UNCLONEABLE QUANTUM ENCRYPTION VIA RANDOM ORACLES

Sébastien Lord

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

Department of Mathematics and Statistics
Faculty of Science
University of Ottawa

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

Abstract

One of the key distinctions between classical and quantum information is given by the *no-cloning theorem*: unlike bits, arbitrary qubits cannot be perfectly copied. This fact has been the inspiration for many quantum cryptographic protocols.

In this thesis, we introduce a new cryptographic functionality called *uncloneable encryption*. This functionality allows the encryption of a classical message such that two collaborating but non-communicating adversaries may not both simultaneously recover the message, even when the encryption key is revealed.

We achieve this functionality by using Wiesner's conjugate coding scheme to encrypt the message. We show that the adversaries cannot both obtain all the necessary information for the correct decryption with high probability. Quantum-secure pseudorandom functions, modelled as random oracles, are then used to ensure that any partial information that the adversaries obtain does not give them an advantage in recovering the message.

Résumé

Une différence fondamentale entre l'information classique et quantique est énoncée par le théorème d'impossibilité du clonage: contrairement à des bits, il est impossible de produire des copies de qubits. Ceci est la base de plusieurs protocoles en cryptographie quantique.

Dans cette thèse, nous présentons une nouvelle fonctionnalité cryptographique nommée *chiffrage inclonable*. Cette fonctionnalité assure qu'un message chiffré ne puisse être utilisé pour produire deux états qui permettraient d'obtenir le message, même quand la clé est dévoilée.

Nous implémentons cette fonctionnalité en utilisant le code conjugué de Wiesner pour le chiffrement. Ainsi, il est improbable que deux adversaires puissent recevoir toute l'information nécessaire. Des fonctions pseudo-aléatoires, modélisées par des oracles aléatoires, sont utilisées afin de garantir que n'importe quelle information partielle que les adversaires obtiennent ne puisse les aider à obtenir le message.

Acknowledgements

First and foremost, I would like to thank my supervisor Dr. Anne Broadbent. Over the past few years, she has given me all the opportunities and mentorship I could have hoped to obtain from a graduate program. This work would not have been possible without her insight, advice, and patience.

I would also like to thank all the administrative and support staff at the University of Ottawa's Department of Mathematics and Statistics. They have continuously gone above and beyond to provide us with a great research environment.

I also take this opportunity to thank the examiners who have given me invaluable feedback which has helped me put the final touches on this work.

Finally, I want to thank Mireille for her extraordinary and boundless support as well as my sister Jasmine for twenty-three years of constructive criticism.

Contents

List of Figures

Chapter 1

Introduction

How can two parties communicate privately over a public channel? This is a fundamental problem studied in the field of cryptography, and it is solved using *encryption schemes*. In this thesis, we study a particular type of security notion for encryption schemes. This notion is called *uncloneable encryption*, and we show how to achieve it using tools from quantum cryptography.

In this chapter, we give a brief and informal overview of some notions from classical and quantum cryptography, as well as a few historical notes. We hope that this development helps the reader situate this work within the existing literature and understand the problem that we wish to solve.

Thesis Outline. Chapter 2 is be dedicated to defining the general mathematical notions which we use. This includes an overview of the mathematical formalism of quantum mechanics. In Chapter 3, we define and elaborate on a few specific notions from quantum computing. Chapters 4 and 5 contain the core original contributions of this work. In Chapter 4, we formally define the notion of uncloneable encryption and give two candidate encryption schemes. In Chapter 5, we show that one of these schemes satisfies our security notions. Finally, we conclude by collecting a few open questions in Chapter 6.

1.1 Encryption and Keys

What problem does *encryption* solve? We often imagine a scenario where Alice wants to send a message, called the *plaintext*, to Bob. However, Alice and Bob only have

access to a public channel. This means that an eavesdropping Eve can see all the information transmitted between Alice and Bob. An *encryption scheme* is a protocol which allows Alice to encode her plaintext into a *ciphertext* such that Bob is be able to recover the plaintext but Eve is not. We assume that Alice and Bob share a common secret which we call the *key* and that Eve does not know this key. We illustrate this scenario in Figure 1.1.

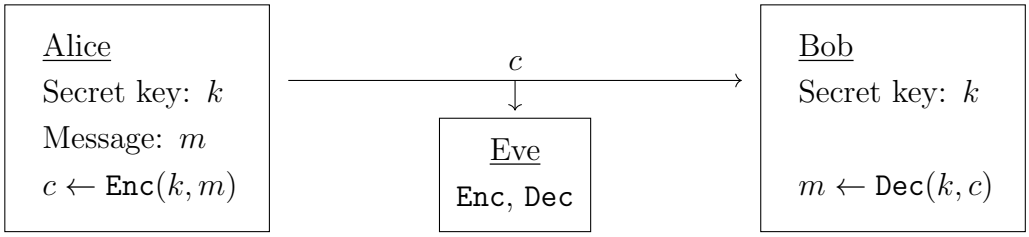


Figure 1.1: Encrypted communication in the presence of an eavesdropper. Eve knows the encryption and decryption procedures, but not the key.

Formally, such a scheme is known as a *private-key encryption scheme*. The key is private in the sense that Eve knows nothing about it. We emphasize that both Alice and Bob have the same key. It is important to note that private-key encryption schemes do not consider the question of how Alice and Bob have established a common secret key. This is known as the *key distribution problem*.

We briefly mention the existence of *public-key encryption schemes*, such as the one presented by Rivest, Shamir, and Adleman [RSA78]. In a public-key encryption scheme, the key Alice uses to encrypt a messages is known to all, even Eve. However, a different key, which only Bob knows, is needed to correctly decrypt the message. In general, the security of public-key encryption schemes rely on the unproven difficulty of solving a particular instance of a mathematical problem (*e.g.*, factoring a semiprime). We do not discuss public-key encryption schemes any further in this thesis.

In an article appearing in the *Journal des Sciences Militaires*, and later published as part of a book, Kerckhoffs details six properties that a good encryption scheme should possess. One of these properties, "*Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvéniant tomber entre les mains de l'ennemi;*" [Ker83], is now known as *Kerckhoffs' principle*. It may be translated as: "The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without

inconvenience".

In practice, Kerckhoffs' principle tell us that we should assume that an eavesdropper has a complete and accurate description of both the encryption and decryption procedures used by Alice and Bob. The only information that the eavesdropper does not know ahead of time is the encryption key.

It follows that the secrecy of an encrypted message should only depend on the secrecy of the key. It also follows that if Alice and Bob wish to keep their message secret from Eve, they must ensure that Eve never learns the key at a later point. Indeed, Eve may have kept a copy of the ciphertext in the hopes of later learning the key. The possibility of this type of attack seems to be considered in another of Kerckhoffs' desired properties: "*La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifié au gré des correspondants;*" [Ker83]. This may be translated as: "It must be possible to easily change the key as well as to transmit and remember it without the use of written notes". Every time the key is written down, it creates a new opportunity for the eavesdropper to steal it.

This has become a very real practical problem in the implementation of cryptographic systems. Keys are often stored in a computer's memory, and significant effort is sometimes deployed to ensure that they are properly destroyed. This is an aspect of the larger problem of *key management*. A technical overview of this problem can be found in [Bar16].

1.2 Uncloneability of Quantum States

One of the key distinctions between classical information (*e.g.*, bits on a hard drive) and quantum information (*e.g.*, the polarization of a photon) is that quantum information cannot be perfectly copied. This statement can be made precise via the *no-cloning theorem*.

In this section, we give a brief history and an informal statement of the no-cloning theorem. A formal statement of this theorem is given later in Theorem 2.2.28. Then, we discuss a few scenarios in which the no-cloning theorem allows quantum cryptography to achieve goals which are impossible for classical cryptography. These goals relate, in one way or another, to the key distribution and management problems.

1.2.1 No-Cloning Theorem

The story of the no-cloning theorem often begins with the tale of a fundamentally flawed proposal for superluminal communication. One of the referees of the paper containing the proposal, Peres, later published his reasoning for accepting a paper that they knew to be wrong [Per03]. In short, Peres knew that the paper must have been wrong as it contradicted special relativity. However, the paper did not make any type of reference to relativity, and so the error must have been somewhere else. Peres believed that finding and discussing this error would be beneficial to the field of quantum information. We give a short account of this story.

In December of 1982, Hebert published an intriguing paper titled *FLASH—A Superluminal Communicator Based Upon a New Kind of Quantum Measurement* [Her82]. In this paper, Hebert describes a scheme that would allow faster-than-light communication between Alice and Bob via quantum entanglement and measurements.

The FLASH scheme is remarkably simple. It relies on the idea that when a measurement is made on one half of an entangled quantum system, the complete system must *collapse* into a particular state, including the half that was not measured. This collapse is instantaneous and different measurements can lead to different possible outcomes for the resulting state.

