theorem 1.2.2 thus follows from Theorem 4.3.3 and Lemma 4.3.4.

4.3.2 Quantum Public-Key Encryption from Trapdoor Permutations

For the construction of public-key schemes, we will need qOWFs with an additional property: the existence of *trapdoors* which enable efficient inversion. Following the classical approach of Diffie and Hellman [DH76], we set down the notion of a quantum-secure trapdoor one-way permutation (or qTOWP), and then show how to use any qTOWP to construct IND-CPA secure public-key encryption schemes for quantum data. This will establish Theorem 1.2.3: *If quantum-secure trapdoor one-way permutations exist, then so do semantically secure public-key quantum encryption schemes.* Some of the proofs that are omitted or only sketched here are done in detail in Chapter 5.

We begin with a definition of qTOWPs. We require a slight (but standard) variation of Definition 4.3.1, namely the notion of a quantum-secure one-way permutation (or qOWP). A qOWP is a qOWF whose input domains are sets D_i; moreover, the function restricted to any such domain must be a permutation. When we augment such a qOWP with trapdoors, with which it can be efficiently inverted, we arrive at the following definition.

Definition 4.3.5. A *quantum-secure trapdoor one-way permutation (qTOWP)* is a PT-computable collection

$$f = \{f_i : D_i \to D_i\}_{i \in I}$$

of permutations on sets $D_i \subseteq \{0,1\}^{l(i)}, i \in I$, for some (infinite) set I of strings, and a PT-computable function $l : \mathbb{N} \to \mathbb{N}$, together with a triple of PPTs $(\mathcal{G}, \mathcal{S}, \mathcal{I})$ which

1. (generate (index, trapdoor) pair) $\mathbf{supp}\, \mathcal{G}(1^n) \subseteq (I \cap \{0,1\}^n) \times \{0,1\}^n$;
2. (sample from domain) for all $i \in I$, $\mathbf{supp}\, \mathcal{S}(i) = D_i$;
3. (invert using trapdoor) for all $(i,t) \in \mathbf{supp}\, \mathcal{G}(1^n)$ and all $x \in D_i$, $\mathcal{I}(f_i(x), t) = x$,

such that for every QPT $\mathcal{A}$,

$$\Pr_{(i,t) \leftarrow \mathcal{G}(1^n), x \leftarrow S(i)} [\mathcal{A}(f_i(x), i) = x] \leq \mathrm{negl}(n)\,. \tag{59}$$

For simplicity, we will assume that $l(i) = |i| = n$.

Before we can describe the public-key scheme and prove its security, we need two additional (well-known) primitives which can be constructed from any qOWP, with or without trapdoors. The first is a quantum-secure "hard-core" predicate, which is a "yes" or "no" question about the uniformly random input x that is difficult to answer if one only knows $f(x)$.

Definition 4.3.6. A PT-computable $b : \{0,1\}^* \to \{0,1\}$ is a *(quantum-secure) hard-core* of a qOWP f if for every QPT $\mathcal{A}$,

$$\Pr_{x \xleftarrow{\$} \{0,1\}^n} [\mathcal{A}(f(x), 1^n) = b(x)] \leq \frac{1}{2} + \mathrm{negl}(n)\,. \tag{60}$$

The definition of hard-core may also be modified in the case of quantum-secure trapdoor one-way functions or permutations in the obvious way, by indexing f and b by i, generating $x \leftarrow S(i)$, where $(i,t) \leftarrow \mathcal{G}(1^n)$, and giving $\mathcal{A}$ access to i in place of 1^n.

Definition 4.3.7. A *hard-core* of a qTOWP $(f, \mathcal{G}, \mathcal{S}, \mathcal{I})$ is a PT-computable collection $b = \{b_i : D_i \to \{0,1\}\}_{i \in I}$ such that for every QPT $\mathcal{A}$,

$$\Pr_{(i,t) \leftarrow \mathcal{G}(1^n), x \leftarrow S(i)} [\mathcal{A}(f_i(x), i) = b_i(x)] \leq \frac{1}{2} + \mathrm{negl}(n)\,. \tag{61}$$

A Goldreich-Levin theorem for our setting implies the following[2]:

Theorem 4.3.8. *([AC02], quantum analogue of [GL89]) If qOWPs (or qTOWPs) exist, then qOWPs (or qTOWPs, respectively) with hard-cores exist.*

The other primitive we need is a quantum-secure pseudorandom generator, which expands a uniformly random seed to an output that is computationally indistinguishable from a longer uniformly random string, hence "pseudorandom". The classical proof that one-way permutations with hard-cores imply pseudorandom generators carries over with little modification (see Lemma 4.3.10).

Definition 4.3.9. A PT-computable function $G : \{0,1\}^* \to \{0,1\}^*$ is a *quantum-secure pseudorandom generator (qPRG)* if $|G(s)| = p(|s|)$ for all $s \in \{0,1\}^*$ and for every QPT $\mathcal{D}$,

$$\left| \Pr_{s \xleftarrow{\$} \{0,1\}^n} [\mathcal{D}(G(s)) = 1] \quad - \Pr_{y \xleftarrow{\$} \{0,1\}^{p(n)}} [\mathcal{D}(y) = 1] \right| \leq \mathrm{negl}(n)\,. \tag{62}$$

We write $m := p(n)$. Note that p must necessarily itself be PT-computable, and hence polynomially bounded.

Lemma 4.3.10. *If f is a qOWP with hard-core predicate b, and $p : \mathbb{N} \to \mathbb{N}$ is PT-computable, then $G : s \mapsto b(f^{p(|s|)-1}(s))b(f^{p(|s|)-2}(s)) \ldots b(s)$ is a qPRG.*

Sketch. [3] The proof proceeds almost identically as in the classical case (see, e.g., [Gol04].) Let $\mathcal{D}$ be a quantum adversary that distinguishes $G(U_n)$ from uniform. Note that, as stated in Definition 4.3.9, $\mathcal{D}$ gets only classical bitstring outputs from the pseudorandom generator. In the classical proof, one constructs an adversary $\mathcal{A}$ which uses $\mathcal{D}$ as a black-box subroutine, and breaks the hard-core of f. We use the exact same $\mathcal{A}$ now; in particular, we only need to invoke $\mathcal{D}$ on classical inputs and read out its (post-measurement) classical outputs (0 or 1). Of course, by virtue of needing to invoke $\mathcal{D}$, $\mathcal{A}$ itself will now be a QPT.

In slightly greater detail, we use a standard hybrid argument to give a "predictor" algorithm $\mathcal{A}$ that, for some index $i \leq m = p(n)$, can predict the $i+1^{\text{st}}$ bit of $G(U_n)$,

[2] It is proven in detail as Theorem 5.2.1 in Section 5.2.

[3] A more general result is proven in detail as Theorem 5.3.1 in Section 5.3.

given as input the first i bits of the output of G. $\mathcal{A}$ succeeds with non-negligible advantage over random, i.e., the probability over s that $\mathcal{A}(b(f^{m-1}(s))\dots b(f^{m-i}(s)))$ outputs $b(f^{m-(i+1)}(s))$ is at least $1/2+1/q(n)$ where q is some positive polynomial. Crucially, since f implements a permutation over $\{0,1\}^n$, we have that $b(f^{i-1}(U_n))\dots b(U_n)$ is distributed identically to $b(f^{m-1}(U_n))\dots b(f^{m-i}(U_n))$. Therefore, given uniform x, and $y = f(x)$, we can use the output of the predictor, $A(b(f^{i-1}(y))\dots b(y)) = A(b(f^i(x))\dots b(f(x)))$ to predict $b(x)$ with non-negligible advantage, in violation of the security guarantee of the hard-core predicate. □

We can now describe a public-key scheme for encrypting quantum data.

Scheme 2. If f is a qTOWP, and assume for simplicity that $l(i) = |i| = n$, and let b and $G : \{0,1\}^* \to \{0,1\}^*$ be the corresponding hard-core and qPRG, respectively with $p(n) = 2n$ as in Lemma 4.3.10 [4]. Let qTOWP-PKE be the following triple of algorithms:

1. ((public, private) key-pair generation) $\mathsf{KeyGen}(1^n)$:
   - output $\mathcal{G}(1^n) = (i,t) \in \{0,1\}^n \times \{0,1\}^n$;
2. (encryption with public key) $\mathsf{Enc}_i(\rho)$, for $\rho \in \mathfrak{D}(\mathbb{C}^{2^n})$, an n-qubit state:
   - apply $\mathcal{S}(i)$ to select $d \in D_i$, and compute $r := G(d) = b(f^{2n-1}(d))\dots b(d)$;
   - output $|f_i^{2n}(d)\rangle\langle f_i^{2n}(d)| \otimes P_r \rho P_r$;
3. (decryption with private key) $\mathsf{Dec}_t(\sigma)$, for $\sigma \in \mathfrak{D}(\mathbb{C}^{2^{2n}})$, a $2n$-qubit state:
   - measure the first n qubits in the computational basis to obtain $s \in \{0,1\}^n$
   - for $j = 1,\dots,2n$, apply $b \circ (\mathcal{I}_t)^j$ to s, where $\mathcal{I}_t := \mathcal{I}(\cdot,t)$; concatenate the resulting bits to get $u = b(f_i^{-1}(s))b(f_i^{-2}(s))\dots b(f_i^{-2n}(s)) \in \{0,1\}^{2n}$;
   - apply P_u to the remaining n qubits of σ and output the result.

The correctness of the scheme is straightforward; fix a key-pair (i,t), a randomly

[4] As with the qPRF in the private-key scheme, we can use $G = \{G_{n,m} : \{0,1\}^n \to \{0,1\}^{2m}\}_{n,m}$ to encrypt and decrypt messages of different lengths with the same keys, and this will remain secure, noting that messages must be polynomially bounded in length, so that m will be bounded above by the same polynomial

sampled $d \in D_i$, and the corresponding r. Then

$$\mathsf{Dec}_t(\mathsf{Enc}_i(\rho)) = \mathsf{Dec}_t\big(|f_i^{2n}(d)\rangle\langle f_i^{2n}(d)| \otimes P_r \rho P_r\big) = P_u P_r \rho P_r P_u = \rho\,, \tag{63}$$

where the last step follows from the fact that $u = r$ for valid ciphertexts: in this case, $s = f_i^{2n}(d)$, so

$$\begin{aligned} u &= b(f_i^{-1}(s)) \dots b(f_i^{-2n}(s)) \\ &= b(f_i^{-1}(f_i^{2n}(d))) \dots b(f_i^{-2n}(f_i^{2n}(d))) \\ &= b(f^{2n-1}(d)) \dots b(d) \\ &= G(d) \\ &= r\,. \end{aligned} \tag{64}$$

It remains to show that this scheme is secure against chosen plaintext attacks. We begin by proving indistinguishability of ciphertexts for the quantum one-time pad which uses randomness supplied by a qPRG. We first set the following notation. Recall from Subsection 3.8.1 that a string r of $2n$ bits determines a Pauli group element $P_r \in U(2^n)$. Given an n-qubit register A, an arbitrary register B, and $\rho \in \mathfrak{D}(\mathcal{H}_A \otimes H_B)$, define $\mathbb{P}_{r;A}(\rho) := (P_r \otimes \mathbb{1}_B)\rho(P_r \otimes \mathbb{1}_B)$.

Lemma 4.3.11. *If $G : \{0,1\}^* \to \{0,1\}^*$ is a qPRG, then for any efficiently preparable states $\rho_{AB} \in \mathfrak{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\sigma_A \in \mathfrak{D}(\mathcal{H}_A)$, and any QPT $\mathcal{D}$*

$$\left| \Pr_{s \xleftarrow{\$} \{0,1\}^n} \big[\mathcal{D}(\mathbb{P}_{G(s);A}(\rho_{AB})) = 1\big] - \Pr_{s \xleftarrow{\$} \{0,1\}^n} \big[\mathcal{D}(\mathbb{P}_{G(s);A}(\sigma_A \otimes \rho_B)) = 1\big] \right| \leq \mathrm{negl}(n)\,. \tag{65}$$

Proof. The two key observations are (i.) distinguishability as in Equation (65) is impossible if we replace $G(s)$ with uniform randomness, and (ii.) with only classical input/output access to G, we can simulate $\mathcal{D}(\mathbb{P}_{G(s);A}(\cdot))$. Putting these two facts together, it follows that violating (65) implies that outputs of G can be distinguished from uniformly random.

Formally, let us assume that there is an adversary $\mathcal{D}$ that violates our hypothesis, i.e., that distinguishes some pair of inputs $(\mathbb{P}_{G(s);A}(\rho_{AB}),\ \mathbb{P}_{G(s);A}(\sigma_A \otimes \rho_B))$ with probability at least $1/q(n)$ for some positive polynomial q. Then we'll show an algorithm

$\mathcal{D}'$, that breaks the pseudorandom generator G. On input $y \in \{0,1\}^m$, algorithm $\mathcal{D}'$ does the following:

- with probability 1/2, run $\mathcal{D}$ on input $\mathbb{P}_{y;A}(\rho_{AB})$;
- with probability 1/2, run $\mathcal{D}$ on input $\mathbb{P}_{y;A}(\sigma_A \otimes \rho_B)$.

Now if $\mathcal{D}$ is able to correctly determine which of the cases we gave it, $\mathcal{D}'$ decides that y must have been distributed pseudorandomly and outputs 1, else it decides that y is uniformly distributed and outputs 0.