Thus, in the FLASH scheme, Alice can send a one bit message to Bob by using one of two distinct measurements on her half of an entangled system she shares with Bob. However, Bob needs more than one measurement on his half to identify the measurement Alice has made. To be able to complete the necessary number of measurements, he uses an apparatus to "xerox" his half of the quantum system to obtain multiple exact copies. Each of these copies are then subject to the necessary measurements.

Near the end of his paper, Herbert writes:

> "The weakest link in the FLASH scheme is the assumption that a laser gain tube is able to exactly duplicate single photons."

He was quite right.

A preprint of Herbert's paper was circulated prior to its publication, and a fundamental problem was identified. In two separate papers, published before Herbert's, Dieks [Die82], Wooters, and Zurek [WZ82] showed that such duplication of quantum

states was fundamentally impossible. In other words, the laws of quantum mechanics do not allow the existence of an apparatus that can take as input any arbitrary quantum state and return as output two or more *exact* copies of this state. This fact has become known as the no-cloning theorem.

We note that it is argued, by Ortigoso [Ort18] for example, that the no-cloning theorem was already known to the community prior to the works of Dieks, Wooters, and Zurek. In fact, Ortigoso points to the works of Park [Par70] as the original publication of the no-cloning theorem.

We give a formal statement of the no-cloning theorem in Theorem 2.2.28. However, to our knowledge, this formulation of the no-cloning theorem has never explicitly appeared in any formal proof of security for cryptographic protocols. Instead, cryptographers sometimes refer to the "no-cloning principle", which is the intuitive idea that quantum states may not be perfectly cloned. This principle is then used to argue that a given protocol could very well be shown to be secure, typically by arguing that breaking the protocol should imply some sort of cloning of quantum states.

1.2.2 Applications of the No-Cloning Theorem

Quantum cryptography, via the no-cloning theorem, offers some solutions to the key distribution and key management problems. We discuss a few of them here.

1.2.2.1 Quantum Key Distribution

There is little doubt that *quantum key distribution* has been quantum cryptography's most notable contribution to date. Introduced by Bennett and Brassard [BB84], it gives a solution to the key distribution problem in which security is based not on the assumed hardness of some mathematical problem but on the fundamental laws of physics. The protocol presented by Bennett and Brassard was heavily influenced by Wiesner's foundational work on conjugate coding [Wie83].

In fact, quantum key distribution is sometimes considered as the whole of quantum cryptography. We emphasize that this identification of quantum cryptography and quantum key distribution is incorrect. An overview of quantum cryptography beyond key distribution can be found in the survey paper of the same name by Broadbent and Schaffner [BS16].

What exactly is a quantum key distribution scheme? By exchanging quantum

states (*e.g.*, photons) instead of classical messages, Alice and Bob are able to expand a small secret key into a larger one, even in the presence of an eavesdropping Eve. A typical quantum key distribution protocol, such as the BB84 protocol, has at least three rounds of communication. First, Alice sends quantum states to Bob who acknowledges the receipt of the quantum states. Then, multiple rounds of (classical) communications take place between Alice and Bob to distill a common secret from the quantum states as well as to verify for eavesdropping. The initial small secret key is needed to authenticate the classical channel that Alice and Bob share.

The security guarantee of a quantum key distribution protocol can be formulated in the following way. Either Alice and Bob detect the eavesdropping attempt by Eve, or Eve is left with an arbitrarily small amount of information on the key. In the case that eavesdropping is detected, Alice and Bob simply do not use the key that was established. Shor and Preskill [SP00] offer a concise proof of security for Bennet and Brassard's protocol. Their work builds on and simplifies the earlier proofs of Lo, Chau [LC99], and Mayers [May96].

The no-cloning theorem does not explicitly appear in the Shor-Preskill proof of security. However, it is possible to appeal to the no-cloning principle to argue for the feasibility of quantum key distribution. Since Eve is unable to perfectly clone quantum states, she cannot keep a copy of the quantum states sent by Alice and wait to eavesdrop on the classical communication. It is then argued that any action Eve could take on the transmitted quantum states is either be detected with high probability, or leaves her with almost no information on the final distilled key.

1.2.2.2 Quantum Encryptions for Classical Messages

Quantum key distribution ensures that an eavesdropping Eve is either detected or stays ignorant of the distilled key. In fact, encrypting a classical message into a quantum ciphertext can give Alice and Bob a similar type of advantage over Eve. We present two slightly different notions of this advantage that have already appeared in the literature.

Quantum tamper-evident encryption. Gottesman, in his work *Uncloneable Encryption* [Got03], gives an encryption scheme for classical messages that produces quantum ciphertexts. The advantage that this scheme holds over any classical scheme is that it allows the recipient to verify if an eavesdropper has attempted to obtain

information on the ciphertext. At a high level, Gottesman's protocol can be seen as an implementation of the BB84 protocol but with all of the classical communication replaced with a shared secret key.

Gottesman's security criteria can be phrased as follows. Either an eavesdropping Eve is detected with high probability by the receiving Bob, or she does not retain enough information to obtain the message even if she later learns the key. Clearly, it would be impossible to achieve such a goal if there existed a method by which arbitrary quantum states could be cloned: Eve would simply keep a copy of the entire ciphertext.

We refer to such encryption schemes as *quantum tamper-evident encryption schemes* instead of uncloneable encryption schemes. Gottesman himself mentioned the possibly misleading nature of the term "uncloneable":

> "One difficulty with such generalizations is that it is unclear to what extent the name 'uncloneable encryption' is really deserved. I have not shown that a message protected by uncloneable encryption cannot be copied — only that Eve cannot copy it without being detected. Is it possible for Eve to create two states, neither of which will pass Bob's test but which can each be used (in conjunctions with the secret key) to extract a good deal of information about the message?" [Got03]

We note that there is a connection between quantum key distribution and quantum tamper-evident encryption. Gottesman gives a generic way to construct a quantum key distribution protocol from a tamper-evident encryption: simply send a larger key with a tamper-evident encryption scheme.

Quantum tamper-evident encryptions offer an interesting partial solution to the key management problem. If no eavesdropper was detected, Alice and Bob do not need to take great care in keeping their key secret.

Quantum key-recycling. Prior to their groundbreaking work on quantum key distribution, Bennett and Brassard, accompanied by Breidbart, had written a manuscript where a message, encrypted with a one-time-pad, was sent using Wiesner's conjugate coding. This manuscript remained unpublished until it was printed, virtually unchanged and slightly annotated, in celebration of the 30$^{\text{th}}$anniversary of the BB84 protocol [BBB14].

We briefly recall that the one-time-pad is a private-key encryption scheme which offers *perfect secrecy*. This is to say that the ciphertext reveals absolutely no information on the plaintext, even to a computationally unbounded eavesdropper. The one-time-pad does, however, have two major drawbacks. First, the key must be as long as the message. Second, the key can only be used once. Indeed, an eavesdropper who obtains two ciphertext encrypted with the same one-time-pad has obtained a lot of information on both underlying plaintext.

Bennett, Brassard, and Breidbart's core idea was that if a message encrypted using a one-time-pad is sent using Wiesner's conjugate coding scheme, it should be possible to detect an eavesdropping attack. If no eavesdropping is detected, then the key for the one-time-pad could be reused safely. These type of schemes are now known as *quantum key-recycling schemes*.

Quantum key-recycling was rediscovered by Damgågard, Pedersan and Salvail in 2005 [DPS05]. A recent proposal for quantum key recycling by Fehr and Salvail [FS17] could be implemented with technology quite similar to what is necessary to implement quantum key distribution.

In a quantum key-recycling scheme, the receiver of the quantum ciphertext also checks if an eavesdropper obtained information during transmission. If no eavesdropping is detected then a large part of the key can be reused. Unlike the inherently interactive nature of quantum key distribution, only a single bit needs to be communicated by the receiver back to the sender.

Are these two notions related? Quantum key-recycling and tamper-evident encryptions seem quite similar. They are both encryption schemes in which the receiver checks if there was eavesdropping during the transmission. However, their goals are different. In key-recycling, we guarantee that if the verification passes, a portion of the key can be reused with future messages without any loss of secrecy. In tamper evident encryption, we make a guarantee that if the verification passes, the eavesdropper can learn the key without compromising the secrecy of the previously sent message.

It is an open question to precisely relate these two security notions.

1.3 Contributions

In short, this thesis can be seen as offering an initial answer to Gottesman's question from Section 1.2.2.2: Is it possible to construct an encryption scheme with truly uncloneable ciphertexts? Informally, we say that a scheme is uncloneable if the ciphertext produced cannot be used to create two states from which the plaintext could be recovered once the key is announced. We formally define this notion and give a scheme which satisfies it under the assumption that pseudorandom functions are modelled as random oracles.

Our scheme, however, is not quite optimal. If the message is a randomly sampled bit string of length n, we show that the probability that both adversaries obtain the message is upper bounded by $9 \cdot 2^{-n} + \eta(\lambda)$, where $\eta(\lambda)$ can be made arbitrarily small. In an ideal setting, we would obtain an upper bound of $2^{-n} + \eta(\lambda)$. However, for $n \geq 4$, we still obtain something which classical encryption schemes cannot achieve.

Our technical tools are drawn primarily from two sources. First, Tomamichel, Fehr, Kaniewski and Wehner have defined and studied *monogamy-of-entanglement games* [TFKW13]. We discuss how these games can be used to limit the ability of Bob and Charlie to both simultaneously obtain information sent by Alice if she uses Wiesner's conjugate coding scheme. Second, we adapt Unruh's one-way-to-hiding lemma [Unr15] to the two player case. Unruh's lemma can be seen as bounding the probability that that an adversary guesses the output of a random Boolean function on a particular input by the probability of being able to identify that particular input. While this lemma is almost trivial in the classical case, Unruh's contribution was to account for the possibility of an adversary querying the random oracle *in superposition*. Our variation on his lemma bounds the probability that two players can guess the output of a random Boolean function on a particular input by the probability that they can both guess the input.

Chapter 2

Preliminaries

In this chapter, we develop the basic mathematics that will be used throughout this work. In Section 2.1, we fix some notation and recall some common theorems and notions. We review the mathematical formalism of quantum mechanics in Section 2.2. That section also contains a review of the necessary notions concerning linear operators on Hilbert spaces.

2.1 Basic Notation and Notions

2.1.1 Sets and Strings

Definition 2.1.1 (Number Sets)**.**
We define the following sets:

1. *The strictly positive integers are denoted by* $\mathbb{N}^+$*. Specifically,* $0 \notin \mathbb{N}^+$*.*
2. *For any* $n \in \mathbb{N}^+$*, we define* $[n] = \{m \in \mathbb{N}^+ \mid m \leq n\}$ *and* $[n]_0 = [n] \cup \{0\}$*.*
3. *The set of all real numbers is denoted by* $\mathbb{R}$*, the set of strictly positive real numbers by* $\mathbb{R}^+$ *and we also define* $\mathbb{R}_0^+ = \mathbb{R}^+ \cup \{0\}$*.*
4. *The set of complex numbers is denoted by* $\mathbb{C}$*. We also define the complex conjugate of any* $c \in \mathbb{C}$ *by* $\overline{c}$*.*

Definition 2.1.2 (Bit String)**.**
A bit string of length $n \in \mathbb{N}^+$ *is an element of* $\{0,1\}^n$*. We also denote the set of all*

finite length bit strings as $\{0,1\}^*$. *Formally, we have*

$$\{0,1\}^* = \bigcup_{n \in \mathbb{N}^+} \{0,1\}^n. \tag{2.1.1}$$

For any bit string $s \in \{0,1\}^*$, we denote the length of s as $|s| \in \mathbb{N}^+$. In other words, $|s| = n$ if and only if $s \in \{0,1\}^n$.

We typically avoid writing a bit string as a tuple and instead write out each element one after the next. For example, $(1,0,1) = 101 \in \{0,1\}^3$ is a bit string of length 3.

We may also refer to individual bits in a bit string. We do this with an subscript indicating the location of the bit, starting from the left and at 1. For example, for the string $s = 0100$, then $s_2 = 1$. We will use a bolded zero, $\mathbf{0}$, to denote the all zero bit string when the length of the string is clear from context.

Definition 2.1.3 (Exclusive Or)**.**
For any $n \in \mathbb{N}^+$, *the exclusive or (sometimes called "xor") is a binary operator on bit strings,* $\oplus : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, *defined as the element-wise addition mod* 2.

For example, if $n = 5$, we may write

$$(1,1,1,0,0) \oplus (1,0,1,1,0) = 11100 \oplus 10110 = 01010 = (0,1,0,1,0). \tag{2.1.2}$$

The exclusive or also gives a very simple permutation on bit strings.

Lemma 2.1.4.
For all $s \in \{0,1\}^*$, *the mapping* $x \mapsto x \oplus s$ *is a permutation on* $\{0,1\}^{|s|}$.

Definition 2.1.5.
Let $n, m \in \mathbb{N}^+$ *be two positive integers. We denote by* $\mathrm{Bool}(n,m)$ *the set of all functions of the form* $f : \{0,1\}^n \to \{0,1\}^m$.

We use $\mathrm{Bool}(n,m)$ as notation to evoke the notion of Boolean functions. However, we note that Boolean functions are functions of the form $f : \{0,1\}^n \to \{0,1\}$. We slightly extended this notion to consider functions of any output length.

Note that the size of this set is given by $|\mathrm{Bool}(n,m)| = (2^m)^{2^n}$.

2.1.2 Probability Theory

We are often interested in the expectation value of a function evaluated on a uniformly distributed random variable over its domain. In the goal of simplifying our notation, we avoid explicitly defining such a random variable. Instead, we overload the expectation symbol in the following way.

Definition 2.1.6.
Let $\mathcal{X}$ be a finite set and let $f : \mathcal{X} \to \mathbb{R}$ be a function. Then, we write

$$\mathop{\mathbb{E}}_{x} f(x) = \frac{1}{|\mathcal{X}|} \sum_{x \in \mathcal{X}} f(x). \tag{2.1.3}$$

In the case that x is sampled from $\mathcal{X}$ according to the possibly non-uniform random variable X, we write

$$\mathop{\mathbb{E}}_{x \leftarrow X} f(x) = \sum_{x \in \mathcal{X}} \Pr[X = x] \cdot f(x). \tag{2.1.4}$$

We note that this notation also implies that $\sum_{x \in \mathcal{X}} f(x) = |\mathcal{X}| \cdot \mathbb{E}_x f(x)$.

Lemma 2.1.7 (Jensen's Inequality [Jen06])**.**
Let X be a random variable on $\mathbb{R}$ and let $f : \mathbb{R} \to \mathbb{R}$ be a convex function such that both $\mathbb{E}[X]$ and $\mathbb{E}[f(X)]$ exist. Then,

$$f\left(\mathbb{E}[X]\right) \leq \mathbb{E}\left[f(X)\right]. \tag{2.1.5}$$

A corollary gives an analogue statement for concave functions.

Corollary 2.1.1.
Let X be a random variable on $\mathbb{R}$ and let $f : \mathbb{R} \to \mathbb{R}$ be a concave function such that both $\mathbb{E}[X]$ and $\mathbb{E}[f(X)]$ exist. Then,

$$f\left(\mathbb{E}[X]\right) \geq \mathbb{E}\left[f(X)\right]. \tag{2.1.6}$$

We take the time here to demonstrate the use of Jensen's inequality in a particular case using the square root (which is a concave function) and our overloaded notation for the expectation. In fact, almost all of our applications of Corollary 2.1.1 will be in cases covered in the following proposition.

Proposition 2.1.8.
Let $\mathcal{X}$ be a finite set and $f : \mathcal{X} \to \mathbb{R}_0^+$ some function. Then,

$$\mathop{\mathbb{E}}_{x} \sqrt{f(x)} \leq \sqrt{\mathop{\mathbb{E}}_{x} f(x)}. \tag{2.1.7}$$

Proof: Let X be a uniformly distributed random variable over $\mathcal{X}$. Let $Y = f(X)$ be the induced random variable on $\mathbb{R}_0^+$. Since Y has finite support, it is clear that both $\mathbb{E}[Y]$ and $\mathbb{E}[\sqrt{Y}]$ exist. Since the square root is a concave function, we can apply Corollary 2.1.1 to write

$$\mathbb{E}\left[\sqrt{Y}\right] \leq \sqrt{\mathbb{E}[Y]} \implies \mathbb{E}\left[\sqrt{f(X)}\right] \leq \sqrt{\mathbb{E}[f(X)]}. \tag{2.1.8}$$

Finally, we note that

$$\mathbb{E}\left[\sqrt{f(X)}\right] = \frac{1}{|\mathcal{X}|} \sum_{x \in \mathcal{X}} \sqrt{f(x)} = \mathop{\mathbb{E}}_{x} \sqrt{f(x)} \tag{2.1.9}$$

and similarly for $\mathbb{E}[f(X)] = \mathbb{E}_x f(x)$. ∎

Our upcoming security notions are expressed as expectations, explicitly with an expectation over the possible keys and implicitly with an expectation over the randomness of the encryption. There are few tricks that will make the evaluations of these expectations easier. We collect them here.