Notice that if $y = G(s)$, by definition $\mathcal{D}'$ outputs 1 when $\mathcal{D}$ correctly distinguishes the two inputs, which occurs with probability at least $1/2 + 1/q(n)$ by the assumption on $\mathcal{D}$. On the other hand, suppose $y \xleftarrow{\$} \{0,1\}^m$; then after mixing over y, the register A is mapped to the maximally mixed state, i.e. $\frac{1}{2^m}\sum_y \mathbb{P}_{y;A}(\rho_{AB}) = \frac{1}{2^m}\sum_y \mathbb{P}_{y;A}(\sigma_A \otimes \rho_B) = \mathbb{1}_A \otimes \rho_B$. In that case, $\mathcal{D}$ is correct with probability at most 1/2 (indeed, this is true for any QPT.) We conclude that $\mathcal{D}'$ distinguishes the case $y = G(s)$ from the case $y \xleftarrow{\$} \{0,1\}^m$ with non-negligible probability; this contradicts the assumption that G is a qPRG. □

Finally, to prove that the construction in Scheme 2 is IND-CPA-secure, and thus establish Theorem 1.2.3, it remains to extend the above proof to a slightly more general scenario. Recall that $\mathsf{Enc}_i(\rho) = |f_i^{2n}(d)\rangle\langle f_i^{2n}(d)| \otimes P_r \rho P_r$ where $r = G(d)$. Lemma 4.3.11 already shows that essentially no QPT adversary can distinguish $(P_r \otimes \mathbb{1}_E)\rho_{ME}(P_r \otimes \mathbb{1}_E)$ from $(P_r \otimes \mathbb{1}_E)(|0\rangle\langle 0| \otimes \rho_E)(P_r \otimes \mathbb{1}_E)$, for any efficiently preparable bipartite state ρ_{ME} over the message space and the environment. It remains to show that this indistinguishability still holds if the adversary is also provided the classical advice i and $f_i^{2n}(d)$. We can prove this extended indistinguishability by extending the hybrid argument in the proof of Lemma 4.3.10 in a standard way. To sketch the argument, first recall that the "predictor" algorithm succeeds at predicting the $j+1^{\text{st}}$ bit of $G(U_n)$ given as input the first j bits of the output of G. Now we also allow the predictor to read the bits of i and $f_i^{2n}(d)$. Success implies breaking the hard-core of f (which is used to define the qPRG G and ensure its security). We

conclude that the strings

$$i\ f_i^{2n}(d)\ G(s) \quad \text{and} \quad i\ f_i^{2n}(d)\ r'$$

are computationally indistinguishable for uniformly random s, r', and $(i,t) \leftarrow \mathcal{G}(1^n)$.[5] Hence the states

$$|i\rangle\langle i| \otimes |f_i^{2n}(d)\rangle\langle f_i^{2n}(d)| \otimes \mathbb{P}_{G(s);M}(\rho_{ME}) \text{ and } |i\rangle\langle i| \otimes |f_i^{2n}(d)\rangle\langle f_i^{2n}(d)| \otimes \mathbb{P}_{r';M}(\rho_{ME})$$

must also be computationally indistinguishable, since they are obtained by the application of a quantum algorithm to the previous pairs of strings, respectively, where $\rho_{ME} \leftarrow \mathcal{M}(i)$ (i is copied, and $\mathcal{M}$ is applied to one of the copies; then the quantum one-time pad is applied to the result with $G(s)$ or r', respectively). The right-hand side is indistinguishable from the same state with $|0\rangle\langle 0|_M \otimes \rho_E$ in place of ρ_{ME}, by observing that their mixtures over r' are identical, so we also have the computational indistinguishability of

$$\begin{aligned} &|i\rangle\langle i| \otimes |f_i^{2n}(d)\rangle\langle f_i^{2n}(d)| \otimes \mathbb{P}_{r';M}(\rho_{ME}) \qquad \text{and} \\ &|i\rangle\langle i| \otimes |f_i^{2n}(d)\rangle\langle f_i^{2n}(d)| \otimes \mathbb{P}_{r';M}(|0\rangle\langle 0|_M \otimes \rho_E)\,. \end{aligned}$$

By the transitivity of computational indistinguishability, we conclude that

$$\begin{aligned} &|i\rangle\langle i| \otimes |f_i^{2n}(d)\rangle\langle f_i^{2n}(d)| \otimes \mathbb{P}_{G(s);M}(\rho_{ME}) \qquad \text{and} \\ &|i\rangle\langle i| \otimes |f_i^{2n}(d)\rangle\langle f_i^{2n}(d)| \otimes \mathbb{P}_{G(s);M}(|0\rangle\langle 0|_M \otimes \rho_E) \end{aligned}$$

are indistinguishable, which completes the proof of Theorem 1.2.3. □

4.4 Alternative Definitions of Quantum Security

Here, we present further definitions of quantum semantic security and indistinguishability, and prove their equivalence. The full chain of equivalences is given in Figure 4.

SEM3 (Definition 4.4.5) helps to illustrate that quantum semantic security as defined in this thesis is a proper quantum analogue of classical semantic security, while

[5] This is proven in detail as Theorem 5.3.1 in Section 5.3.

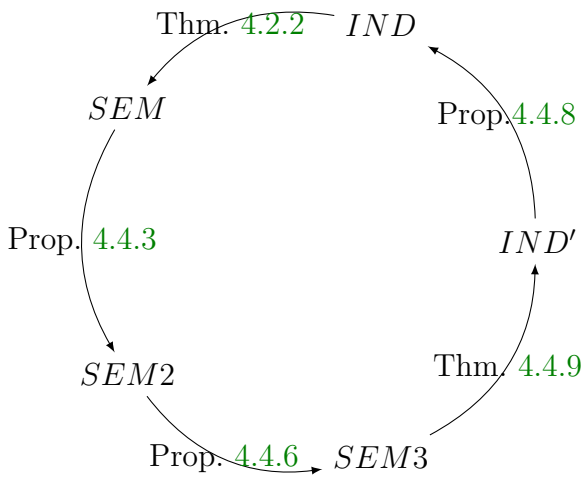

Figure 4: Relationship between security definitions.

SEM2 (Definition 4.4.2) serves primarily as an intermediate between SEM (Definition 4.2.1) and SEM3. IND' (Definition 4.4.7) is the quantum version of a common reformulation of IND (Definition 4.1.3), which is essentially used in the proof of Theorem 4.2.3 SEM $\implies$ IND.

4.4.1 SEM2

Definition 4.4.1 (Message-classical function generator)**.** A *message-classical function generator* $\mathcal{M}$ is a QPT message generator (as in SEM (Definition 4.2.1)) such that for each $pk \in \mathcal{K}_{pub}$ and ρ_{MEF} in the range of $\mathcal{M}(pk)$, there is some binary string y such that $|y\rangle \in \mathcal{H}_F$ and $\rho_{MEF} = \rho_{ME} \otimes |y\rangle\langle y|$.

That is, the F system is classical, unentangled from and uncorrelated with the rest of ρ.

In particular, $\rho_F = |y\rangle\langle y|$.

Definition 4.4.2 (SEM2)**.** A qPKE scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is *SEM2-secure* if for any QPT adversary $\mathcal{A}$, there exists a QPT simulator $\mathcal{S}$ such that for all message-classical function generators $\mathcal{M}$,

$$\left|\Pr\left[\,\mathcal{A}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho_{ME} = y\,\right] - \Pr\left[\,\mathcal{S}\rho_E = y\,\right]\right| \leq \mathrm{negl}(n)\,, \tag{66}$$

where the outputs of $\mathcal{A}$ and $\mathcal{S}$ are measured in the computational basis before equality is checked, $\rho_{ME} \otimes |y\rangle\langle y|_F \leftarrow \mathcal{M}(pk)$, and the probabilities are taken over $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$ and the internal randomness of Enc, $\mathcal{A}, \mathcal{S}, \mathcal{M}$ and $\mathcal{D}$.

- ***SEM2-CPA:*** In addition to the above, all QPTs have oracle access to Enc_{pk}.
- ***SEM2-CCA1:*** In addition to SEM2-CPA, $\mathcal{M}$ has oracle access to Dec_{sk}.

Proposition 4.4.3. *If a quantum encryption scheme is semantically secure, then it is SEM2 secure.*

Proof. A message-classical function generator is also a message. In SEM, have the distinguisher $\mathcal{D}$ implement an equality test (simulate any efficient classical circuit implementing it; if the input lengths aren't the same, output 0 immediately). □

4.4.2 SEM3

Definition 4.4.4 (Message Generator-Function Pair)**.** A *message generator-function pair* is a tuple $(\mathcal{M}, f)$, such that $\mathcal{M}$ is a QPT message generator (as in IND (Definition 4.1.3)) and $f = (f_n)_n$ is a QPT algorithm, such that $f_{pk} := f_n(pk)$ is the description of a boolean circuit, for $pk \in \mathcal{K}_{pub}$, with the number of input bits to f_{pk} equal to the number of measurement gates in the quantum circuit $\mathcal{M}_n$. In the symmetric-key scenario, f_n has no input.

Definition 4.4.5 (SEM3)**.** A qPKE scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is *SEM3-secure* if for any QPT adversary $\mathcal{A}$, there exists a QPT simulator $\mathcal{S}$ such that for all message generator-function pairs $(\mathcal{M}, f)$,

$$\left|\Pr\left[\ \mathcal{A}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho_{ME} = f_{pk}(x)\ \right] - \Pr\left[\ \mathcal{S}\rho_E = f_{pk}(x)\ \right]\right| \leq \mathrm{negl}(n)\,, \tag{67}$$

where the outputs of $\mathcal{A}$ and $\mathcal{S}$ are measured in the computational basis before equality is checked, $\rho_{ME} \leftarrow \mathcal{M}(pk)$, x is the string of measurement results generating ρ_{ME}, and the probabilities are taken over $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$ and the internal randomness of Enc, $\mathcal{A}, \mathcal{M}$ and $\mathcal{S}$.

- ***SEM3-CPA:*** In addition to the above, all QPTs have oracle access to Enc_{pk}.

- ***SEM3-CCA1:*** In addition to SEM3-CPA, $\mathcal{M}$ has oracle access to Dec_{sk}.

We note that f_{pk} is a function of the random input and measurement results, which completely determine the state. Hence, if f_{pk} is the identity for all pk, and it can be computed given a ciphertext, this means we can compute measurement results necessary to prepare the state. Simulating the message generator but selecting for the correct measurement results would allow the preparation of the same state again, although this is not in general efficient.

Proposition 4.4.6 (SEM2 $\implies$ SEM3)**.** *If a quantum encryption scheme is SEM2 secure, then it is SEM3 secure.*

Proof. A message generator-function pair $(\mathcal{M}, f)$ can be turned into a message-classical function generator $\mathcal{M}$ by copying the measurement results $x_1, x_2, \ldots, x_m$ after each measurement gate, and applying f_{pk} to $x_1 x_2 \ldots x_m$ and letting the result be the F system. □

4.4.3 IND'

Definition 4.4.7 (IND')**.** A qPKE scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is *IND' secure* if for every QPT adversary $\mathcal{A} = (\mathcal{M}, \mathcal{D})$ we have:

$$\Pr\left[\, \mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho_{ME}^{(b)} = b\right] \leq \tfrac{1}{2} + \mathrm{negl}(n)\,, \tag{68}$$

where $\rho_{ME} \leftarrow \mathcal{M}(pk)$, for b a uniformly random bit, $\rho_{ME}^{(1)} = \rho_{ME}$ and $\rho_{ME}^{(0)} = |0\rangle\langle 0|_M \otimes \rho_E$, and the probabilities are taken over $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$, b and the internal randomness of Enc, $\mathcal{M}$, and $\mathcal{D}$.

- ***IND'-CPA:*** In addition to the above, $\mathcal{M}$ and $\mathcal{D}$ have oracle access to Enc_{pk}.
- ***IND'-CCA1:*** In addition to IND'-CPA, $\mathcal{M}$ has oracle access to Dec_{sk}.

Proposition 4.4.8 (IND' $\iff$ IND)**.** *A quantum encryption scheme is IND' secure if and only if it is IND secure.*

Proof. We drop the register subscripts where possible.

$$\begin{aligned}
&\Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho^{(b)} = b] \\
&= \Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho^{(b)} = b \mid b = 1] \Pr[b = 1] \\
&\quad + \Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho^{(b)} = b \mid b = 0] \Pr[b = 0] \\
&= \tfrac{1}{2}(\Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho = 1] + \Pr[\mathcal{D}(\mathsf{Enc}_{pk} |0\rangle \langle 0| \otimes \rho_E) = 0]) \\
&\leq \tfrac{1}{2}(\Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho = 1] + 1 - \Pr[\mathcal{D}(\mathsf{Enc}_{pk} |0\rangle \langle 0| \otimes \rho_E) = 1]) \\
&= \tfrac{1}{2} + \tfrac{1}{2}(\Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho = 1] - \Pr[\mathcal{D}(\mathsf{Enc}_{pk} |0\rangle \langle 0| \otimes \rho_E) = 1]) . \qquad (69)
\end{aligned}$$

Note that we only get $\leq$ since $\mathcal{D}$ may output some binary string other than 0 or 1. So:

$$\begin{aligned}
&\Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho^{(b)} = b] - \tfrac{1}{2} \\
&\leq \tfrac{1}{2} |\Pr[\mathcal{D}((\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho = 1] - \Pr[\mathcal{D}(\mathsf{Enc}_{pk} |0\rangle \langle 0| \otimes \rho_E) = 1]| . \qquad (70)
\end{aligned}$$

Thus, IND $\implies$ IND'.

Now consider replacing $\mathcal{D}$ with the distinguisher which starts the same as $\mathcal{D}$, but if $\mathcal{D}$ would have output something other than 0 or 1, it simply outputs 0. Then the quantity $|\Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho = 1] - \Pr[\mathcal{D}(\mathsf{Enc}_{pk} |0\rangle \langle 0| \otimes \rho_E) = 1]|$ is the same for this new distinguisher, so without loss of generality, $\mathcal{D}$ only outputs 0 or 1.

Then the first $\leq$ becomes an $=$, i.e.

$$\begin{aligned}
&\Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho^{(b)} = b] - \tfrac{1}{2} \\
&= \tfrac{1}{2}(\Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho = 1] - \Pr[\mathcal{D}(\mathsf{Enc}_{pk} |0\rangle \langle 0| \otimes \rho_E) = 1]) \qquad (71)
\end{aligned}$$

and, similarly,

$$\begin{aligned}
&\Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho^{(b)} = b \oplus 1] \\
&= \Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho^{(b)} = b \oplus 1 \mid b = 1] \Pr[b = 1] \\
&\quad + \Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho^{(b)} = b \oplus 1 \mid b = 0] \Pr[b = 0] \\
&= \tfrac{1}{2}(\Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho = 0] + \Pr[\mathcal{D}(\mathsf{Enc}_{pk} |0\rangle \langle 0| \otimes \rho_E) = 1]) \\
&= \tfrac{1}{2}(1 - \Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho = 1] + \Pr[\mathcal{D}(\mathsf{Enc}_{pk} |0\rangle \langle 0| \otimes \rho_E) = 1]) \\
&= \tfrac{1}{2} + \tfrac{1}{2}(\Pr[\mathcal{D}(\mathsf{Enc}_{pk} |0\rangle \langle 0| \otimes \rho_E) = 1] - \Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho = 1]) , \qquad (72)
\end{aligned}$$

so,

$$\begin{aligned}&\Pr[\mathcal{D}(\mathsf{Enc}_{pk}\otimes \mathbb{1}_E)\rho^{(b)}=b\oplus 1]-\tfrac{1}{2}\\&=\tfrac{1}{2}(\Pr[\mathcal{D}(\mathsf{Enc}_{pk}\left|0\right\rangle\left\langle 0\right|\otimes\rho_E)=1]-\Pr[\mathcal{D}(\mathsf{Enc}_{pk}\otimes\mathbb{1}_E)\rho=1])\,.\end{aligned}\tag{73}$$

Combining the above,

$$\begin{aligned}&\tfrac{1}{2}|\Pr[\mathcal{D}(\mathsf{Enc}_{pk}\otimes\mathbb{1}_E)\rho=1]-\Pr[\mathcal{D}(\mathsf{Enc}_{pk}\left|0\right\rangle\left\langle 0\right|\otimes\rho_E)=1]|\\&=\max\{\Pr[\mathcal{D}(\mathsf{Enc}_{pk}\otimes\mathbb{1}_E)\rho^{(b)}=b]-\tfrac{1}{2},\Pr[\mathcal{D}(\mathsf{Enc}_{pk}\otimes\mathbb{1}_E)\rho^{(b)}=b\oplus 1]-\tfrac{1}{2}\}\,.\end{aligned}\tag{74}$$

Hence IND' $\implies$ IND by applying IND to both $\mathcal{D}$ and $\mathcal{D}\oplus 1$ (the latter outputs the answer opposite to $\mathcal{D}$), for $\Pr[\mathcal{D}(\mathsf{Enc}_{pk}\otimes\mathbb{1}_E)\rho^{(b)}=b]$ and $\Pr[\mathcal{D}(\mathsf{Enc}_{pk}\otimes\mathbb{1}_E)\rho^{(b)}=b\oplus 1]$, respectively. The maximum of two negligible functions is again negligible. □

Theorem 4.4.9 (SEM3 $\implies$ IND')**.** *If a quantum encryption scheme is SEM3 secure, then it is IND' secure.*

Proof. Let $(\mathcal{M},\mathcal{D})$ be an IND' adversary.