Proposition 2.1.9.
Let $\mathcal{X}$ be a finite set, $f : \mathcal{X} \to \mathbb{R}$ a function, and $p : \mathcal{X} \to \mathcal{X}$ a permutation. Then,

$$\mathop{\mathbb{E}}_{x} f(x) = \mathop{\mathbb{E}}_{x} f(p(x)). \tag{2.1.10}$$

Proof: It suffices to note that $\sum_{x \in \mathcal{X}} f(x) = \sum_{x \in \mathcal{X}} f(p(x))$. ∎

In particular, it is sometimes possible to move around a permutation when we compute the expectation of a function with multiple arguments. We formalize this in the next proposition.

Proposition 2.1.10.
Let $\mathcal{X}$ be a finite set, $f : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$ a function, and $p : \mathcal{X} \to \mathcal{X}$ a permutation. Then,

$$\mathop{\mathbb{E}}_{x} f(x, p(x)) = \mathop{\mathbb{E}}_{x} f(p^{-1}(x), x). \tag{2.1.11}$$

Proof: Define $g : \mathcal{X} \to \mathbb{R}$ by the function $x \mapsto f(x, p(x))$. Since p^{-1} is also a permutation, applying Proposition 2.1.9 yields

$$\mathop{\mathbb{E}}_{x} f(x, p(x)) = \mathop{\mathbb{E}}_{x} g(x) = \mathop{\mathbb{E}}_{x} g(p^{-1}(x)) = \mathop{\mathbb{E}}_{x} f(p^{-1}(x), x) \tag{2.1.12}$$

which completes the proof. ∎

In our security proofs, we will need to compute the expectation over uniformly sampled boolean functions. However, it will often suffices to fix some particular input x and suppose that H is fixed on all inputs, except x. We then average over the possible values of $H(x)$. We formalize this in the next proposition.

We note that this proposition was implicitly used in Unruh's proof of the one-way-to-hiding lemma [Unr15].

Proposition 2.1.11.
Let $\lambda, n \in \mathbb{N}^+$ be integers and let $x \in \{0,1\}^\lambda$ be a string. For all $H \in \mathrm{Bool}(\lambda, n)$ and all $y \in \{0,1\}^n$, we define $H_{x,y} \in \mathrm{Bool}(\lambda, n)$ by the mapping

$$s \mapsto \begin{cases} H(s) & \text{if } s \neq x \\ y & \text{if } s = x. \end{cases} \tag{2.1.13}$$

Let $f : \mathrm{Bool}(\lambda, n) \to \mathbb{R}$ be a function. Then,

$$\mathop{\mathbb{E}}_{H} f(H) = \mathop{\mathbb{E}}_{H} \mathop{\mathbb{E}}_{y} f(H_{x,y}). \tag{2.1.14}$$

Proof: Consider the set $S = \mathrm{Bool}(\lambda, n) \times \{0,1\}^n$ and the mapping $h : \mathrm{Bool}(\lambda, n) \times \{0,1\}^n \to \mathrm{Bool}(\lambda, n)$ defined by:

$$(H, y) \mapsto H_{x,y} \tag{2.1.15}$$

For any $H \in \text{Bool}(\lambda, n)$, $|h^{-1}(H)| = 2^n$. Indeed, if $(H', y) \in h^{-1}(H)$, then $H'_{x,y} = H$. This implies that $y = H(x)$ and that H' and H have to agree on all strings that are not x. There are precisely 2^n such H', since $H'(x)$ can take 2^n different values. Furthermore, it can be seen that $\{h^{-1}(H)\}_{H \in \text{Bool}(\lambda,n)}$ forms a disjoint covering of S. Using these facts, we may write:

$$\begin{aligned}
\mathop{\mathbb{E}}_{H} f(H) &= \mathop{\mathbb{E}}_{H} \frac{1}{2^n} \sum_{(H',y) \in h^{-1}(H)} f(H_{x,y}) \\
&= \frac{1}{2^{n2^\lambda}} \frac{1}{2^n} \sum_{H \in \text{Bool}(\lambda,n)} \sum_{(H',y) \in h^{-1}(H)} f(H'_{x,y}) \\
&= \frac{1}{2^{n2^\lambda}} \frac{1}{2^n} \sum_{(H',y) \in S} f(H'_{x,y}) \\
&= \mathop{\mathbb{E}}_{H} \mathop{\mathbb{E}}_{y} f(H_{x,y})
\end{aligned} \tag{2.1.16}$$

which concludes the proof. ∎

2.1.3 Negligible Functions

What does it mean for something to be "small"?

Looking ahead a bit, we realize that it is sometimes unreasonable to expect "perfect security", whatever that may mean, from cryptographic protocols. Thus, we typically accept a failure probability that can be made arbitrarily small.

So, we suppose that our protocol is parametrized by a certain integer $\lambda \in \mathbb{N}^+$ called the security parameter. We say that λ is a security parameter in the sense that as it takes larger and larger values, the probability of failure becomes smaller and smaller. In fact, we require that the probability of failure becomes small "fast enough". Specifically, the probability of failure should be a negligible function of the security parameter.

Definition 2.1.12 (Negligible Function)**.**
A function $f : \mathbb{N}^+ \to \mathbb{R}_0^+$ is negligible if for all positive polynomials $p : \mathbb{N}^+ \to \mathbb{R}_0^+$

there exists an integer $n_p \in \mathbb{N}$ *such that*

$$n \geq n_p \implies f(n) < \frac{1}{p(n)}. \tag{2.1.17}$$

For this work, we will need to know that one particular form of function is negligible.

Definition 2.1.13 (Polynomially Bounded Function)**.**
A function $f : \mathbb{N}^+ \to \mathbb{R}_0^+$ *is said to be* polynomially bounded *if there exists a polynomial* $p : \mathbb{N}^+ \to \mathbb{R}_0^+$ *such that* $f(n) \leq p(n)$ *for all* $n \in \mathbb{N}^+$*.*

Lemma 2.1.14.
Let $f : \mathbb{N}^+ \to \mathbb{R}^+$ *be a polynomially bounded function and* $c \in \mathbb{R}^+$ *a positive constant strictly smaller than* 1*. Then, the function* $g : \mathbb{N}^+ \to \mathbb{R}_0^+$ *defined by*

$$n \mapsto f(n)c^n \tag{2.1.18}$$

is a negligible function.

2.1.4 Vector Spaces

We suppose that the reader is familiar with the notion of vector spaces. However, we review the notions of inner products, norms, linear operators as well as the Dirac notation. Once again, this is mainly to fix notation and to make explicit the facts that will be used later.

We assume that all vector spaces are of finite dimension and over $\mathbb{C}$.

2.1.4.1 Inner Products and Norms

We recall the notion of an inner product on a vector space. We adopt the convention that the inner product is linear in the second, and not the first, argument. This convention is common in physics and, in particular, in quantum mechanics.

Definition 2.1.15 (Inner Product)**.**
Let V *be a vector space. A function* $f : V \times V \to \mathbb{C}$ *is said to be an* inner product *on* V *if, for all* $v, w, z \in V$ *and all* $s \in \mathbb{C}$*, we have that*

1. $f(v, w) = \overline{f(w, v)}$
2. f *is linear in the second argument, which is to say that*
   (a) $f(v, w + z) = f(v, w) + f(v, z)$ *and*
   (b) $f(v, s \cdot w) = s \cdot f(v, w)$,
3. $f(v, v) \in \mathbb{R}_0^+$, *and*
4. $f(v, v) = 0 \iff v = 0$.

Note that the above also implies that $f(s \cdot v, w) = \overline{s} \cdot f(v, w)$, *which we describe by saying that* f *is conjugate-linear in its first argument.*

If f *is an inner product, we say that* (V, f) *is an inner product space.*

It is common to denote the inner product as a binary operator instead of a function. Specifically, if (V, f) is an inner product space, we may write

$$f(v, w) = \langle v, w \rangle \tag{2.1.19}$$

for any $v, w \in V$.

If V is a vector space, then any inner product f on V induces a norm on V.

Definition 2.1.16 (Norm)**.**
Let V *be a vector space. A function* $g : V \to \mathbb{R}_0^+$ *is said to be a* norm *on* V *if, for all* $v, w \in V$ *and all* $s \in \mathbb{C}$, *we have that*

1. $g(v) = 0 \iff v = 0$,
2. $g(v + w) \leq g(v) + g(w)$, *which is to say that* g *satisfies the triangle inequality, and*
3. $g(s \cdot v) = |s| \cdot g(v)$.

If g *is a norm on a vector space, we say that* (V, g) *is a normed vector space.*

Lemma 2.1.17.
Let (V, f) *be an inner product space. Then,* $v \mapsto \sqrt{f(v, v)}$ *is a norm on* V. *We call this function the* induced norm.

It is common to denote the norm as a unary operator instead of a function. Specifically, if (V, g) is a normed vector space, we may write

$$g(v) = \|v\| \tag{2.1.20}$$

for all $v \in V$.

Unless otherwise specified, a norm on an inner product space is assumed to be the induced norm.

Definition 2.1.18 (Orthonormal Basis)**.**
Let (V, f) be an inner product space. We say that a basis $B = \{b_i\}_{i \in I}$ is an orthonormal basis *if and only if $\|b_i\| = 1$ and $\langle b_i, b_j \rangle = 0$ for all $b_i, b_j \in B$ with $i \neq j$.*

Theorem 2.1.19 (The Cauchy-Schwarz Inequality)**.**
Let (V, f) be an inner product space. Then, for all $u, v \in V$, we have:

$$|\langle u, v \rangle| \leq \|u\| \cdot \|v\| \tag{2.1.21}$$

We also recall that the canonical inner product on $\mathbb{C}^n$ is given by

$$\langle v, w \rangle = \sum_{i=1}^{n} \overline{v_i} \cdot w_i \tag{2.1.22}$$

where v_i (respectively, w_i) is the i^{th} coordinate of v (respectively, w) in any fixed orthonormal basis. We emphasize, but do not prove, that this inner product is independent of the particular orthonormal basis used.

2.1.4.2 Linear Operators

Definition 2.1.20 (Set of Linear Operators)**.**
Let V and W be two vector spaces. We denote by $\mathcal{L}(V, W)$ the set of all linear operators $L : V \to W$. We also write $\mathcal{L}(V, V) = \mathcal{L}(V)$.

Following convention, we may omit the use of parentheses when applying a linear operator to a vector and write

$$L(v) = Lv. \tag{2.1.23}$$

Linear operators may be composed to obtain other linear operators. In particular, if $L \in \mathcal{L}(V, W)$ and $L' \in \mathcal{L}(W, X)$, then $L' \circ L = L'L \in \mathcal{L}(V, X)$.

We note that $\mathcal{L}(V, W)$ is itself a vector space with natural operations of addition and scalar multiplication give by

$$(s \cdot L')\, v = s \cdot (Lv) \qquad \text{and} \qquad (L + L')v = Lv + L'v \tag{2.1.24}$$

for all $L, L' \in \mathcal{L}(V, W)$, all $v \in V$, and all $s \in \mathbb{C}$.

Finally, for any vector space V, we define the identity operator $\mathbb{1} \in \mathcal{L}(V)$. This operator satisfies $\mathbb{1}v = v$ for all $v \in V$.

For any two normed vector spaces V and W, we can define a particular norm on the space of linear operators $\mathcal{L}(V, W)$ called the operator norm. This norm measures the maximal effect that the operator can have on the norm of a vector on which it is applied.

Theorem 2.1.21.
For any normed vector spaces V and M, the function

$$L \mapsto \max_{v \in V} \frac{\|Lv\|_W}{\|v\|_V} \tag{2.1.25}$$

is a norm on $\mathcal{L}(V, W)$ which we will call the operator norm.

We emphasize two properties of the operator norm. First, if $L \in \mathcal{L}(V, W)$ and $M \in \mathcal{L}(W, X)$ are operators on normed vector spaces, then

$$\|ML\| \leq \|M\| \cdot \|L\|. \tag{2.1.26}$$

Second, for any vector $v \in V$, we have that

$$\|Lv\| \leq \|L\| \cdot \|v\|. \tag{2.1.27}$$

Finally, we recall the definition of the dual of a vector space.

Definition 2.1.22 (Dual of a Vector Space)**.**
Let V be a vector space. Then, $V' = \mathcal{L}(V, \mathbb{C})$ is called the dual of V.

If (V, f) is an inner product space, then we can naturally associate to each element of V and element of V'. We do this via the mapping $v \mapsto \phi_v$ where $\phi_v \in \mathcal{L}(V, \mathbb{C})$ is the function defined by

$$w \mapsto f(v, w). \tag{2.1.28}$$

2.1.4.3 Dirac Notation

The *Dirac notation*, also known as the *bra-ket notation*, is a common notational scheme for inner product spaces used in quantum mechanics which we will adopt. For the remainder of this discussion, we assume that (V, f) is an inner product space.

At the core of this scheme is the notion of a ket, identified with the symbol

$$|\cdot\rangle\,. \tag{2.1.29}$$

In general, a ket is simply a "decoration" around a symbol. A symbol adorned with this decoration denotes an element a vector space V. In other words, $|\psi\rangle \in V$. To denote different vectors, we may use different symbols inside of this decoration. Thus, in general, we have that

$$|\psi\rangle \neq |\phi\rangle\,. \tag{2.1.30}$$

We may now introduce the bra, identified with the symbol

$$\langle\cdot|\,. \tag{2.1.31}$$

For any vector $|\psi\rangle \in V$, the bra $\langle\psi|$ is the element in the dual space of V corresponding to $|\psi\rangle$. In other words, $\langle\psi| = \phi_{|\psi\rangle} \in V' = \mathcal{L}(V, \mathbb{C})$ is the linear operator defined by

$$|\phi\rangle \mapsto |\psi\rangle\langle\phi|\,. \tag{2.1.32}$$

Let $|\psi\rangle\,, |\phi\rangle$ be two vectors in our inner product space (V, f). We may then write

$$f(|\psi\rangle\,, |\phi\rangle) = \langle\psi|\,|\phi\rangle = \langle\psi|\phi\rangle \tag{2.1.33}$$

where the first equality follows from the definition of the bra and the second equality is a notational shorthand.

It may be convenient to identify vectors $|\psi\rangle \in V$ as linear operators $|\psi\rangle \in \mathcal{L}(\mathbb{C}, V)$ defined by the mapping $s \mapsto s \cdot |\psi\rangle$. This identification then allows us to naturally

interpret the expression

$$|\psi\rangle\langle\phi| \tag{2.1.34}$$

as a linear operator in $\mathcal{L}(V)$ since it is the composition of an operator in $\mathcal{L}(V,\mathbb{C})$ and an operator in $\mathcal{L}(\mathbb{C},V)$.

With all this notation, we can write equations such as

$$\underbrace{|\psi\rangle\langle\phi|}_{\text{Operator}} \overbrace{|\varphi\rangle}^{\text{Vector}} = \underbrace{\langle\phi|\varphi\rangle}_{\text{Scalar}} \overbrace{|\psi\rangle}^{\text{Vector}} \tag{2.1.35}$$

for any vectors $|\psi\rangle, |\phi\rangle, |\varphi\rangle \in V$. Of course, both sides of this equation represent the same vector in V.

Finally, we note that if the set of vectors $\{|b_i\rangle\}_{i\in I}$ forms a basis of the vector space V, then the set of operators $\{|b_i\rangle\langle b_j|\}_{i,j\in I}$ forms a basis for $\mathcal{L}(V)$.

2.2 Mathematics of Quantum Mechanics

It is common (e.g.: [SC94]) to introduce a newcomer to quantum mechanics in two steps. First, an experiment is discussed where the classical predictions do not match the experimental data. Once they are convinced that something is lacking in the classical analysis of the experiment, they are introduced to a series of postulates which define a framework in which a better analysis of the experiment in question is possible. This framework is quantum mechanics.

We skip the discussion of an experiment (but point to the Stern-Gerlash experiment as the usual example) and immediately discuss the postulates. We may consider these postulates as the axioms of quantum mechanics. We adopt a form of the postulates which are more directly applicable to quantum information and cryptography. These may be found in [NC10].

We also define and develop the relevant mathematical notions as the postulates call for them. Thus, this section also covers the necessary preliminaries for linear operators on Hilbert spaces. We take our definitions from the excellent discussion given in [Wat18].

2.2.1 First Postulate: Describing Quantum Systems

P1. (a) To every physical system is associated a complex Hilbert space $\mathcal{H}$ called the *state space* of the system.

(b) If the system is isolated, then its state at any given time is completely described by a single vector of norm 1, $|\psi\rangle \in \mathcal{H}$, in this space.

We quickly recall the definition of a complex Hilbert space.

Definition 2.2.1 (Complex Hilbert Space)**.**
A complex Hilbert space $\mathcal{H}$ is an inner product space over the field $\mathbb{C}$ which is complete with respect to the metric induced by its inner product.

In general quantum systems may have state spaces of infinite dimensions. However, in this work, we assume that all Hilbert spaces are finite dimensional. In particular, this lets us ignore all the discussion of completeness from the above definition as all finite dimensional Hilbert spaces are complete.

Definition 2.2.2 (Pure State)**.**
Let $\mathcal{H}$ be a Hilbert space. A pure state *in $\mathcal{H}$ is a vector of norm* 1*.*

The reason for the adjective "pure" will become clear once we reach Section 2.2.6.3. Until then and when the context is clear, we refer to "pure states" as simply "states".

For any finite dimensional complex Hilbert space $\mathcal{H}$, there is an integer $n \in \mathbb{N}^+$ such that $\mathcal{H}$ is isomorphic to $\mathbb{C}^n$ with the canonical inner product. Thus, for the remainder of this work, we can assume that all Hilbert spaces are of the form $\mathbb{C}^n$ for a certain n. Note that this implies that every linear operator between Hilbert spaces can be represented by a matrix. We will rarely use these facts but keeping them in mind can help maintain an intuitive understanding of the underlying mathematics.