Let us consider the SEM3 message generator $\mathcal{M}'$ which runs $\rho_{ME}\leftarrow\mathcal{M}$ and outputs (with probability $\frac{1}{2}$ each) either the state ρ_{ME} or the state $\left|0\right\rangle\left\langle 0\right|_M\otimes\rho_E$, and we denote its output by ρ'_{ME}. In particular, it prepares a random bit b to do so by measuring a ancilary qubit to which the Hadamard was applied.

Define $f_{pk}(xb)=b$.

Define the SEM3 adversary $\mathcal{A}:=\mathcal{D}$.

In this way, the SEM3 game simulates the indistinguishability game, and

$$\Pr[\mathcal{A}(\mathsf{Enc}_{pk}\otimes\mathbb{1}_E)\rho'_{ME}=f_{pk}(xb)]=\Pr[\mathcal{D}(\mathsf{Enc}_{pk}\otimes\mathbb{1}_E)\rho^{(b)}=b]\,.\tag{75}$$

Now, by SEM3, there is some simulator $\mathcal{S}$ for $\mathcal{A}$ so that

$$|\Pr[\mathcal{A}(\mathsf{Enc}_{pk}\otimes\mathbb{1}_E)\rho'_{ME}=f_{pk}(xb)]-\Pr[\mathcal{S}\rho'_E=f_{pk}(xb)]|\leq\mathrm{negl}(n)\,,\tag{76}$$

i.e.

$$|\Pr[\mathcal{D}(\mathsf{Enc}_{pk}\otimes\mathbb{1}_E)\rho^{(b)}=b]-\Pr[\mathcal{S}\rho'_E=b]|\leq\mathrm{negl}(n)\,.\tag{77}$$

Note that $\mathcal{S}$'s input ρ'_E is independent of b. Hence

$$\Pr[\mathcal{S}\rho'_E = b] \leq \tfrac{1}{2}\,. \tag{78}$$

Finally, by summing the last two inequalities and dropping the absolute values,

$$\Pr[\mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho^{(b)} = b] \leq \tfrac{1}{2} + \mathrm{negl}(n)\,. \tag{79}$$

□

Chapter 5

Proofs for Cryptographic Primitives

Results that were sketched or omitted in Section 4.3 are reviewed here. Classical results, whose extensions to our setting may be used to prove Theorem 4.3.3, are mentioned in Section 5.1. This theorem was used for the construction of the private-key quantum encryption scheme in Section 4.3.1.

The remaining results in this chapter are used in the construction of the public-key quantum encryption scheme in Section 4.3.2, based on their classical counterparts as found in [Gol06]. They are the quantum analogues of the Goldreich-Levin theorem for trapdoor one-way permutations (Theorem 4.3.8 in Section 4.3.2, and Theorem 5.2.1 here in Section 5.2) and an extended proof of security for the construction of quantum-secure pseudorandom generators from quantum-secure trapdoor one-way permutations with hard-cores (Lemma 4.3.10 in Section 4.3.2, and Theorem 5.3.1 here in Section 5.3).

5.1 qOWFs to qPRFs

For the construction of the private-key quantum encryption scheme in Section 4.3.1, the following result is used:

Theorem 5.1.1 (qOWF to qPRF)**.** *If quantum-secure one way functions exist, then*

quantum-secure pseudorandom functions exist.

In the classical literature, the above was proven as a consequence of the two following results:

Theorem 5.1.2 (qOWF to qPRG)**.** *If quantum-secure one-way functions exist, then quantum-secure pseudorandom generators exist.*

Theorem 5.1.3 (qPRG to qPRF)**.** *If quantum-secure pseudorandom generators exist, then quantum-secure pseudorandom functions exist.*

The adaptation to the quantum case of the (long) proofs for the two results above is straightforward: it suffices to simply replace all occurrences of classical adversaries/distinguishers with quantum ones. See [HILL99] and [GGM86], respectively. The proofs are therefore omitted.

5.2 The Goldreich-Levin Theorem

Theorem 4.3.8 is proven for quantum-secure trapdoor one-way permutations. The proof is rather technical.

Adcock and Cleve [AC02] give a more efficient reduction in the quantum setting from an adversary beaking the hard-core to an adversary breaking the one-way function than the original one by Goldreich and Levin in [GL89].

Theorem 5.2.1 (The Goldreich-Levin Theorem for qTOWPs [Gol06])**.** *If $(f, \mathcal{G}, \mathcal{S}, \mathcal{I})$ is a quantum-secure trapdoor one-way permutation, define*

- *g by $g_i(xr) = f_i(x)r$ where $|r| = |f_i(x)|$;*
- *$\mathcal{S}'$ by $xr \leftarrow \mathcal{S}'(i)$, where $x \leftarrow \mathcal{S}(i)$ and $r \xleftarrow{\$} \{0,1\}^{|f_i(x)|}$;*
- *$\mathcal{I}'$ by $\mathcal{I}'(yr, t) = \mathcal{I}(y, t)r$ (where $|y| = |r|$); and*
- *$b_i(xr) = x \odot r = \bigoplus_{j=1}^{|x|} x_j \cdot r_j$, the dot product of x and r, mod 2 (where $|x| = |r|$).*

Then $(g, \mathcal{G}, \mathcal{S}', \mathcal{I}')$ is a quantum-secure trapdoor one-way permutation with hard-core predicate b_i.

Note that b_i does not depend on i.

Proof. We follow the proof of Theorem 2.5.2 in [Gol06]. First, note that $(g, \mathcal{G}, \mathcal{S}', \mathcal{I}')$ is a trapdoor one-way permutation, since
$\mathcal{I}'(g_i(xr), t) = \mathcal{I}'(f_i(x)r, t) = \mathcal{I}(f_i(x), t)r = xr$. It is quantum-secure, since an algorithm capable of guessing xr from $(g_i(xr), i) = (f_i(x)r, i)$ with non-negligible probability can be used as a subroutine in an algorithm to guess x from $(f_i(x), i)$, by simply generating a random string r of length $|f_i(x)|$ and applying the first algorithm to $(f_i(x)r, i)$.

For one-way functions, an algorithm guessing $y \in g^{-1}(g(x))$ can be used similarly.

Now, we prove by way of contradiction that b_i is a hard-core. Suppose that is isn't, i.e. there exists a quantum algorithm $\mathcal{A}$ and a positive polynomial p such that $\epsilon(n) := \Pr[\mathcal{A}(g_i(xr), i) = b_i(xr)] - \frac{1}{2} > \dfrac{1}{p(n)}$ for infinitely many n, where

$(i,t) \leftarrow \mathcal{G}(1^n), x \leftarrow \mathcal{S}(i)$. We define an algorithm $\mathcal{A}'$ to break the one-way permutation, i.e. such that $\Pr[\mathcal{A}'(f_i(x), i) = x]$ is not negligible:

$\underline{\mathcal{A}'(y,i)}$ $(y = f_i(x))$ (80)

$l := \lceil \log_2(2|y|p(n)^2 + 1) \rceil$

where $p(n)$ is such that $\epsilon(n) > \dfrac{1}{p(n)}$ for infinitely many n,

and without loss of generality, all algorithms receive 1^n or 1^n can be computed from i

for $j = 1, \ldots, l$,

$s^j \xleftarrow{\$} \{0,1\}^{|y|}$

$\sigma^j \xleftarrow{\$} \{0,1\}$

for every nonempty $J \subseteq \{1, 2, \ldots, l\}$

$r^J := \bigoplus_{j \in K} s^j \ (\in \{0,1\}^{|y|})$

$\rho^J := \bigoplus_{j \in K} \sigma^j \ (\in \{0,1\})$

for every $k \in \{1, \ldots, |y|\}$ *and every nonempty* $J \ \subseteq \{1, \ldots, l\}$,

$z_k^J \leftarrow \rho^J \oplus A(y, r^J \oplus e^k)$

for every $k \in \{1, \ldots, |y|\}$,

$z_k :=$ *the majority value of the* $(z_k^J)_J$

output $z := z_1 \ldots z_{|y|}$

Two lemmas are used to prove that $\mathcal{A}'$ breaks f. First, $\mathcal{A}$ must guess b_i with nonnegligible advantage on a set S_n of pairs (x,i), where $x \in D_i$, of nonnegligible probability:

Lemma 5.2.2. *There exists a set* $S_n \subseteq \bigcup_{i:(i,t) \in \mathbf{supp}\, \mathcal{G}(1^n)} D_i \times \{i\}$ *of probability at least* $\frac{\epsilon(n)}{2}$*, such that for all* $(x,i) \in S_n$*,*

$$s(x,i) := \Pr[\mathcal{A}(g_i(xr), i) = b_i(xr)] \geq \frac{1}{2} + \frac{\epsilon(n)}{2}\,, \tag{81}$$

taken over $r \xleftarrow{\$} \{0,1\}^{|f_i(x)|}$*. (Claim 2.5.2.1 from [Gol06])*

Proof. Let S_n be the set of all such (x,i), i.e $S_n = \{(x,i)|s(x,i) \geq \frac{1}{2} + \frac{\epsilon(n)}{2}\}$, and let $a = \frac{1}{2} + \frac{\epsilon(n)}{2}$. Note that $\mathbb{E}(s(x,i)) = \frac{1}{2} + \epsilon(n)$. If $\Pr[(x,i) \in S_n] < \frac{\epsilon(n)}{2}$, then

$$\begin{aligned}
\frac{1}{2} + \epsilon(n) &= \mathbb{E}[s(x,i)] \\
&= \sum_x s(x,i)p(x,i) \\
&\quad \text{where } p(x,i) \text{ is the joint probability of } x \text{ and } i \\
&= \sum_{(x,i):s(x,i)<a} s(x,i)p(x,i) + \sum_{(x,i):s(x,i)\geq a} s(x,i)p(x,i) \\
&\leq \sum_{(x,i):s(x,i)<a} ap(x,i) + \sum_{(x,i):s(x,i)\geq a} 1p(x,i) \qquad \text{since } s \leq 1 \\
&= a\Pr[s(x,i) < a] + \Pr[s(x,i) \geq a] \\
&= a(1 - \Pr[s(x,i) \geq a]) + \Pr[s(x,i) \geq a] \\
&= (1-a)\Pr[s(x,i) \geq a] + a \\
&= \left(\frac{1}{2} - \frac{\epsilon(n)}{2}\right)\Pr[s(x,i) \geq a] + \frac{1}{2} + \frac{\epsilon(n)}{2} \\
\iff \frac{\epsilon(n)}{2} &\leq \left(\frac{1}{2} - \frac{\epsilon(n)}{2}\right)\Pr[s(x,i) \geq a]
\end{aligned}$$

$$\implies \Pr[s(x,i) \geq a] \geq \frac{\frac{\epsilon(n)}{2}}{\frac{1}{2} - \frac{\epsilon(n)}{2}} = \frac{\epsilon(n)}{1-\epsilon(n)} > \epsilon(n)\,, \quad \text{if } 0 < \epsilon(n) < 1, \tag{82}$$

and if this last implication doesn't hold, either $\epsilon(n) = 0$ or $\epsilon(n) = 1$, and we just let $S_n = \bigcup_{i:(i,t)\in \mathit{supp}\,\mathcal{G}(1^n)} D_i \times \{i\}$. This completes the proof of the lemma. □

Now we prove a lemma regarding the behaviour of $\mathcal{A}$ for $(x,i) \in S_n$:

Lemma 5.2.3. *For all $(x,i) \in S_n$ and for all $1 \leq k \leq |f_i(x)|$,*

$$\Pr[|\{J|b_i(x,r^J) \oplus \mathcal{A}(f_i(x), r^J \oplus e^k) = x_k\}| > \tfrac{1}{2}(2^l - 1)] > 1 - \frac{1}{2|f_i(x)|}\,, \tag{83}$$

for infinitely many n, where x_k is the kth character of the string x, $e^k := 0^{k-1}10^{|f_i(x)|-k}$ is the string of the length $|f_i(x)|$ with 1 in its kth position and 0 in all others, and r^J and l are defined and distributed as above in the definition of A'. (Claim 2.5.2.2 from [Gol06])

Proof. For each nonempty $J \subseteq \{1, \ldots, l\}$, let

$$\xi^J = \begin{cases} 1, & \text{if } b_i(x, r^J) \oplus \mathcal{A}(f_i(x), r^J \oplus e^k) = x_k \\ 0, & \text{otherwise,} \end{cases} \tag{84}$$

and let $m = 2^l - 1$, the number of nonempty subsets of $\{1, \ldots, l\}$.

Note that this condition for $\xi^J = 1$ is equivalent to $\mathcal{A}(f_i(x), r^J \oplus e^k) = b_i(x, r^J \oplus e^k)$, since

$$b_i(x, r^J) \oplus b_i(x, r^J \oplus e^k) = b_i(x, e^k) = x_k \,. \tag{85}$$

Then, since the r_J and hence the $r^J \oplus e^k$ are uniformly distributed in $\{0,1\}^{|f_i(x)|}$,

$$\Pr[\xi^J = 1] = \Pr[\mathcal{A}(f_i(x), r^J \oplus e^k) = b_i(x, r^J \oplus e^k)] = s(x, i) \geq \frac{1}{2} + \frac{1}{2p(n)} \,, \tag{86}$$

for infinitely many n.

Furthermore,

$$|\{J | b_i(x, r^J) \oplus \mathcal{A}(f_i(x), r^J \oplus e^k) = x_k\}| = \sum_J \xi^J \,. \tag{87}$$

Recall *Chebyshev's inequality*:

Lemma 5.2.4 (Chebyshev's inequality)**.** *For X a random variable with finite mean μ and variance σ^2, and $c > 0$,*

$$\Pr[|X - \mu| \geq c] \leq \frac{\sigma^2}{c^2} \,. \tag{88}$$

We would like to apply it to $X = \sum_J \xi^J$ with $c = \frac{m}{2p(n)}$, and to do so, we need the variance of $\sum_J \xi^J$. Note that the ξ^J are all identically distributed, since the r^J are. Then, if the ξ^J are pairwise independent, it follows that $\mathrm{Var}[\sum_J \xi^J] = m\mathrm{Var}[\xi]$, where ξ is any of the ξ^J and $m = 2^l - 1$, the number of J's. To prove that the ξ^J are pairwise independent, it suffices to show that the r^J are, since the ξ^J differ only through their dependence on the corresponding r^J (i.e. $\xi^J = F(r^J, w^J)$, where F is a deterministic function and w^J is a random variable for the independent random coin tosses in the use of A for each J). Let $J \neq J'$ be two nonempty subsets of $\{1, \ldots, l\}$.

Then, without loss of generality, $J' \not\subseteq J$, so that there exists $j'_0 \in J' \setminus J$ and $j_0 \in J$. Then, for all $\alpha, \beta \in \{0,1\}^{|f_i(x)|}$,

$$\begin{aligned}
\Pr[r^{J'} = \beta | r^J = \alpha] &= \Pr\left[\Big(\bigoplus_{j' \in J', j' \neq j'_0} s^{j'}\Big) \oplus s^{j'_0} = \beta \,\Big|\, \Big(\bigoplus_{j \in J, j \neq j_0} s^{j}\Big) \oplus s^{j_0} = \alpha\right] \\
&= \Pr\left[s^{j'_0} = \Big(\bigoplus_{j' \in J', j' \neq j'_0} s^{j'}\Big) \oplus \beta \,\Big|\, s^{j_0} = \Big(\bigoplus_{j \in J, j \neq j_0} s^{j}\Big) \oplus \alpha\right] \\
&= \Pr\left[s^{j'_0} = \Big(\bigoplus_{j' \in J', j' \neq j'_0} s^{j'}\Big) \oplus \beta\right] \\
&\quad \text{since } s^{j'_0} \text{ and } s^{j_0} \text{ are independent} \\
&= \Pr[r^{J'} = \beta]\,. \qquad (89)
\end{aligned}$$

Hence the ξ^J are pairwise independent.

Then

$$\begin{aligned}
\mu = \mathbb{E}[\sum_J \xi^J] = \sum_J \mathbb{E}[\xi^J] = \sum_J \Pr[\xi^J = 1] = \sum_J \Pr[\mathcal{A}(f_i(x), r^J \oplus e^k) = b_i(x, r^J \oplus e^k)] \\
= \sum_J \Pr[\mathcal{A}(g_i(xr), i) = b_i(xr)] = ms(x,i) \qquad (90)
\end{aligned}$$

(so $\mathbb{E}[\xi^J] = s(x,i)$).

Now,

$$\begin{aligned}
\sum_J \xi^J \leq \frac{m}{2} &\iff \sum_J \xi^J - \frac{m}{2} \leq 0 \\
&\iff \sum_J \xi^J - \frac{m}{2} - \frac{m}{2p(n)} \leq -\frac{m}{2p(n)} \\
&\implies \sum_J \xi^J - ms(x,i) \leq -\frac{m}{2p(n)} \text{ (for infinitely many } n) \\
&\iff |\sum_J \xi^J - ms(x,i)| \geq \frac{m}{2p(n)} \text{ (for infinitely many } n). \qquad (91)
\end{aligned}$$

So,

$$
\begin{aligned}
&1 - \Pr\left[|\{J|b_i(x, r^J) \oplus \mathcal{A}(f_i(x), r^J \oplus e^k) = x_k\}| > \tfrac{1}{2}(2^l - 1)\right] \\
&= \Pr\left[\sum_J \xi^J \leq \frac{m}{2}\right] \\
&\leq \Pr\left[\left|\sum_J \xi^J - ms(x,i)\right| \geq \frac{m}{2p(n)}\right] \text{ (for infinitely many } n) \\
&\leq \frac{\mathrm{Var}\left[\sum_J \xi^J\right]}{\left(\frac{m}{2p(n)}\right)^2} \text{ (by Chebyshev's inequality)} \\
&= \frac{m\mathrm{Var}[\xi]}{\left(\frac{m}{2p(n)}\right)^2} \text{ (by pairwise independence of the } \xi^J) \\
&= \frac{\mathrm{Var}[\xi]}{\left(\frac{1}{2p(n)}\right)^2 m} \\
&\leq \frac{\mathrm{Var}[\xi]}{\left(\frac{1}{2p(n)}\right)^2 2|f_i(x)|p(n)^2} \text{(since } m = 2^l - 1 \text{ and } l = \lceil \log_2(2|f_i(x)|p(n)^2 + 1)\rceil) \\
&= \frac{2\mathrm{Var}[\xi]}{|f_i(x)|} \\
&< \frac{1}{2|f_i(x)|}\,,
\end{aligned}
\tag{92}
$$

where the last inequality follows if $\mathrm{Var}[\xi] \leq \frac{1}{4}$. Indeed,

$$\begin{aligned}
\mathrm{Var}[\xi] &= \mathbb{E}[\xi^2] - \mathbb{E}[\xi]^2 \\
&= \mathbb{E}[\xi] - \mathbb{E}[\xi]^2 \text{ (since } \xi \text{ is binary)} \\
&= s(x,i) - s(x,i)^2 \\
&= s(x,i)(1 - s(x,i)) \\
&\leq \left(\frac{1}{2} + \frac{1}{2p(n)}\right)\left(1 - \left(\frac{1}{2} + \frac{1}{2p(n)}\right)\right) \text{ for infinitely many } n, \\
&\quad \text{since } f(x) = x(1-x) = x - x^2 \text{ is strictly decreasing for } x > \frac{1}{2} \\
&= \left(\frac{1}{2} + \frac{1}{2p(n)}\right)\left(\frac{1}{2} - \frac{1}{2p(n)}\right) \\
&= \frac{1}{4} - \frac{1}{4p(n)^2} \\
&< \frac{1}{4}\,. \qquad (93)
\end{aligned}$$

This proves the lemma. □

We finally return to the proof of the main theorem. The goal is to show that $\Pr[\mathcal{A}'(f_i(x), i) = x]$ is not negligible, and we do so by first restricting ourselves to fixed $(x, i) \in S_n$.

Let us consider the case where $\sigma^j = b_i(x, s^j)$ for all $j \in \{1, \ldots l\}$. Note that this implies $\rho^J = \bigoplus_{j \in J} \sigma^j = \bigoplus_{j \in J} b_i(x, s^j) = b_i(x, \bigoplus_{j \in J} s^j) = b_i(x, r^J)$. So, subscripting the ξ^J with k, as ξ^J_k, given $\sigma^j = b_i(x, s^j)$ for all j,

$$\begin{aligned}
\mathcal{A}'(f_i(x), i) = x &\iff z = x \\
&\iff z_k = x_k, \text{ for all } k \\
&\iff z^J_k = x_k \text{ for at least half of the } J, \text{ i.e. at least } \frac{2^l - 1}{2} \ J\text{'s, for all } k \\
&\iff |\{J | b_i(x, r^J) \oplus \mathcal{A}(f_i(x), r^J \oplus e^k) = x_k\}| > \tfrac{1}{2}(2^l - 1), \text{ for all } k, \qquad (94)
\end{aligned}$$

since $\rho^J = b_i(x, r^J)$, so $z^J_k = \rho^J \oplus \mathcal{A}(f_i(x), r^J \oplus e^k) = b_i(x, r^J) \oplus \mathcal{A}(f_i(x), r^J \oplus e^k)$.

Hence, for fixed $(x, i) \in S_n$, letting E_k denote the event

$$|\{J|b_i(x, r^J) \oplus A(f_i(x), r^J \oplus e^k) = x_k\}| > \tfrac{1}{2}(2^l - 1), \tag{95}$$

$$\begin{aligned}
&\Pr[\mathcal{A}'(f_i(x), i) = x|\sigma^j = b_i(x, s^j)\ \forall j] \\
&= \Pr[|\{J|b_i(x, r^J) \oplus \mathcal{A}(f_i(x), r^J \oplus e^k) = x_k\}| > \tfrac{1}{2}(2^l - 1)\ \forall k|\sigma^j = b_i(x, s^j)\ \forall j] \\
&= \Pr[\bigcap_k E_k|\sigma^j = b_i(x, s^j)\ \forall j] \\
&= 1 - \Pr[\bigcup_k E_k^c|\sigma^j = b_i(x, s^j)\ \forall j] \\
&\geq 1 - \sum_k \Pr[E_k^c|\sigma^j = b_i(x, s^j)\ \forall j] \\
&= 1 - \sum_k (1 - \Pr[E_k|\sigma^j = b_i(x, s^j)\ \forall j]) \\
&> 1 - \sum_k \frac{1}{2|f_i(x)|} \quad \text{by } \textit{Lemma } 5.2.3. \\
&= 1 - \frac{1}{2} = \frac{1}{2}.
\end{aligned} \tag{96}$$

Finally,

$$\begin{aligned}
&\Pr[\mathcal{A}'(f_i(x), i) = x] \\
&\geq \Pr[\mathcal{A}'(f_i(x), i) = x|(x, i) \in S_n, \sigma^j = b_i(x, s^j)\ \forall j] \Pr[(x, i) \in S_n, \sigma^j = b_i(x, s^j)\ \forall j] \\
&= \Pr[\mathcal{A}'(f_i(x), i) = x|(x, i) \in S_n, \sigma^j = b_i(x, s^j)\ \forall j] \Pr[(x, i) \in S_n] Pr[\sigma^j = b_i(x, s^j)\ \forall j] \\
&> \frac{1}{2}\epsilon(n)\frac{1}{2^l} \\
&\geq \frac{1}{2}\epsilon(n)\frac{1}{2|f_i(x)|p(n)^2 + 1} \\
&\geq \frac{1}{2p(n)(2|f_i(x)|p(n)^2 + 1)}\ \text{, for infinitely many } n,
\end{aligned} \tag{97}$$

which, since $|f_i(x)|$ must also be polynomially bounded, is not negligible, contrary to f being one-way, completing the proof of the theorem. □

Note that the above proof can be simplified in the case of qOWFs, since we did not use the fact that we were dealing with quantum one-way permutations or trapdoor one-way permutations in the proof except to show that g is also a trapdoor one-way permutation. Even in this case, $\mathcal{A}'$ above not only guesses some $y \in f^{-1}(f(x))$, but x itself. Hence,

Theorem 5.2.5 (The Goldreich-Levin Theorem for qOWFs)**.** *If quantum-secure one-way functions exist, then quantum-secure one-way functions with hard-core predicates exist.*

5.3 qTOWPs with Hard-cores to qPRGs

It is necessary to prove a slightly stronger result than Lemma 4.3.10 to prove the security of the public-key scheme. It is:

Theorem 5.3.1. *If $(f, \mathcal{G}, \mathcal{S}, \mathcal{I})$ (permutation, key generator, sample, invert) is a quantum-secure trapdoor one-way permutation with hard-core predicate b, let $p : \mathbb{N} \to \mathbb{N}$ be polynomially bounded, $(i, t) \leftarrow \mathcal{G}(1^n), x \leftarrow \mathcal{S}(i)$, and suppose further that x is distributed uniformly in D_i for each such i. Let*

$$X_n = (i, f_i^{p(n)}(x), b(i, f_i^{p(n)-1}(x)) \dots b(i, f_i(x))b(i, x)), \text{ and}$$
$$Y_n = (i, f_i^{p(n)}(x), r), \text{ where } r \xleftarrow{\$} \{0,1\}^{p(n)}.$$

Then $(X_n)_n$ and $(Y_n)_n$ are computationally indistinguishable (as sequential quantum ensembles).

Proof. This proof is a more direct version of that found in [Gol06] for Theorem 3.4.6, circumventing the use of the equivalence of pseudorandom generator and unpredictability of its output (passing all next-bit-tests).

By way of contradiction, suppose there is some distinguisher $\mathcal{D}$ for $(X_n)_n$ and $(Y_n)_n$ such that, without loss of generality,

$$\Pr[\mathcal{D}(X_n) = 1] - \Pr[\mathcal{D}(Y_n) = 1] \geq \frac{1}{q(n)}, \tag{98}$$

for some polynomial q, for infinitely many n.

Define, for $j = 0, 1, \ldots, p(n)$,

$$H_n^j = (i, f_i^{p(n)}(x), b(i, f_i^{p(n)-1}(x)) \ldots b(i, f_i^{p(n)-j}(x))U_{p(n)-j}), \tag{99}$$

where $U_{p(n)-j} \xleftarrow{\$} \{0,1\}^{p(n)-j}$. Note that $H_n^{p(n)} = X_n$, and $H_n^0 = Y_n$, and so

$$\begin{aligned} \frac{1}{p(n)} \sum_{j=0}^{p(n)-1} &= \Pr[\mathcal{D}(H_n^{j+1}) = 1] - Pr[\mathcal{D}(H_n^j) = 1]) \\ &= \frac{1}{p(n)}(\Pr[\mathcal{D}(X_n) = 1] - \Pr[\mathcal{D}(Y_n) = 1]) \\ &\geq \frac{1}{p(n)q(n)}\,, \end{aligned} \tag{100}$$

for infinitely many n.

Define

$$\begin{aligned} &\underline{\mathcal{A}(i, z)} \\ &j \xleftarrow{\$} \{0, \ldots, p(n) - 1\} \\ &\alpha := b(i, f_i^{j-1}(z))b(i, f_i^{j-2}(z)) \ldots b(i, z) \\ &\beta = \beta_1 \ldots \beta_{p(n)-j} \xleftarrow{\$} \{0,1\}^{p(n)-j} \\ &\textit{output } \beta_1 \oplus \mathcal{D}(i, f_i^j(z), \alpha\beta) \\ &\text{(without loss of generality, } \mathcal{D} \text{ only outputs 0 or 1)} \end{aligned} \tag{101}$$

It is claimed that

$$\Pr[\mathcal{A}(i, f_i(x)) = b(i, x)] \geq \frac{1}{2} + \frac{1}{p(n)q(n)}\,, \tag{102}$$

for infinitely many n, i.e. $\mathcal{A}$ breaks the hard-core (Claim 3.3.7.2 from [Gol06]):

Conditioning on j and β_1,

$$\begin{aligned}
&\Pr[\mathcal{A}(i, f_i(x)) = b(i,x)] \\
&= \Pr(j) \sum_{j=0}^{p(n)-1} (\Pr[\mathcal{D}(i, f_i^j(f(x)), \alpha\beta) = 1 \; and \; \beta_1 = b(i,x)] \\
&+ \; Pr[\mathcal{D}(i, f_i^j(f(x)), \alpha\beta) = 0 \; and \; \beta_1 \oplus 1 = b(i,x)]) \\
&= \frac{1}{p(n)} \sum_{j=0}^{p(n)-1} (\Pr[\mathcal{D}(i, f_i^{j+1}(x), b(i, f_i^j(x))b(i, f_i^{j-1}(x)) \ldots b(i, f(x))\beta) = 1 \; and \; \beta_1 = b(i,x)] \\
&+ \; \Pr[\mathcal{D}(i, f_i^{j+1}(x), b(i, f_i^j(x))b(i, f_i^{j-1}(x)) \ldots b(i, f(x))\beta) = 0 \; and \; \beta_1 \oplus 1 = b(i,x)]) \\
&= \frac{1}{2p(n)} \sum_{j=0}^{p(n)-1} (\Pr[\mathcal{D}(i, f_i^{j+1}(x), b(i, f_i^j(x))b(i, f_i^{j-1}(x)) \ldots b(i, f(x))b(i,x)\beta_2 \ldots \beta_{p(n)-j}) = 1] \\
&+ \; \Pr[\mathcal{D}(i, f_i^{j+1}(x), b(i, f_i^j(x))b(i, f_i^{j-1}(x)) \ldots b(i, f(x))(b(i,x) \oplus 1)\beta_2 \ldots \beta_{p(n)-j}) = 0]) \,,
\end{aligned} \tag{103}$$

since $\Pr[\beta_1 \oplus 1 = b(i,x)] = \Pr[\beta_1 = b(i,x)] = \frac{1}{2}$.