In analogy to the classical bit, which may only be in one of two states, we call any quantum system with a 2 dimensional state space a *qubit*.

Definition 2.2.3 (State Space of a Qubit)**.**
We denote the Hilbert space $\mathbb{C}^2$ by $\mathcal{Q}$. We assume that $\mathcal{Q}$ admits $\{|0\rangle, |1\rangle\}$ as an orthonormal basis and call this the computational basis of $\mathcal{Q}$.

2.2.2 Second Postulate: Combining Quantum Systems

P2. A physical system composed of two sub-systems, each with respective state spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, has a state space given by the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$.

A formal construction of the tensor product can be found in [Wat18]. We simply recall the facts that will be necessary for this work.

1. $\mathcal{H}_A \otimes \mathcal{H}_B$ is a complex vector space whose elements are called *tensors*.

2. For any vectors $|\psi\rangle_A \in \mathcal{H}_A$ and $|\phi\rangle_B \in \mathcal{H}_B$, $|\psi\rangle_A \otimes |\phi\rangle_B$ is an element of $\mathcal{H}_A \otimes \mathcal{H}_B$. Elements of this form are called *elementary tensors* and they span $\mathcal{H}_A \otimes \mathcal{H}_B$, which is to say that

$$\mathcal{H}_A \otimes \mathcal{H}_B = \mathrm{Span}\{|\psi\rangle_A \otimes |\phi\rangle_B \mid |\psi\rangle_A \in \mathcal{H}_A \text{ and } |\phi\rangle_B \in \mathcal{H}_B\}. \tag{2.2.1}$$

3. For any vectors $|a_0\rangle, |a_1\rangle \in \mathcal{H}_A$, $|b_0\rangle, |b_1\rangle \in \mathcal{H}_B$ and any scalar $s \in \mathbb{C}$, we identify the following elements of $\mathcal{H}_A \otimes \mathcal{H}_B$:

   - $\big(|a_0\rangle + |a_1\rangle\big) \otimes |b_0\rangle = \big(|a_0\rangle \otimes |b_0\rangle\big) + \big(|a_1\rangle \otimes |b_0\rangle\big)$
   - $|a_0\rangle \otimes \big(|b_0\rangle + |b_1\rangle\big) = \big(|a_0\rangle \otimes |b_0\rangle\big) + \big(|a_0\rangle \otimes |b_1\rangle\big)$
   - $s \cdot \big(|a_0\rangle \otimes |b_0\rangle\big) = \big(s \cdot |a_0\rangle\big) \otimes |b_0\rangle = |a_0\rangle \otimes \big(s \cdot |b_0\rangle\big)$

4. The inner product on $\mathcal{H}_A \otimes \mathcal{H}_B$ is defined on elementary tensors by the function

$$\big(|a_0\rangle \otimes |b_0\rangle, |a_1\rangle \otimes |b_1\rangle\big) \mapsto \langle a_0|a_1\rangle \cdot \langle b_0|b_1\rangle \tag{2.2.2}$$

   and extended to all other elements of $\mathcal{H}_A \otimes \mathcal{H}_B$ by linearity in the second argument and conjugate-linearity in the first.

In particular, this definition of the inner product on $\mathcal{H}_A \otimes \mathcal{H}_B$ implies that the norm of elementary tensors is the product of the norms. This is to say that

$$\||\psi\rangle_A \otimes |\phi\rangle_B\| = \||\psi\rangle_A\| \cdot \||\phi\rangle_B\| \tag{2.2.3}$$

for any vectors $|\psi\rangle \in \mathcal{H}_A$ and $|\phi\rangle \in \mathcal{H}_B$.

It can be deduced from these facts that if $\{|a_i\rangle\}_{i\in I}$ and $\{|b_i\rangle\}_{j\in J}$ are orthonormal bases of $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, then $\{|a_i\rangle \otimes |b_j\rangle\}_{i\in I, j\in J}$ forms an orthonormal basis

of $\mathcal{H}_A \otimes \mathcal{H}_B$. In particular, the dimension of the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is the product of the dimensions of the $\mathcal{H}_A$ and $\mathcal{H}_B$. Thus, if $\mathcal{H}_A$ and $\mathcal{H}_B$ are isomorphic to $\mathbb{C}^n$ and to $\mathbb{C}^m$, respectively, then $\mathcal{H}_A \otimes \mathcal{H}_B$ is isomorphic to $\mathbb{C}^{n \cdot m}$.

As can be seen above, we will sometimes use the same subscript to identify a particular Hilbert space, the vectors on that Hilbert space, and linear operators on that Hilbert space.

We also define a tensor product for linear operators.

Definition 2.2.4.
Let $\mathcal{H}_A$, $\mathcal{H}_{A'}$, $\mathcal{H}_B$, $\mathcal{H}_{B'}$ be Hilbert spaces. Consider linear operators $L_A \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_{A'})$ and $L_B \in \mathcal{L}(\mathcal{H}_B, \mathcal{H}_{B'})$. Then, $L_A \otimes L_B \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B, \mathcal{H}_{A'} \otimes \mathcal{H}_{B'})$ is the linear operator defined by

$$|a_i\rangle \otimes |b_j\rangle \mapsto (L_A |a_i\rangle) \otimes (L_B |b_i\rangle) \tag{2.2.4}$$

for any bases $\{|a_i\rangle\}_{i \in I}$, $\{|b_j\rangle\}_{j \in J}$ of $\mathcal{H}_A$, $\mathcal{H}_B$ respectively and extended linearly to all other elements of $\mathcal{H}_A \otimes \mathcal{H}_B$.

It can be shown that the tensor product of linear operators satisfies the same identifications as vectors. Moreover, the operator norm of a tensor product is the product of the operator norms, which is to say that $\|L \otimes L'\| = \|L\| \cdot \|L'\|$.

We will sometimes omit the identity operator in the tensor product of linear operators. In particular, if $L_A \in \mathcal{L}(\mathcal{H}_A)$ is a linear operator, we will also write L_A to represent $L_A \otimes \mathbb{1}_B \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ when the context is clear.

Finally, the ordering of the tensor product will not matter much to us. If we consider three Hilbert spaces $\mathcal{H}_A$, $\mathcal{H}_B$, and $\mathcal{H}_C$ and $L \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_C)$is a linear operator which, for some particular vectors, satisfies $L_{AC} |a\rangle \otimes |c\rangle = |a'\rangle \otimes |c'\rangle$, then:

$$(L_{AC} \otimes \mathbb{1}_B) (|a\rangle_A \otimes |b\rangle_B \otimes |c\rangle_C) = |a'\rangle_A \otimes |b\rangle_B \otimes |c'\rangle_C \tag{2.2.5}$$

We will, however, try to maintain a consistent ordering in our tensor products.

We sometimes omit the tensor symbol when used with vectors and write

$$|a\rangle \otimes |b\rangle = |a\rangle |b\rangle . \tag{2.2.6}$$

For elements of the computational basis of $\mathcal{Q}$, we will sometimes combine them into

the same ket to have

$$|0\rangle \otimes |1\rangle = |0\rangle\,|1\rangle = |01\rangle \in \mathcal{Q} \otimes \mathcal{Q} \tag{2.2.7}$$

Finally, we introduce some notation for the state space of multiple qubits, which is simply the result of the tensor product of the appropriate number of $\mathcal{Q}$.

Definition 2.2.5 (State Space of Multiple Qubits)**.**
For all $n \in \mathbb{N}^+$, we define

$$\mathcal{Q}(n) = \underbrace{\mathcal{Q} \otimes \cdots \otimes \mathcal{Q}}_{n \text{ instances of } \mathcal{Q}} = \mathcal{Q}^{\otimes n} \tag{2.2.8}$$

to be the state space of n qubits.

For every $n \in \mathbb{N}^+$, we will freely make use of the correspondence between bit strings of length n and elements of the computational basis of $\mathcal{Q}(n)$.

2.2.3 Third Postulate: The Evolution of Quantum Systems

P3. The evolution of a closed quantum system is described by unitary operators.

To properly interpret this postulate, we need a few more mathematical notions concerning linear operators on Hilbert spaces.

Definition 2.2.6 (Adjoint Operator)**.**
Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two Hilbert spaces and let $L \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$ be a linear operator. The adjoint *of L is the unique linear operator $L^\dagger \in \mathcal{L}(\mathcal{H}_B, \mathcal{H}_A)$ such that for all vectors $|\psi\rangle \in \mathcal{H}_B$, the dual of $L^\dagger\,|\psi\rangle \in \mathcal{H}_A$ is given by $\langle\psi|\,L \in \mathcal{L}(\mathcal{H}_A, \mathbb{C})$.*

In other words, the adjoint operator of L is the unique linear operator $L^\dagger$ such that

$$\langle u, Lv\rangle = \langle L^\dagger u, v\rangle \tag{2.2.9}$$

for all vectors $v \in \mathcal{H}_A$ and $u \in \mathcal{H}_B$.