Now, note that

$$(i, f_i^{j+1}(x), b(i, f_i^j(x))b(i, f_i^{j-1}(x)) \ldots b(i, f(x))b(i,x)\beta_2 \ldots \beta_{p(n)-j}) \,, \text{and}$$

$$H_n^{j+1} = (i, f_i^{p(n)}(x), b(i, f_i^{p(n)-1}(x))b(i, f_i^{p(n)-j-1}(x)) \ldots b(i, f(x))b(i,x)\beta_2 \ldots \beta_{p(n)-j})$$

are identically distributed, since x being distributed uniformly implies that $f_i^{p(n)-j-1}(x)$ is as well, as the image of x under the permutation $f_i^{p(n)-j-1}$.

Define $H_n'^j$ to be H_n^j but with the jth bit in the third component flipped (the last bit before $U_{p(n)-j}$). By the same reasoning,

$$(i, f_i^{j+1}(x), b(i, f_i^j(x))b(i, f_i^{j-1}(x)) \ldots b(i, f(x))(b(i,x) \oplus 1)\beta_2 \ldots \beta_{p(n)-j}) \,, \text{and}$$

$$H_n'^{j+1} = (i, f_i^{p(n)}(x), b(i, f_i^{p(n)-1}(x))b(i, f_i^{p(n)-j-1}(x)) \ldots b(i, f(x))(b(i,x) \oplus 1)\beta_2 \ldots \beta_{p(n)-j})$$

are identically distributed.

Hence,

$$\begin{aligned}\Pr[\mathcal{A}(i, f_i(x)) = b(i,x)] &= \frac{1}{2p(n)} \sum_{j=0}^{p(n)-1} (\Pr[\mathcal{D}(H_n^{j+1}) = 1] + \Pr[\mathcal{D}(H_n'^{j+1}) = 0]) \\ &= \frac{1}{2p(n)} \sum_{j=0}^{p(n)-1} (Pr[\mathcal{D}(H_n^{j+1}) = 1] + 1 - \Pr[\mathcal{D}(H_n'^{j+1}) = 1]) \\ &= \frac{1}{2} + \frac{1}{2p(n)} \sum_{j=0}^{p(n)-1} (\Pr[\mathcal{D}(H_n^{j+1}) = 1] - \Pr[\mathcal{D}(H_n'^{j+1}) = 1]) .\end{aligned} \tag{104}$$

Now, since $H_n^j = H_n^{j+1}$ and $H_n^j = H_n'^{j+1}$ each with probability $\frac{1}{2}$ because H_n^j's $j+1$st bit is uniformly random,

$$\Pr[\mathcal{D}(H_n^j) = 1] = \frac{1}{2}(\Pr[\mathcal{D}(H_n^{j+1}) = 1] + \Pr[\mathcal{D}(H_n'^{j+1}) = 1]). \tag{105}$$

Hence

$$\Pr[\mathcal{D}(H_n'^{j+1}) = 1]) = 2\Pr[\mathcal{D}(H_n^j) = 1] - \Pr[\mathcal{D}(H_n^{j+1}) = 1] \tag{106}$$

and

$$\Pr[\mathcal{D}(H_n^{j+1}) = 1]) - \Pr[\mathcal{D}(H_n'^{j+1}) = 1]) = 2(\Pr[\mathcal{D}(H_n^j) = 1] - \Pr[\mathcal{D}(H_n^{j+1}). \tag{107}$$

Finally,

$$\begin{aligned}\Pr[\mathcal{A}(i, f_i(x)) = b(i,x)] &= \frac{1}{2} + \frac{1}{2p(n)} \sum_{j=0}^{p(n)-1} 2(\Pr[\mathcal{D}(H_n^j) = 1] - \Pr[\mathcal{D}(H_n^{j+1}) \\ &= \frac{1}{2} + \frac{1}{p(n)} \sum_{j=0}^{p(n)-1} (\Pr[\mathcal{D}(H_n^j) = 1] - \Pr[\mathcal{D}(H_n^{j+1}) \\ &\geq \frac{1}{2} + \frac{1}{p(n)q(n)} ,\end{aligned} \tag{108}$$

for infinitely many n. Hence b is not a hard-core for f, a contradiction. □

Theorem 5.3.2. *If f is a quantum one-way permutation with hard-core predicate b, then $G(x) := b(i, f_i^{p(n)-1}(x)) \dots b(i, f_i(x))b(i, x)$ defines a quantum-secure pseudorandom generator.*

Proof. Same as the above, omitting the i's and $f_i^{p(n)}(x)$. □

Chapter 6

More (on) Security Definitions

In this chapter, further security definitions are discussed. In Section 6.1, indistinguishability is defined so that the adversary generates a pair of messages, and it is proven equivalent to IND (Definition 4.1.3). In Section 6.2, security for the encryption of multiple messages encrypted with the same key is defined, and it is shown that security under CPA or CCA1 implies security for multiple messages under CPA or CCA1, respectively. The last section of this chapter contains discussion on the absolute values in the semantic security definitions in Subsection 6.3.1, semantic security with the SWAP test as the distinguisher in Subsection 6.3.2, security in which the simulator never has oracle access under CPA or CCA1 in Subsection 6.3.3, semantic security with a channel as the target in Subsection 6.3.4, and security for more general message distributions in Subsection 6.3.5.

6.1 IND with a Pair of Challenge Messages

Rather than fixing one of the messages to be the trivial message, $|0\rangle\langle 0|$ as in IND and IND' (Definitions 4.1.3 and 4.4.7, the adversary can generate a pair of messages.

Definition 6.1.1 (INDp)**.** [BJ15] A qPKE scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is *INDp secure*

if for every QPT adversary $\mathcal{A} = (\mathcal{M}, \mathcal{D})$ we have:

$$\begin{aligned}\big|\Pr\big[\ \mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho_{M_0E} = 1\ \big] \\ - \Pr\big[\ \mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho_{M_1E} = 1\ \big]\big| \leq \mathrm{negl}(n)\,,\end{aligned} \tag{109}$$

where $\rho_{M_0M_1E} \leftarrow \mathcal{M}(pk)$, and the probabilities are taken over $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$ and the internal randomness of Enc, $\mathcal{M}$, and $\mathcal{D}$.

- ***INDp-CPA:*** In addition to the above, $\mathcal{M}$ and $\mathcal{D}$ have oracle access to Enc_{pk}.
- ***INDp-CCA1:*** In addition to INDp-CPA, $\mathcal{M}$ has oracle access to Dec_{sk}.

INDp' can also be defined by modifying IND' in the same way. These are all proven equivalent by IND' $\iff$ IND $\iff$ INDp $\iff$ INDp', where the first is already proven, the third can be proven the same way as the first, and the second is proven as follows:

Proposition 6.1.2 (INDp $\iff$ IND)**.** *[BJ15] A quantum encryption scheme* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *is INDp secure if and only if it is IND secure.*

Proof. INDp secure $\implies$ IND secure: IND is essentially a special case of INDp. From any IND adversary $\mathcal{A} = (\mathcal{M}, \mathcal{D})$, define an INDp adversary $\mathcal{A}' = (\mathcal{M}', \mathcal{D}')$ such that $\mathcal{D}' = \mathcal{D}$, and $\mathcal{M}'$ on input pk, outputs $\rho_{M_0M_1E} = |0\rangle\langle 0|_{M_0} \otimes \rho_{ME}$, where $\rho_{ME} \leftarrow \mathcal{M}(pk)$, and $M_1 = M$.

IND secure $\implies$ INDp secure: this is essentially the transitivity of indistinguishable ensembles. From any INDp adversary $\mathcal{A} = (\mathcal{M}, \mathcal{D})$, define two IND message generators $\mathcal{M}_0 = \mathrm{Tr}_{M_1}\mathcal{M}$ and $\mathcal{M}_1 = \mathrm{Tr}_{M_0}\mathcal{M}$. Then,

$$\begin{aligned}&\big|\Pr\big[\ \mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho_{M_0E} = 1\ \big] - \Pr\big[\ \mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho_{M_1E} = 1\ \big]\big| \\ &\quad\leq \big|\Pr\big[\ \mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho_{M_0E} = 1\ \big] - \Pr\big[\ \mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)(|0\rangle\langle 0|_M \otimes \rho_E) = 1\ \big]\big| \\ &\qquad + \big|\Pr\big[\ \mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)(|0\rangle\langle 0|_M \otimes \rho_E) = 1\ \big] - \big|\Pr\big[\ \mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho_{M_0E} = 1\ \big]\big|\,.\end{aligned} \tag{110}$$

By the triangle inequality, where $\rho_{M_0M_1E} \leftarrow \mathcal{M}(pk)$, and the probabilities are taken over $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$ and the internal randomness of Enc, $\mathcal{M}$, and $\mathcal{D}$. By IND

applied to the adversary $(\mathcal{M}_0, \mathcal{D})$, the quantity on the second line is negligible, and, applied to the adversary $(\mathcal{M}_1, \mathcal{D})$, the quantity on the third line is also negligible. Hence, their sum is negligible, and so must be the quantity on the first line. □

6.2 Multiple Message Security

Security in the multiple message setting, where the output of the message generator is to be divided into multiple message registers, $M^1, \ldots, M^t$ (where t may depend on n) and E (and F) can be defined as follows:

Definition 6.2.1 (IND-mult)**.** [BJ15] A qPKE scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is *IND-mult secure* if for every QPT adversary $\mathcal{A} = (\mathcal{M}, \mathcal{D})$ we have:

$$\begin{aligned}&\big|\Pr\big[\ \mathcal{D}(\mathsf{Enc}_{pk,M^1} \otimes \cdots \otimes \mathsf{Enc}_{pk,M^t} \otimes \mathbb{1}_E)\rho_{M^1\ldots M^tE} = 1\ \big]\\ -\Pr\big[\ &\mathcal{D}(\mathsf{Enc}_{pk,M^1} \otimes \cdots \otimes \mathsf{Enc}_{pk,M^t} \otimes \mathbb{1}_E)(|0\rangle\langle 0|_{M^1\ldots M^t} \otimes \rho_E) = 1\ \big]\big| \leq \mathrm{negl}(n)\,,\end{aligned} \tag{111}$$

where $\rho_{M^1\ldots M^tE} \leftarrow \mathcal{M}(pk)$, $\rho_E = \mathrm{Tr}_{M^1\ldots M^t}(\rho_{M^1\ldots M^tE})$, and the probabilities are taken over $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$ and the internal randomness of Enc, $\mathcal{M}$, and $\mathcal{D}$.

- ***IND-mult-CPA:*** In addition to the above, $\mathcal{M}$ and $\mathcal{D}$ have oracle access to Enc_{pk}.
- ***IND-mult-CCA1:*** In addition to IND-mult-CPA, $\mathcal{M}$ has oracle access to Dec_{sk}.

Note that t must be polynomially bounded (and computable), since $\mathcal{M}$ is polynomial time.

Definition 6.2.2 (INDp-mult)**.** [BJ15] A qPKE scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is *INDp-mult secure* if for every QPT adversary $\mathcal{A} = (\mathcal{M}, \mathcal{D})$ we have:

$$\begin{aligned}&\big|\Pr\big[\ \mathcal{D}(\mathsf{Enc}_{pk,M_0^1} \otimes \cdots \otimes \mathsf{Enc}_{pk,M_0^t} \otimes \mathbb{1}_E)\rho_{M_0^1\ldots M_0^tE} = 1\ \big]\\ -\Pr\big[\ &\mathcal{D}(\mathsf{Enc}_{pk,M_1^1} \otimes \cdots \otimes \mathsf{Enc}_{pk,M_1^t} \otimes \mathbb{1}_E)\rho_{M_1^1\ldots M_1^tE} = 1\ \big]\big| \leq \mathrm{negl}(n)\,,\end{aligned} \tag{112}$$

where $\rho_{M_0^1\ldots M_0^tM_1^1\ldots M_1^tE} \leftarrow \mathcal{M}(pk)$, and the probabilities are taken over $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$ and the internal randomness of Enc, $\mathcal{M}$, and $\mathcal{D}$.

- ***INDp-mult-CPA:*** In addition to the above, $\mathcal{M}$ and $\mathcal{D}$ have oracle access to Enc_{pk}.
- ***INDp-mult-CCA1:*** In addition to INDp-mult-CPA, $\mathcal{M}$ has oracle access to Dec_{sk}.

IND'-mult and INDp'-mult can also be defined similarly. IND-mult, INDp-mult, IND'-mult and INDp'-mult are all equivalent, with proofs as in the single message (or pair of messages) settings.

Definition 6.2.3. [SEM-mult] A qPKE scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is *semantically secure* if for any QPT adversary $\mathcal{A}$, there exists a QPT simulator $\mathcal{S}$ such that for all QPTs $\mathcal{M}$ and $\mathcal{D}$,

$$\Big|\Pr\big[\ \mathcal{D}(\mathcal{A}\otimes \mathbb{1}_F)(\mathsf{Enc}_{pk,M^1}\otimes\cdots\otimes\mathsf{Enc}_{pk,M^t}\otimes\mathbb{1}_{EF})\rho_{M^1\ldots M^tEF}=1\ \big] - \Pr\big[\ \mathcal{D}(\mathcal{S}\otimes\mathbb{1}_F)\rho_{EF}=1\ \big]\Big| \leq \mathrm{negl}(n)\,, \tag{113}$$

where $\rho_{M^1\ldots M^tEF} \leftarrow \mathcal{M}(pk)$, $\rho_{EF} = \mathrm{Tr}_{M^1\ldots M^t}(\rho_{M^1\ldots M^tEF})$, and the probabilities are taken over $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$ and the internal randomness of Enc, $\mathcal{A}, \mathcal{S}, \mathcal{M}$ and $\mathcal{D}$.

- ***SEM-mult-CPA:*** In addition to the above, all QPTs have oracle access to Enc_{pk}.
- ***SEM-mult-CCA1:*** In addition to IND-mult-CPA, $\mathcal{M}$ has oracle access to Dec_{sk}.

As in the single message setting, indistinguishability and semantic security are equivalent under the same form of attack.

Furthermore, under CPA, multiple message security and single message security are equivalent. This allows the construction of CPA-secure quantum encryption schemes that can encrypt messages of arbitrary (polynomial) length from CPA-secure quantum encryption schemes that can only encrypt messages of a fixed length, by breaking up the intended message and encrypting it in blocks (and padding if necessary). That is, CPA-secure quantum encryption schemes (as we've defined them,

with restricted domains for encryption) are secure *quantum block ciphers*. This is another way (other than using the qPRF and qPRG constructions more generally) the constructed encryption schemes can be applied securely to arbitrary length messages.

Theorem 6.2.4 (IND-CPA $\implies$ IND-mult-CPA)**.** *[KL07, BJ15] If a quantum encryption scheme* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *is IND-CPA secure, then it is IND-mult-CPA secure.*

Proof. We need to show that for every adversary $(\mathcal{M}, \mathcal{D})$,

$$\begin{aligned}\big|\Pr\big[\ \mathcal{D}(\mathsf{Enc}_{pk,M_0^1}\otimes\cdots\otimes\mathsf{Enc}_{pk,M_0^t}\otimes\mathbb{1}_E)\rho_{M_0^1\ldots M_0^tE}=1\ \big]\\ -\Pr\big[\ \mathcal{D}(\mathsf{Enc}_{pk,M_1^1}\otimes\cdots\otimes\mathsf{Enc}_{pk,M_1^t}\otimes\mathbb{1}_E)\rho_{M_1^1\ldots M_1^tE}=1\ \big]\big|\leq \mathrm{negl}(n)\,,\end{aligned} \tag{114}$$

(using the equivalence with INDp-mult-CPA, for ease of notation), for $\rho_{M_0^1\ldots M_0^tM_1^1\ldots M_1^tE}\leftarrow\mathcal{M}(pk), (pk,sk)\leftarrow\mathsf{KeyGen}(1^n)$.

Consider the following circuits $\mathcal{M}_{i,pk}$, for $i=1,\ldots,t+1$:

$\underline{\mathcal{M}_{i,pk}}$ (115)

$\rho_{M_0^1\ldots M_0^tM_1^1\ldots M_1^tE}\leftarrow\mathcal{M}(pk)$

output $\rho_{M_0,M_1,E'}=$

$$(\mathbb{1}_{M_0^i,M_1^i}\otimes\mathrm{Tr}_{M_0^1\ldots M_0^{i-1}M_1^{i+1}\ldots M_1^t}\otimes\mathsf{Enc}_{pk,M_1^1}\otimes\ldots\mathsf{Enc}_{pk,M_1^{i-1}}\otimes\mathsf{Enc}_{pk,M_0^{i+1}}\otimes\cdots\otimes\mathsf{Enc}_{pk,M_0^t}\otimes\mathbb{1}_E)\rho\,,$$

where $M_0=M_0^i, M_1=M_1^i$ and the rest is all in E'.

That is, $\mathcal{M}_{i,pk}$ keeps the M_0^i and M_1^i registers for the pair of challenges, E for the new environment E' and encrypts $M_1^1,\ldots M_1^{i-1}, M_0^{i+1}\ldots M_0^t$ and places the result with E in E'.

Here, we use oracle access to Enc_{pk} or pk for the encryptions.

Let

$$\begin{aligned}\sigma_0^i&=(Enc_{pk,M_0}\otimes\mathrm{Tr}_{M_1}\otimes\mathbb{1}'_E)\mathcal{M}_{i,pk}\,,\ \text{and}\\ \sigma_1^i&=(\mathrm{Tr}_{M_0}\otimes Enc_{pk,M_1}\otimes\mathbb{1}'_E)\mathcal{M}_{i,pk}\,.\end{aligned}$$

Then σ_0^1 is distributed identically with $(\mathsf{Enc}_{pk,M_0^1} \otimes \cdots \otimes \mathsf{Enc}_{pk,M_0^t} \otimes \mathbb{1}_E)\rho_{M_0^1 \ldots M_0^t E}$, and σ_1^t, with $(\mathsf{Enc}_{pk,M_1^1} \otimes \cdots \otimes \mathsf{Enc}_{pk,M_1^t} \otimes \mathbb{1}_E)\rho_{M_1^1 \ldots M_1^t E}$, where $\rho_{M_0^1 \ldots M_0^t M_1^1 \ldots M_1^t E} \leftarrow \mathcal{M}(pk)$. Furthermore, σ_0^{i+1} and σ_1^i are distirbuted identically (they both have the encrypted registers of $M_1^1, \ldots, M_1^i, M_0^{i+1}, \ldots, M_0^t$).

Hence, we need to show

$$|\Pr[\mathcal{D}(\sigma_0^1) = 1] - \Pr[\mathcal{D}(\sigma_1^t) = 1]| \leq \mathrm{negl}(n)\,. \tag{116}$$

Define the new message generator $\mathcal{M}'$ by

$$\begin{array}{l} \underline{\mathcal{M}'(pk)} \\ i \xleftarrow{\$} \{1, \ldots, t\} \\ \textit{output } \rho' \leftarrow \mathcal{M}_{i,pk} \end{array} \tag{117}$$

Now, using the fact that σ_0^{i+1} and σ_1^i are distributed identically,

$$\begin{aligned} &\big|\Pr\big[\ \mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_{E'})\rho'_{M_0 E'} = 1\ \big] - \Pr\big[\ \mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_{E'})\rho'_{M_1 E'} = 1\ \big]\big| \\ =&\Big|\sum_{i=1}^{t} \Pr\big[\ \mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_{E'})\rho'_{M_0 E'} = 1 \mid i\ \big]\Pr[i] \\ &\quad - \sum_{i=1}^{t} \Pr\big[\ \mathcal{D}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_{E'})\rho'_{M_1 E'} = 1 \mid i\ \big]\Pr[i]\Big| \\ =&\tfrac{1}{t}\Big|\sum_{i=1}^{t}(\Pr[\mathcal{D}(\sigma_0^i) = 1] - \Pr[\mathcal{D}(\sigma_1^i) = 1])\Big| \\ =&\tfrac{1}{t}\Big|\sum_{i=1}^{t}(\Pr[\mathcal{D}(\sigma_0^i) = 1] - \Pr[\mathcal{D}(\sigma_0^{i+1}) = 1])\Big|, \ \text{ where } \ \sigma_0^{t+1} := \sigma_1^t \\ =&\tfrac{1}{t}\Big|\sum_{i=1}^{t}\Pr[\mathcal{D}(\sigma_0^i) = 1] - \sum_{i=2}^{t+1}\Pr[\mathcal{D}(\sigma_0^i) = 1]\Big| \\ =&\tfrac{1}{t}|\Pr[\mathcal{D}(\sigma_0^1) = 1] - \Pr[\mathcal{D}(\sigma_0^{t+1}) = 1]| \\ =&\tfrac{1}{t}|\Pr[\mathcal{D}(\sigma_0^1) = 1] - \Pr[\mathcal{D}(\sigma_1^t) = 1]|\,. \end{aligned} \tag{118}$$

Then, by INDp-CPA, applied to $(\mathcal{M}', \mathcal{D})$ the above quantity is negligible, and since $|\Pr[\mathcal{D}(\sigma_0^1) = 1] - \Pr[\mathcal{D}(\sigma_1^t) = 1]|$ is the product of this negligible function and t, polynomially bounded in n, it is also negligible. □

6.3 Further Motivation for SEM and Alternatives

This sections discusses further variations on semantic security and indistinguishability.

6.3.1 Absolute Values in Semantic Security

Note that SEM, SEM2 and SEM3 (Definitions 4.2.1, 4.4.2 and 4.4.5) were defined with the expression in absolute values. This was not necessary, and previous definitions did not include the absolute values [Gol04, GM84]. Without absolute values, semantic security means that for each adversary, there exists a simulator that does just as well or better. With absolute values, semantic security means that for each adversary, there exists a simulator that does just as well *and just as poorly*. Clearly semantic security with absolute values implies semantic security without, but these definitions are, in fact, equivalent. The proofs for Theorem 4.2.3 SEM $\implies$ IND and Theorem 4.4.9 SEM3 $\implies$ IND' carry through when the absolute values are dropped, so that, combined with Proposition 4.4.8 IND' $\iff$ IND and Theorem 4.2.2 IND $\implies$ SEM, semantic security without absolute values implies semantic security with absolute values.

6.3.2 The Swap Test as a Distinguisher for SEM

The swap test [GC01] can be used as the distinguisher $\mathcal{D}$ in SEM. The swap test proceeds by applying controlled-$SWAP$s ($CSWAP$ or Fredkin gates) to the corresponding qubits of ρ and σ, controlled on the state $H|0\rangle = |+\rangle = \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle$, applying the Hadamard again to the control qubit, measuring the control qubit and outputting the (negation of) the result.

The probability of acceptance of the swap test applied to a product state $\rho \otimes \sigma$ (where ρ and σ have the same number of qubits) is

$$\frac{1 + \mathrm{Tr}(\sigma\rho)}{2}. \tag{119}$$

Then, taking $\mathcal{D}$ in SEM to be the SWAP-test and considering only message generators whose outputs are product states of the form $\rho_{ME} \otimes \rho_F$ and adversaries whose

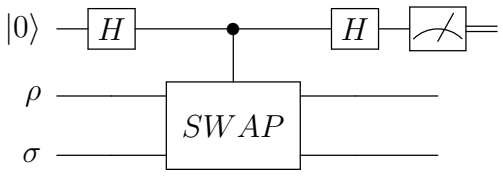

Figure 5: Circuit for the swap test

output has the same number of qubits as F, the expression in SEM becomes

$$|\operatorname{Tr}[\rho_F(\mathcal{A}(\mathsf{Enc}_{pk}\otimes \mathbb{1}_E)\rho_{ME}-\mathcal{S}\rho_E)]|\leq \operatorname{negl}(n)\,. \tag{120}$$

It's easy to see that defining semantic security in this restricted way implies SEM2 (Definition 4.4.2), since for a message-classical function generator (Definition 4.4.1) outputting $\rho_{MEF}=\rho_{ME}\otimes|y\rangle\langle y|_F$,

$$\begin{aligned}|\operatorname{Tr}[\rho_F(\mathcal{A}(\mathsf{Enc}_{pk}\otimes \mathbb{1}_E)\rho_{ME}-\mathcal{S}\rho_E]| &= |\langle y|\,(\mathcal{A}(\mathsf{Enc}_{pk}\otimes \mathbb{1}_E)(\rho_{ME}-\mathcal{S}\rho_E)\,|y\rangle\,|\\ &= |\Pr[\mathcal{A}(\mathsf{Enc}_{pk}\otimes \mathbb{1}_E)(\rho_{ME})=y]-\Pr[\mathcal{S}(\rho_E)=y]|\,,\end{aligned} \tag{121}$$

where the probabilities are taken after measuring in the computational basis.

6.3.3 Simulator Oracle Access

Semantic security could be defined, not by $\forall\mathcal{A}\exists\mathcal{S}\forall\mathcal{M}\forall\mathcal{D}$, but by $\forall\mathcal{A}\exists\mathcal{A}'\forall\mathcal{M}\exists\mathcal{M}'\forall\mathcal{D}$ with some restrictions on $\mathcal{M}'$, i.e.:

Definition 6.3.1. A qPKE scheme $(\mathsf{KeyGen},\mathsf{Enc},\mathsf{Dec})$ is *SEM'* if for any QPT $\mathcal{A}$, there exists a QPT $\mathcal{A}'$ such that for every QPT $\mathcal{M}$, there exists a QPT $\mathcal{M}'$ such that $\forall n$, ρ_{MEF} and ρ'_{MEF} are identically distributed, where $\rho_{MEF}\leftarrow\mathcal{M}(pk)$, $(pk,sk)\leftarrow\mathsf{KeyGen}(1^n)$ and $\rho'_{MEE'F}=\rho'_{MEF}\otimes|x\rangle\langle x|_{E'}\leftarrow\mathcal{M}'(1^n)$, and for every QPT $\mathcal{D}$,

$$\begin{aligned}&\big|\Pr\big[\,\mathcal{D}(\mathcal{A}\otimes\mathbb{1}_F)(\mathsf{Enc}_{pk}\otimes\mathbb{1}_{EF})\rho_{MEF}=1\,\big]\\ &\quad-\Pr\big[\,\mathcal{D}(\mathcal{A}'\otimes\mathbb{1}_F)(\rho'_{EF}\otimes|x\rangle\langle x|_{E'})=1\,\big]\big|\leq\operatorname{negl}(n)\,,\end{aligned} \tag{122}$$

where $\rho_{MEF} \leftarrow \mathcal{M}(pk), \rho'_{MEF} \otimes |x\rangle \langle x|_{E'} \leftarrow \mathcal{M}'(1^n)$, and the probabilities are taken over $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$ and the internal randomness of $\mathsf{Enc}, \mathcal{A}, \mathcal{A}', \mathcal{M}, \mathcal{M}'$ and $\mathcal{D}$.

- ***SEM'-CPA:*** In addition to the above, $\mathcal{A}$ and $\mathcal{M}$ have oracle access to Enc_{pk}.
- ***SEM'-CCA1:*** In addition to SEM'-CPA, $\mathcal{M}$ has oracle access to Dec_{sk}.

This definition is closer to that in [Gol04]. $\mathcal{A}$ and $\mathcal{M}$ are as before in SEM (Definition 4.2.1), but $\mathcal{A}'$ and $\mathcal{S}'$ do not receive public keys in the public-key setting or oracle access under CPA or CCA1. Furthermore, $\mathcal{M}'$ also outputs a binary string x into an extra register E', on top of ρ'_{MEF}, to be passed along to $\mathcal{A}'$, which receives this x on top of ρ_E. Of course, one could allow more general states in E', even for E' to be entangled with the rest, as long as the "challenges" are the same, i.e. ρ_{MEF} and ρ'_{MEF} are identically distributed, where $\rho_{MEF} \leftarrow \mathcal{M}(pk)$, $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$ and $\rho'_{MEF} \leftarrow \mathrm{Tr}_{E'} \mathcal{M}'(1^n)$. However, just a classical binary string is sufficient for (an easy proof that) IND $\implies$ SEM, so the definition is seemingly stronger by further restricting $\mathcal{M}'$, whose existence is required for SEM' to hold.

To prove IND $\implies$ SEM', as in [Gol04], A' is defined as before in the proof of Theorem 4.2.3, but also takes extra classical input to use as keys in the encryption and decryption algorithms as subroutines in place of oracle queries. $\mathcal{M}'$ is defined from $\mathcal{M}$ by generating its own $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$, using $\mathcal{M}$ on the pk it generated, replacing any oracle queries with the use of the encryption and decryption algorithms as subroutines with these keys, and then forwarding the keys as x in E' along to $\mathcal{A}'$. In the private-key scenario under regular attack (neither CPA nor CCA1), there's no need to pass along a key at all, as $\mathcal{A}'$ simply generates its own, as did $\mathcal{S}$ previously.