For any operators A, B, $(AB)^\dagger = B^\dagger A^\dagger$, $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$ and $\left(A^\dagger\right)^\dagger = A$. Furthermore, if $A = A^\dagger$, then A is said to be *self-adjoint*.

Definition 2.2.7 (Unitary Operators)**.**
Let $\mathcal{H}$ be a Hilbert space. An operator $U \in \mathcal{L}(\mathcal{H})$ is said to be unitary *if and only if*

$$U^\dagger U = UU^\dagger = \mathbb{1}_{\mathcal{H}}. \tag{2.2.10}$$

The set of all unitary operators on $\mathcal{H}$ is denoted by $\mathcal{U}(\mathcal{H})$.

We note that the identity is a unitary operator and that if U_1 and U_2 are unitary operators, then so is $U_1 \otimes U_2$ and $U_1^\dagger$. Also note that if $\{|b_i\rangle\}_{i\in I}$ forms an orthonormal basis of a Hilbert space $\mathcal{H}$ and $U \in \mathcal{U}(\mathcal{H})$ is a unitary operator, then $\{U|b_i\rangle\}_{i\in I}$ also forms an orthonormal basis of this space. Finally, we have that the operator norm of any unitary operator is one, which is to say that $\|U\| = 1$.

Thus, the second postulate tells us that if an isolated quantum system undergoes some evolution, its final state will be of the form $U|\psi\rangle$ where U is the unitary operator defined by the evolution and $|\psi\rangle$ is the initial state of the system. In particular, U is independent of the initial state $|\psi\rangle$.

A noteworthy unitary operator is the Hadamard operator.

Definition 2.2.8.
The Hadamard operator is the unitary operator $H \in \mathcal{U}(\mathcal{Q})$ defined on the computational basis as

$$|0\rangle \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad |1\rangle \mapsto \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{2.2.11}$$

and extended linearly to all other vectors. We define $|+\rangle = H|0\rangle$ and $|-\rangle = H|1\rangle$.

We note that $\{|+\rangle, |-\rangle\}$ also forms an orthonormal basis for $\mathcal{Q}$ and we call this basis the Hadamard basis. Moreover, the Hadamard operator is self-adjoint, $H^\dagger = H$, and self-inverse, $H^2 = \mathbb{1}$.

Definition 2.2.9 (Wiesner States)**.**
Let $n \in \mathbb{N}^+$. For any two strings $x, \theta \in \{0,1\}^n$, we define

$$\left|x^\theta\right\rangle = \bigotimes_{i=1}^{n} H^{\theta_i} |x_i\rangle \in \mathcal{Q}(n) \tag{2.2.12}$$

where $H^1 = H$ is the Hadamard operator and $H^0 = \mathbb{1}$ is the identity. We call vectors

of this form Wiesner states.

For example, if $x = 011$ and $\theta = 110$, then:

$$\left|x^{\theta}\right\rangle = \left(H^1 \left|0\right\rangle\right) \otimes \left(H^1 \left|1\right\rangle\right) \otimes \left(H^0 \left|1\right\rangle\right) = \left|+\right\rangle \left|-\right\rangle \left|1\right\rangle \in \mathcal{Q}(3) \tag{2.2.13}$$

For any $\theta \in \{0,1\}^n$, $\left\{\left|s^{\theta}\right\rangle\right\}_{s\in\{0,1\}^n}$ forms an orthonormal basis of $\mathcal{Q}(n)$. This follows from the fact that $\bigotimes_{i=1}^{n} H^{\theta_i}$ is a unitary operator and a unitary operators maps any orthonormal basis (such as the computational basis) to another orthonormal basis.

Wiesner states are often referred to as *BB84 states* in the literature. This is a bit of a misnomer as Wiesner's use of these states [Wie83] predates, and in fact inspired, their use by Bennett and Brassard [BB84].

Wiesner's conjugate coding is the process of picking some $\theta \in \{0,1\}^n$ and to encode a bit string $x \in \{0,1\}^n$ as the state $\left|x^{\theta}\right\rangle$. Specifically, the conjugate coding of the string x in the base θ refers to the state $\left|x^{\theta}\right\rangle$.

The use of θ seems to suggest the notion of an angle. This is in reference to many implementations of Wiesner's conjugate coding where photons are sent in one of four different polarizations. The θ symbolically relates to the angle of the polarization.

2.2.4 Fourth Postulate: Measuring Quantum Systems

P4. A measurement $\mathcal{M}$ on a quantum system with state space $\mathcal{H}$ is defined by a collection of linear operators on $\mathcal{H}$ indexed by a finite set, $\mathcal{M} = \{M_i\}_{i\in I}$, and satisfying:

$$\sum_{i\in I} M_i^{\dagger} M_i = \mathbb{1}_{\mathcal{H}} \tag{2.2.14}$$

If the system is in the state $|\psi\rangle \in \mathcal{H}$ when the measurement $\mathcal{M}$ is made, then, with probability

$$p_i = \langle\psi|M_i^{\dagger} M_i|\psi\rangle = \left\|M_i \left|\psi\right\rangle\right\|^2 \tag{2.2.15}$$

the quantum system adopts the state

$$\frac{M_i \left|\psi\right\rangle}{\sqrt{p_i}} \tag{2.2.16}$$

and the measurement outputs i as a result.

An important class of measurements are *projective* measurements. To properly introduce these measurements, we need a few more definitions.

Definition 2.2.10 (Positive Semidefinite Operator)**.**
Let $\mathcal{H}$ be a Hilbert space. An operator $P \in \mathcal{L}(\mathcal{H})$ is said to be positive semidefinite if and only if there exists a $Q \in \mathcal{L}(\mathcal{H})$ such that

$$P = Q^\dagger Q. \tag{2.2.17}$$

The set of all positive semidefinite operators on $\mathcal{H}$ is denoted by $\mathcal{P}(\mathcal{H})$.

Note that all positive semidefinite operators are self-adjoint since $(Q^\dagger Q)^\dagger = Q^\dagger Q$. Positive semidefinite operators may also be characterized in another way.

Lemma 2.2.11.
Let $\mathcal{H}$ be a Hilbert space. An operator $P \in \mathcal{L}(\mathcal{H})$ is positive semidefinite if and only if $\langle\psi| P |\psi\rangle \in \mathbb{R}_0^+$ for all $|\psi\rangle \in \mathcal{H}$.

Definition 2.2.12 (Projector)**.**
Let $\mathcal{H}$ be a Hilbert space. A projector *is a positive semidefinite operator $P \in \mathcal{P}(\mathcal{H})$ which satisfies*

$$P^2 = P. \tag{2.2.18}$$

There are a handful of properties concerning projectors which we will need.

If $|\psi\rangle \in \mathcal{H}$, then $|\psi\rangle\langle\psi| \in \mathcal{P}(\mathcal{H})$. Indeed, we note that $|\psi\rangle\langle\psi| \, |\psi\rangle\langle\psi| = 1 \cdot |\psi\rangle\langle\psi|$ and that for all $|\phi\rangle \in \mathcal{H}$, we have that

$$\langle\phi| \, |\psi\rangle\langle\psi| \, |\phi\rangle = \langle\phi|\psi\rangle \, \langle\psi|\phi\rangle = |\langle\phi|\psi\rangle|^2 \geq 0. \tag{2.2.19}$$

We also have that the identity is a projector and that if P_A and P_B are projectors on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, then $P_A \otimes P_B$ is a projector on $\mathcal{H}_A \otimes \mathcal{H}_B$. Finally, $\mathbb{1} - P_A$ is also projector.

If P is a projector on $\mathcal{H}$ and $U \in \mathcal{U}(\mathcal{H})$ is a unitary operator, then $UPU^\dagger$ is also a projector.

An important class of measurements are the projective measurements.

Definition 2.2.13 (Projective Measurement)**.**
Let $\mathcal{H}$ be a Hilbert space. A projective measurement is a finite collection of projective operators $\mathcal{M} = \{P_i\}_{i\in I}$ such that $\sum_{i\in I} P_i = \mathbb{1}_{\mathcal{H}}$.

Noting that $P_i = P_i^\dagger$ (since $P_i \in \mathcal{P}(\mathcal{H})$), it is easy to see that projective measurements are indeed measurements as defined by the fourth postulate.

We also note that if $\mathcal{M} = \{P_i\}_{i\in I}$ is a projective measurement on $\mathcal{H}$, then for any two vectors $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ and any two distinct $i, j \in I$, then $P_i |\psi\rangle$ and $P_j |\phi\rangle$ are orthogonal vectors. Specifically, the elements of $\mathcal{M}$ all project on mutually orthogonal states.