SEM2 and SEM3 can also be modified accordingly, and the rest of the cycle of implications from SEM' $\implies$ SEM2' $\implies$ SEM3' $\implies$ IND' $\implies$ IND can again be completed as before.

Such a definition may appear stronger, since a simulator that knows nothing about the keys and without any oracle access always suffices. It is, however, much clunkier. Furthermore, once it's fully parsed and understood, it seems less intuitive if one interprets $\mathcal{M}$ as the behaviour of some honest party sending messages, since the adversary and simulator should be working on the *same* message generator, not

different ones that output identically distributed messages when the probabilities are taken over the keys (and the internal randomness of $\mathcal{M}$ and $\mathcal{M}'$). That being said, the interpretation of the behaviour of $\mathcal{M}$ as honest when it is given oracle access to the encryption or decryption algorithms is itself somewhat tenuous, although perhaps justified by the possibility that the message sender can be deceived into using the oracles or into sending particular messages after interacting with a malicious party with access to the oracles.

6.3.4 Semantic Security with a Channel as the Target

As mentioned already in Subsection 4.2.1, one of first obvious definitions of semantic security for the encryption of quantum states is to replace, in the classical definition, the function of the plaintext that adversaries attempt to predict with quantum circuits or general quantum channels (which may not be efficiently implemented) and consider how well the adversaries approximate them.

In more detail, in the classical setting, semantic security is defined with some function f of the plaintext to be predicted by the adversary $\mathcal{A}$ and simulator $\mathcal{S}$. A natural quantum version of this could mean replacing f by a quantum channel Φ, and rather than looking for the difference between the probability that the output of $\mathcal{A}$ and the output of Φ are *strictly identical*, and the probability that the output of $\mathcal{S}$ and the output of Φ are *strictly identical*, one can pass the outputs through a QPT distinguisher $\mathcal{D}$ (i.e. measurements) and check for equality of the outcomes. Furthermore, in the original definition of semantic security given by Goldwasser and Micali in [GM84], f was *any* sequence of functions, indexed by the keyed encryption algorithm (equivalently, the public key), i.e. it need not be computable.

A candidate definition for semantic security could be the following:

Definition 6.3.2. A qPKE scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is *SEMF* if for any QPT adversary $\mathcal{A}$, there exists a QPT simulator $\mathcal{S}$ such that for all quantum channels Φ, for all QPTs $\mathcal{M}$ and $\mathcal{D}$, there exists a negligible function negl such that

$$|\Pr[\mathcal{D}\mathcal{A}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho_{ME} = \mathcal{D}\Phi_{pk}\rho_M] - \Pr[\mathcal{D}\mathcal{S}\rho_E = \mathcal{D}\Phi_{pk}\rho_M]| \leq \mathrm{negl}(n)\,, \quad (123)$$

for all $n, (pk, sk) \leftarrow \mathsf{KeyGen}(1^n), \rho_{ME} \leftarrow \mathcal{M}(pk)$.

With the usual additions for CPA and CCA1.

The channel Φ above can be restricted to be QPT (or one could allow more general quantum operations, although this misses the point of semantic security).

However, such a definition may be asking too much, since the "game" that the semantic security definition captures does not appear to be generally realistic, as it would require two copies of the message to exist: one for encryption and one to which the quantum circuit or channel is applied: the event $\mathcal{D}\mathcal{A}(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)\rho_{ME} = \mathcal{D}\Phi_{pk}\rho_M$ contains the M subsystem of ρ_{ME} twice, so attempting to generate events distributed this way in an IND game may not be feasible in polynomial time. In the original proof by Goldwasser and Micali in [GM84], despite defining a different IND message generator based on the original SEM one, the algorithm they defined required multiple encryptions of the same message. Of course, cloning arbitrary quantum states is known to be impossible (by the no-cloning theorem, Theorem 3.4.13, but we need only prepare states $\rho \otimes \rho$, such that ρ is distributed identically to the output of $\mathcal{M}$ (or some other suitable message generator).

One might instead hope that setting $\mathcal{D}' := \mathcal{D}\mathcal{A}$ and $\mathcal{M}' := \mathcal{M}$ for a distinguisher would work, but a proof along these lines has not been found. One obstacle is that, since the output of $\mathcal{D}$ is not fixed on each of the trivial 0 and message generator challenges, a priori, $\mathcal{D}' = 1$ may occur with the same probability on the two challenges, despite the non-negligible difference in the probabilities that the outputs of $\mathcal{D}'$ and $\mathcal{D}\Phi_{pk}$ are the same. To illustrate the problem with a simple example, consider two uniformly random bits, x, and y. Then, $|\Pr[x = x] - \Pr[y = x]| = 1 - \frac{1}{2} = \frac{1}{2}$, but $\Pr[x = 1] = \Pr[y = 1] = \frac{1}{2}$.

Furthermore, in SEM3 (Definition 4.4.5, as in [GM84] or [Des09, DD10]), one could allow f to be arbitrary (with polynomially bounded output), not just QPT. However, again the proof in [GM84] does not carry through due to no-cloning, and the proof in [Des09, DD10] has its own problems. The latter uses Goldreich-Levin predicates to go from breaking semantic security with arbitrary f to breaking semantic security with a predicate, and from an adversary $\mathcal{A}$ to the distinguisher $\mathcal{D} := r \odot \mathcal{A}$, the dot product of r and $\mathcal{A}$ for some appropriate r. However, r is not chosen uniformly,

and it's not clear that it can be, nor can r simply be chosen randomly and the same message generator be used, since the same obstacle as in the previous paragraph is encountered. It's also not clear that their proof will carry over into the non-uniform computational setting. The idea is to generate messages that satisfy $r \odot f = 1$ only or $r \odot f = 0$ only, with r fixed, for each pair of keys (so the message generators would become non-uniform, too). Since $r \odot f$ is, in general, an arbitrary function in $\{0,1\}^m \to \{0,1\}$, the 2^m values of $r \odot f$ cannot all be hardcoded into the circuit or used as advice, and the function's circuit complexity may grow faster in n than any polynomial, so no polynomial size subcircuit to implement it may exist.

Returning to the problem of preparing multiple copies of a message, applying the deferred measurement principle to $\mathcal{M}$ and purifying the result will give, on input pk, a pure state $\sum_x \alpha_x |\psi_x\rangle |x\rangle$, so that measuring the x system and tracing out part of the resulting state gives ρ distributed as the output of $\mathcal{M}$.

Two approaches would be

1. Prepare $\sum_x \alpha_x |\psi_x\rangle |x\rangle |\psi_x\rangle |x\rangle$, and then measure and apply traces as appropriate to obtain two identical messages.

2. Generate one message, recording the measurement result x_0, and then "amplify the amplitude" of the x_0 term in $\sum_x \alpha_x |\psi_x\rangle |x\rangle$ to obtain (or approximate) $|\psi_{x_0}\rangle |x_0\rangle$. Then measure and apply traces as appropriate to obtain a second copy of the first message.

It is not clear how to achieve 1. The no-cloning theorem prevents us from passing from *arbitrary* $\sum_x \alpha_x |\psi_x\rangle |x\rangle$ to $\sum_x \alpha_x |\psi_x\rangle |x\rangle |\psi_x\rangle |x\rangle$ with a single deterministic channel, but $\sum_x \alpha_x |\psi_x\rangle |x\rangle$ is fixed for each n or key or pair of keys.

To expand on the second approach, *amplitude amplification* [BHMT02, KLM07] is a generalization of Grover's search algorithm, which would use the purification of the message generator as a black box. However, it appears not to be efficient enough, since the algorithm uses $\Theta(\frac{1}{\sqrt{p}})$ applications of the purified circuit and its inverse in the worst case for p the probability that a particular message is generated: with even a just linear number of measurement gates (fixing the input to the quantum circuit), p may be exponentially small, so the running time may be exponential. This is also for

p known, but they design a quantum search algorithm that works in $\Theta(\frac{1}{\sqrt{p}})$ *expected applications* for p unknown. $\Theta(\frac{1}{\sqrt{p}})$ is optimal (as a generalization of Grover's), but the problem it solves is posed with the preparation circuit and the characteristic function for solutions given as black boxes, which is not the case here: a description of the circuit and the measurements are both given.

One possible solution to avoid the whole issue is to not permit measurement gates at all, or at least limit the number in the message generator to be $O(\log n)$ to be able to use quantum search or just repeatedly generate messages until the measurement matches the first one, but in doing so, the definitions become contrived and may no longer even be equivalent to the ones used in this thesis. When it *is* possible to prepare the messages multiple times and Φ is QPT, SEM as defined in 4.2.1 captures this.

The possible equivalence of IND and SEMF is left as an open problem.

6.3.5 Alternative Message Distributions

However, if SEMF is defined as above in Definition 6.3.2, but where ρ is distributed arbitrarily (not necessarily generated, but indexed by the security parameter n as a sequential ensemble $(\rho_n)_n$, or possibly the public key pk), and the same is done for IND, it is easy to show IND $\implies$ SEM:

Proof. By contrapositive, suppose not SEM. Then there exists an $\mathcal{A}$ such that for all $\mathcal{S}$, there exists ρ^{ME}, Φ and $\mathcal{D}$ and a polynomial p such that the above difference in probabilities is $> 1/p(n)$ for infinitely many n.

Define a simulator $\mathcal{S}$ by $\mathcal{S}\rho_E := \mathcal{A}(\mathsf{Enc}_{pk}(|0\rangle\langle 0|) \otimes \rho_E)$ and consider corresponding $\Phi, \mathcal{D}$ and p that together violate SEM. In the private-key without oracle access to Enc_{pk}, generate a new key, and use it instead.

Simulating the above SEM game by an IND game is enough to show
IND $\implies$ SEM. Given ρ_{ME} distributed arbitrarily, define quantum states distributed as $\rho'_{ME'} = \rho_{ME} \otimes \Phi(\rho_M)$. Here, there are two copies of ρ, but they haven't been obtained from a single one through a quantum channel, so no-cloning is not violated.

Define the IND distinguisher, $\mathcal{D}'$ by $\mathcal{D}'(\sigma_{CEF}) = 1$ if $\mathcal{D}(\mathcal{A} \otimes I)\sigma_{CE} = \mathcal{D}\sigma_F$, and 0 otherwise.

Doing this, we've simulated the SEM game by an IND game in which $\mathcal{D}'$ distinguishes encryptions of $\rho'_{ME'}$ from encryptions of $|0\rangle\langle 0| \otimes \rho'_{E'}$, since the SEM expression becomes

$$|\Pr[\mathcal{D}'(\mathsf{Enc}_{pk} \otimes \mathbb{1}_E)(\rho'_{ME'}) = 1] - \Pr[\mathcal{D}'(\mathsf{Enc}_{pk}(|0\rangle\langle 0|) \otimes \rho'_{E'}) = 1]| > \tfrac{1}{p(n)}\,, \qquad (124)$$

for infinitely many n. □

The above proof can also be adapted to unbounded depth message generators (with at most polynomially many measurement gates, uniform or non-uniform, but still requiring the size of the state to be polynomially bounded in n): ρ could be generated and while doing so, the measurement results that lead to it could be recorded, putting them in E'. Then the message generator is reused until, with high enough probability (so that $1 - \Pr$ is negligible), a second copy of a state resulting from the same measurement results (and thus identical to the first) is obtained. In the non-uniform setting, if Φ is allowed to be arbitrarily chosen (but polynomially bounded in output size), then Φ could be approximated in order to generate $\rho'_{ME'}$ as above. The uniform setting with Φ arbitrary would be a closer analogue of the original formulation of semantic security in [GM84], and a similarly more complex proof would likely be necessary.

However, in having messages distributed this way (either through unbounded depth generators or arbitrary distributions), the following cannot be allowed, as in the classical setting, or else such a definition of security will never be satisfied:

1. the length of the messages ($|M| + |E|$) grows at least exponentially, or
2. the messages depend on (i.e. are indexed by) pk or the encryption or decryption oracle.

The same arguments as in the classical case work, see the exercises 3 and 28.2, respectively, in [Gol04, Chapter 5].

Arbitrary message distributions (with the above restrictions) could allow continuous message distributions (as in [XY12]) or even more general ones. Of course, CCA1 security would have to be defined differently, for example, by having another algorithm taking pk (or 1^n) as input, with access to the encryption and decryption oracles and whose output is given to the adversary and simulator, along with the challenge to the adversary, independently of the message in the challenge.

Chapter 7

Conclusion

This chapter is from the joint paper [ABF+16]: one item in Section 7.1 from the paper has been removed for this thesis, and the second one listed here has been added.

We have defined semantic security for the encryption of quantum data and shown its equivalence with indistinguishability. We have given general constructions of CCA1-secure private-key quantum encryption schemes and a secure public-key quantum encryption schemes from quantum-secure one-way functions and quantum-secure trapdoor one-way permutations.

7.1 Extensions and Future Work

We now briefly discuss some possible extensions of the above results. In most cases, these extensions are a matter of modifying our definitions and proofs in a fairly straightforward way. We leave the other cases as interesting open problems.

1. Our definitions of IND-CPA, IND-CCA1 and SEM assume that all of the relevant messages are generated in polynomial time. In other words, our results assume "uniform" adversaries. As is standard classically (see Chapter 5 of Goldreich's text [Gol04]), these definitions can be adjusted to the case of "non-uniform" (but still polynomial-time) adversaries, whose messages need not be generated efficiently. While the proof is of course somewhat different, the equivalence

of IND and SEM still hold in this case. The encryption schemes (IND-CCA1 private-key and IND-CPA public-key) presented above carry over as well, except that we now require primitives (qPRFs and qTOWPs, respectively) which are secure against non-uniform adversaries.

2. The possible equivalence of IND and a suitable semantic security definition with the contents F as the output of a channel applied to ρ_M (as in Definition 6.3.2 SEMF) is left as an open problem. Various obstacles were raised in Subsection 6.3.4.

3. Another outstanding open problem is to define and construct schemes for CCA2 (adaptive chosen ciphertext attack) security in the case of the encryption of quantum states. Classically, CCA2 security is defined as CCA1, with the further property that the adversary is allowed to query the decryption oracle even *after* the challenge query, *provided* he does not query about the challenge ciphertext itself (otherwise the challenger aborts the game.) The obvious way to define this in the quantum world is to require that every decryption query performed by the adversary after the challenge query is 'very different' from the challenge query itself (e.g., it is orthogonal to the challenge ciphertext.) But the problem here is that this condition might be impossible for the challenger to check: for example, the adversary might embed in a decryption query a component non-orthogonal to the challenge query, but with such a small amplitude that the challenger cannot detect it with high probability. Even if it is unclear whether this issue could raise problems in any actual reduction, it would be anyway a striking asymmetry to the classical case, because there would be no way for the challenger to check that the adversary actually fulfilled the required condition. Hence, giving a satisfactory definition for CCA2 security in the quantum world remains an interesting open problem.

Bibliography

[Aar09] Scott Aaronson. Quantum copy-protection and quantum money. In *Computational Complexity, 2009. CCC'09. 24th Annual IEEE Conference on*, pages 229–242. IEEE, 2009.

[ABB+14] Romain Alléaume, Cyril Branciard, Jan Bouda, Thierry Debuisschert, Mehrdad Dianati, Nicolas Gisin, Mark Godfrey, Philippe Grangier, Thomas Länger, Norbert Lütkenhaus, Christian Monyk, Philippe Painchault, Momtchil Peev, Andreas Poppe, Thomas Pornin, John Rarity, Renato Renner, Gregoire Ribordy, Michel Riguidel, Louis Salvail, Andrew Shields, Harald Weinfurter, and Anton Zeilinger. Using quantum key distribution for cryptographic purposes: A survey. *Theoretical Computer Science*, 560:62–81, 2014.

[ABF+16] Gorjan Alagic, Anne Broadbent, Bill Fefferman, Tommaso Gagliardoni, Christian Schaffner, and Michael St. Jules. Computational security of quantum encryption, 2016. To appear in the *9th International Conference on Information Theoretic Security (ICITS2016)*. http://arxiv.org/abs/1602.01441.

[AC02] Mark Adcock and Richard Cleve. A quantum Goldreich-Levin theorem with cryptographic applications. In Helmut Alt and Afonso Ferreira, editors, *STACS 2002*, volume 2285 of *Lecture Notes in Computer Science*, pages 323–334. Springer Berlin Heidelberg, 2002.

[AC12] Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 41–60. ACM, 2012.

[ACM13] Association for Computing Machinery ACM. Listen to interviews with 2012 ACM Turing Award recipients Shafi Goldwasser and Silvio Micali, 2013. http://www.acm.org/news/featured/awards/turing-award-2012.

[AKN98] Dorit Aharonov, Alexei Kitaev, and Noam Nisan. Quantum circuits with mixed states. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, pages 20–30, New York, NY, USA, 1998. ACM.

[Alb83] David Z. Albert. On quantum-mechanical automata. *Physics Letters A*, 98(5):249 – 252, 1983.

[AMTdW00] Andris Ambainis, Michele Mosca, Alain Tapp, and Ronald de Wolf. Private quantum channels. In *Foundations of Computer Science, 2000. Proceedings. 41st Annual Symposium on*, pages 547–553, 2000.

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984.

[BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, October 1997.

[BBC+93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[Bel64] John Stewart Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195–200, 1964.

[Ben80] Paul Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, 22(5):563–591, 1980.

[Ben82] Paul Benioff. Quantum mechanical Hamiltonian models of Turing machines. *Journal of Statistical Physics*, 29(3):515–546, 1982.

[BFK09] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 517–526. IEEE, 2009.

[BGS13] Anne Broadbent, Gus Gutoski, and Douglas Stebila. Quantum one-time programs. In *Advances in Cryptology–CRYPTO 2013*, pages 344–360. Springer, 2013.

[BHJ26] Max Born, Werner Heisenberg, and Pascual Jordan. Zur quantenmechanik. ii. *Zeitschrift für Physik*, 35(8):557–615, 1926.

[BHMT02] Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. In *Quantum Computation and Quantum Information: A Millennium Volume*, volume 305 of *AMS Contemporary Mathematics Series*, pages 53–74. American Mathematical Society, 2002. Earlier version in arxiv:quant-ph/0005055.

[BJ26] Max Born and Pascual Jordan. Zur quantenmechanik. *Zeitschrift für Physik*, 34(1):858–888, 1926.

[BJ15] Anne Broadbent and Stacey Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity. In *Advances in Cryptology–CRYPTO 2013*, pages 609–629. Springer, 2015.

[BOCG+06] Michael Ben-Or, Claude Crépeau, Daniel Gottesman, Avinatan Hassidim, and Adam Smith. Secure multiparty quantum computation with (only) a strict honest majority. In *Foundations of Computer Science, 2006. FOCS'06. 47th Annual IEEE Symposium on*, pages 249–260. IEEE, 2006.

[BR03] P. Oscar Boykin and Vwani Roychowdhury. Optimal encryption of quantum bits. *Physical Review A*, 67(4):042317, 2003.

[Bro15] Anne Broadbent. Delegating private quantum computations. *Canadian Journal of Physics*, pages 941–946, Jun 2015.

[BV93] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. In *Proceedings of the Twenty-fifth Annual ACM Symposium on Theory of Computing*, STOC '93, pages 11–20, New York, NY, USA, 1993. ACM.

[BZ13] Dan Boneh and Mark Zhandry. Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World. In Ran Canetti and Juan A. Garay, editors, *Crypto 2013*, volume 8043 of *LNCS*, pages 361–379. Springer, 2013.

[Coc73] Clifford C. Cocks. A note on non-secret encryption. *CESG*, 1973.

[dB24] Louis de Broglie. *Recherches sur la théorie des Quanta*. Theses, Migration - université en cours d'affectation, November 1924.

[DD10] Simon Pierre Desrosiers and Frédéric Dupuis. Quantum entropic security and approximate quantum encryption. *IEEE Transactions on Information Theory*, 56(7):3455–3464, 2010.

[Des09] Simon Pierre Desrosiers. Entropic security in quantum cryptography. *Quantum Information Processing*, 8(4):331–345, August 2009.

[Deu85] David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 400(1818):97–117, 1985.

[Deu89] David Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 425(1868):73–90, 1989.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[Die82] Dennis Dieks. Communication by EPR devices. *Physics Letters A*, 92(6):271 – 272, 1982.

[Dir30] Paul. A. M. Dirac. *The Principles of Quantum Mechanics*. International series of monographs on physics (Oxford, England). Oxford, the Clarendon Press, 1930.

[DJ92] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 439(1907):553–558, 1992.

[DN06] Christopher M. Dawson and Michael A. Nielsen. The Solovay-Kitaev algorithm. *Quantum Info. Comput.*, 6(1):81–95, January 2006.

[DNS10] Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. Secure two-party quantum evaluation of unitaries against specious adversaries. In *Advances in Cryptology–CRYPTO 2010*, pages 685–706. Springer, 2010.

[DNS12] Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. Actively secure two-party evaluation of any quantum operation. In *Advances in Cryptology–CRYPTO 2012*, pages 794–811. Springer, 2012.

[Ell70] James Henry Ellis. The possibility of secure non-secret digital encryption. *CESG*, 1970.

[EPR35] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.

[Fey82] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6):467–488, 1982.

[FKS+13] Serge Fehr, Jonathan Katz, Fang Song, Hong-Sheng Zhou, and Vassilis Zikas. Feasibility and completeness of cryptographic tasks in the quantum world. In *Theory of Cryptography*, pages 281–296. Springer, 2013.

[GC01] Daniel Gottesman and Isaac Chuang. Quantum digital signatures, 2001. https://arxiv.org/abs/quant-ph/0105032.

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, 1986.

[GHS15] Tommaso Gagliardoni, Andreas Hülsing, and Christian Schaffner. Semantic security and indistinguishability in the quantum world, 2015. To appear in CRYPTO2016. http://arxiv.org/abs/1504.05255.

[GL89] Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*, STOC '89, pages 25–32, New York, NY, USA, 1989. ACM.

[GM82] Shafi Goldwasser and Silvio Micali. Probabilistic encryption & how to play mental poker keeping secret all partial information. In *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*, STOC '82, pages 365–377, New York, NY, USA, 1982. ACM.

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270 – 299, 1984.

[Gol93] Oded Goldreich. A uniform-complexity treatment of encryption and zero-knowledge. *Journal of Cryptology*, 6(1):21–53, 1993.

[Gol04] Oded Goldreich. *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge University Press, Cambridge, UK, 2004.

[Gol06] Oded Goldreich. *Foundations of Cryptography: Volume 1, Basic Tools*. Cambridge University Press, New York, NY, USA, 2006.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, pages 197–206, New York, NY, USA, 2008. ACM.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual Symposium on the Theory of Computing*, pages 212–219, New York, 1996. ACM Press.

[HBD+15] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, October 2015.

[Hei25] Werner Heisenberg. Über quantentheoretische umdeutung kinematischer und mechanischer beziehungen. *Zeitschrift für Physik*, 33(1):879–893, 1925.

[Hei27] Werner Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik*, 43(3):172–198, 1927.

[Hil06] David Hilbert. Grundzüge einer allgemeinen theorie der linearen integralgleichungen. vierte mitteilung. *Nachrichten von der Gesellschaft*

der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse, 1906:157–228, 1906.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28:1364–1396, March 1999.

[HLSW04] Patrick Hayden, Debbie Leung, Peter W Shor, and Andreas Winter. Randomizing quantum states: Constructions and applications. *Communications in Mathematical Physics*, 250(2):371–391, 2004.

[Hol73] Alexander S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problems of Information Transmission*, 9(3):177–183, 1973.

[HvN28] David Hilbert, John von Neumann, and Lothar Wolfgang Nordheim. Über die grundlagen der quantenmechanik. *Mathematische Annalen*, 98(1):1–30, 1928.

[Ing76] Roman S. Ingarden. Quantum information theory. *Reports on Mathematical Physics*, 10(1):43 – 72, 1976.

[Kit97] Alexei Yu Kitaev. Quantum computations: algorithms and error correction. *Uspekhi Mat. Nauk*, 52:53 – 112, 1997.

[KK07] Elham Kashefi and Iordanis Kerenidis. Statistical zero knowledge and quantum one-way functions. *Theoretical Computer Science*, 378(1):101 – 116, 2007.

[KL07] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman & Hall/CRC Cryptography and Network Security Series, 2007.

[KLM07] Phillip Kaye, Raymond Laflamme, and Michele Mosca. *An Introduction to Quantum Computing*. Oxford University Press, 2007.

[Kos07] Takeshi Koshiba. Security notions for quantum public-key cryptography. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, J90-A(5):367–375, Feb 2007.

[Leu02] Debbie W. Leung. Quantum Vernam cipher. *Quantum Information and Computation*, 2(1):14–34, 2002.

[Llo96] Seth Lloyd. Universal quantum simulators. *Science*, 273(5278):1073–1078, 1996.

[Man80] Yuri Ivanovitch Manin. *Vychislimoe i nevychislimoe (Computable and Uncomputable)*. "Sov. radio," Moskva, 1980.

[Mer78] Ralph C. Merkle. Secure communications over insecure channels. *Commun. ACM*, 21(4):294–299, April 1978.

[Mer10] Ralph C. Merkle. Publishing a new idea, 2010. http://merkle.com/1974/.

[MHS+12] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger. Quantum teleportation over 143 kilometres using active feed-forward. *Nature*, 489:269–273, September 2012.

[MRV07] Cristopher Moore, Alexander Russell, and Umesh Vazirani. A classical one-way function to confound quantum adversaries. *eprint arXiv:quant-ph/0701115*, January 2007.

[MS10] Michele Mosca and Douglas Stebila. Quantum coins. *Error-Correcting Codes, Finite Geometries and Cryptography*, 523:35–47, 2010.

[Nai40] Mark A. Naimark. Spectral functions of a symmetric operator. *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, 4:309 – 318, 1940.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[NY90] Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing*, STOC '90, pages 427–437, New York, NY, USA, 1990. ACM.

[OTU00] Tatsuaki Okamoto, Keisuke Tanaka, and Shigenori Uchiyama. Quantum public-key cryptosystems. In Mihir Bellare, editor, *Advances in Cryptology CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 147–165. Springer Berlin Heidelberg, 2000.

[Pop75] R. P. Poplavskii. Thermodynamic models of information processes. *Physics-Uspekhi*, 18(3):222–241, 1975.

[PW08] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, pages 187–196, New York, NY, USA, 2008. ACM.

[RS92] Charles Rackoff and Daniel R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In Joan Feigenbaum, editor, *Advances in Cryptology — CRYPTO '91: Proceedings*, pages 433–444, Berlin, Heidelberg, 1992. Springer Berlin Heidelberg.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.

[Sch35] Erwin Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31:555–563, 10 1935.

[Sha49] Claude E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, Oct 1949.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *FOCS 1994*, pages 124–134. IEEE Computer Society Press, 1994.

[Sho95] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493–R2496, Oct 1995.

[Sho96] Peter W. Shor. Fault-tolerant quantum computation. In *Proceedings of the 37th Annual Symposium on Foundations of Computer Science*, FOCS '96, pages 56–, Washington, DC, USA, 1996. IEEE Computer Society.

[Sim94] Daniel R. Simon. On the power of quantum computation. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 116–123, Nov 1994.

[Son14] Fang Song. A note on quantum security for post-quantum cryptography. In *Post-Quantum Cryptography*, pages 246–265. Springer, 2014.

[SS82] Michael Schlüter and Lu Jeu Sham. Density functional theory. *Phys. Today*, 35(2):36, 1982.

[Ste73] Lynn A. Steen. Highlights in the history of spectral theory. *The American Mathematical Monthly*, 80(4):359–381, 1973.

[Ste96] Andrew M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77:793–797, Jul 1996.

[Sti55] William Forrest Stinespring. Positive functions on C*-algebras. *Proceedings of the AMS*, 6:211 – 216, 1955.

[Unr10] Dominique Unruh. Universally composable quantum multi-party computation. In *Advances in Cryptology–EUROCRYPT 2010*, pages 486–505. Springer, 2010.

[Unr14] Dominique Unruh. Revocable quantum timed-release encryption. In *Advances in Cryptology–EUROCRYPT 2014*, pages 129–146. Springer, 2014.

[Vel13] Maria Velema. Classical encryption and authentication under quantum attacks. Master's thesis, Master of Logic, University of Amsterdam, 2013. http://arxiv.org/abs/1307.3753.

[vN27] John von Neumann. Wahrscheinlichkeitstheoretischer aufbau der quantenmechanik. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1927:245–272, 1927.

[vN55] John von Neumann. *Mathematical Foundations of Quantum Mechanics*. Princeton Landmarks in Mathematics and Physics. Princeton University Press, Princeton, NJ, USA, 1955. Translated from the German edition by Robert T. Beyer. Original first edition published in German in 1932.

[Wie83] Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

[Wil76] Malcolm J. Williamson. Thoughts on cheaper non-secret encryption. *CESG*, 1976.

[WZ82] William K. Wootters and Wojciech H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, Oct 1982.

[XY12] Chong Xiang and Li Yang. Indistinguishability and semantic security for quantum encryption scheme. *Proc. SPIE*, 8554:85540G–85540G–8, 2012.

[Yao93] Andrew Chi-Chih Yao. Quantum circuit complexity. In *Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on*, pages 352–361, Nov 1993.

[Zha12] Mark Zhandry. How to construct quantum random functions. In *FOCS 2012*, pages 679–687. IEEE, 2012.