A particular type of projective measurement is the measurement "in a basis". If the set $B = \{|b_i\rangle\}_{i\in I}$ forms an orthonormal basis of the Hilbert space $\mathcal{H}$, then we refer to $\{|b_i\rangle\langle b_i|\}_{i\in I}$ as the measurement in the B basis.

We also define another class of measurements, the *positive operator valued measurements*.

Definition 2.2.14 (Positive Operator-Valued Measurement)**.**
Let $\mathcal{H}$ be a Hilbert space. A positive operator-valued measurement (POVM) is a finite collection of positive semidefinite operators $\mathcal{M} = \{A_i\}_{i\in I}$ such that $\sum_{i\in I} A_i = \mathbb{1}_{\mathcal{H}}$.

Strictly speaking, this is *not* a measurement as defined by the fourth postulate. The operators in a POVM are not required to satisfy $\sum_{i\in I} A^\dagger A_i = \mathbb{1}_{\mathcal{H}}$. However, there exists linear operators M_i such that $A_i = M_i^\dagger M_i$ for all A_i since these are positive semi-definite. Then, the set $\{M_i\}_{i\in I}$ forms a proper measurement as described in the fourth postulate.

Why would we be interested in POVMs if they only give part of the picture? As mentioned in [NC10], they are simpler to manipulate then the measurements defined in the postulate as we do not need to consider their adjoints. If we are only interested in the probability of a certain outcome, and not the resulting state after the measurement, the A_i operators are sufficient. Indeed, we have

$$p_i = \langle\psi| A_i |\psi\rangle . \tag{2.2.20}$$

Note that due to the fact that projectors are both self-adjoint and idempotent, a projective measurement is also a POVM.

2.2.5 Entanglement

There is a simple mathematical definition for the notion of *entanglement*.

Definition 2.2.15 (Separable and Entangled States)**.**
Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two Hilbert spaces. A state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is said to be separable *with respect to $\mathcal{H}_A$ and $\mathcal{H}_B$ if and only if there exist states $|\phi\rangle \in \mathcal{H}_A$ and $|\varphi\rangle \in \mathcal{H}_B$ such that:*

$$|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\varphi\rangle_B \tag{2.2.21}$$

A state without such a representation is entangled with respect to $\mathcal{H}_A$ and $\mathcal{H}_B$.

The precise meaning and interpretation of the entanglement of two physical systems is beyond the scope of this thesis. However, we note that entangled states give rise to correlated measurement results.

Perhaps the most recognizable entangled state is the EPR state, named with the initials of Einstein, Podolsky, and Rosen who studied physical systems with such states [EPR35].

Definition 2.2.16 (Einstein-Podolsky-Rosen state)**.**
The Einstein-Podolsky-Rosen state*, or* EPR state*, is given by*

$$|EPR\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \in \mathcal{Q} \otimes \mathcal{Q}. \tag{2.2.22}$$

A bipartite physical system in the EPR state is often called an *EPR pair*.

We note that if both subsystems of an EPR pair are each measured in the computational basis, the measurement outcomes will always be the same. In other words, it is impossible for the measurement on one half to return 0 and the measurement on another half to return 1.

This can be seen by observing that

$$\left\| \left(|0\rangle\langle 0| \otimes |0\rangle\langle 0| \right) |\mathrm{EPR}\rangle \right\|^2 = \left\| \left(|1\rangle\langle 1| \otimes |1\rangle\langle 1| \right) |\mathrm{EPR}\rangle \right\|^2 = \frac{1}{2} \tag{2.2.23}$$

and

$$\left\| \left(|0\rangle\langle 0| \otimes |1\rangle\langle 1| \right) |\mathrm{EPR}\rangle \right\|^2 = \left\| \left(|1\rangle\langle 1| \otimes |0\rangle\langle 0| \right) |\mathrm{EPR}\rangle \right\|^2 = 0. \tag{2.2.24}$$

This type of correlation in the results of measurements performed on distinct

subsystems of quantum states is, in a sense, a signature that the quantum state was entangled.

There is a natural generalization of the EPR state to any 2λ qubits.

Definition 2.2.17.
Let $\lambda \in \mathbb{N}^+$. We define

$$|EPR_\lambda\rangle = \frac{1}{\sqrt{2^\lambda}} \sum_{s\in\{0,1\}^\lambda} |s\rangle\,|s\rangle \in \mathcal{Q}(\lambda) \otimes \mathcal{Q}(\lambda). \tag{2.2.25}$$

The following facts are implicitly used in many quantum information proofs which use EPR pairs. We will use it ourselves later in the proof of Corollary 3.4.1 and its usefulness will be more apparent in the context of that theorem.

Lemma 2.2.18.
For all $\lambda \in \mathbb{N}^+$ and all $\theta \in \{0,1\}^\lambda$, we have that

$$|EPR_\lambda\rangle = \frac{1}{\sqrt{2^\lambda}} \sum_{s\in\{0,1\}^\lambda} \left|s^\theta\right\rangle \left|s^\theta\right\rangle \tag{2.2.26}$$

where $\left|s^\theta\right\rangle$ is as defined in Definition 2.2.9, i.e., $\left|s^\theta\right\rangle = \bigotimes_{i=1}^{\lambda} H^{\theta_i} |s_i\rangle$.

Proof: It suffices to show that

$$\sum_{s\in\{0,1\}^\lambda} \left|s^\theta\right\rangle \left|s^\theta\right\rangle = \sum_{s\in\{0,1\}^\lambda} |s\rangle\,|s\rangle \tag{2.2.27}$$

We proceed by induction on λ.

We first show that this identity holds for $\lambda = 1$. We note that in this case, there only two possible values for θ: 1 or 0. Thus, it suffices to note that

$$\begin{aligned} |{+}{+}\rangle + |{-}{-}\rangle &= \frac{1}{2}\big(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle + |00\rangle - |01\rangle - |10\rangle + |11\rangle\,\big) \\ &= |00\rangle + |11\rangle\,. \end{aligned} \tag{2.2.28}$$

Suppose now that the equality holds for $\lambda = \ell$. Then, we show that it holds when $\lambda = \ell + 1$. Let $\theta \in \{0,1\}^{\ell+1}$ and define $\theta' \in \{0,1\}^\ell$ to be its first ℓ elements from the lest. In other words, we either have $\theta = \theta'0$ or $\theta = \theta'1$.

Thus,

$$\sum_{s\in\{0,1\}^{\ell+1}} \left|s^{\theta}\right\rangle \left|s^{\theta}\right\rangle = \sum_{p\in\{0,1\}^{\ell}} \sum_{b\in\{0,1\}} \left(\left|p^{\theta'}\right\rangle \otimes H^{\theta_{\ell+1}} \left|b\right\rangle\right) \otimes \left(\left|p^{\theta'}\right\rangle \otimes H^{\theta_{\ell+1}} \left|b\right\rangle\right) \quad (2.2.29)$$

and, by assumption, our equality holds for $\lambda = \ell$ and so

$$= \sum_{p\in\{0,1\}^{\ell}} \sum_{b\in\{0,1\}} \left(\left|p\right\rangle \otimes H^{\theta_{\ell+1}} \left|b\right\rangle\right) \otimes \left(\left|p\right\rangle \otimes H^{\theta_{\ell+1}} \left|b\right\rangle\right). \quad (2.2.30)$$

If $\theta_{\ell+1} = 0$, then we obtain

$$\sum_{s\in\{0,1\}^{\ell+1}} \left|s^{\theta}\right\rangle \left|s^{\theta}\right\rangle = \sum_{p\in\{0,1\}^{\ell}} \left(\left|p\right\rangle \left|0\right\rangle \otimes \left|p\right\rangle \left|0\right\rangle + \left|p\right\rangle \left|1\right\rangle \otimes \left|p\right\rangle \left|1\right\rangle\right) = \sum_{s\in\{0,1\}^{\ell+1}} \left|s\right\rangle \left|s\right\rangle \quad (2.2.31)$$

which gives the result. If $\theta_{\ell+1} = 1$, we obtain

$$\sum_{s\in\{0,1\}^{\ell+1}} \left|s^{\theta}\right\rangle \left|s^{\theta}\right\rangle = \sum_{p\in\{0,1\}^{\ell}} \left(\left|p\right\rangle \left|+\right\rangle \otimes \left|p\right\rangle \left|+\right\rangle + \left|p\right\rangle \left|-\right\rangle \otimes \left|p\right\rangle \left|-\right\rangle\right) \quad (2.2.32)$$

and a manipulation similar to the one in Equation (2.2.28) gives the result. ∎

2.2.6 Density Operator Formalism

The postulates, as described in Sections 2.2.1 to 2.2.4, give a description of quantum mechanics for closed, isolated systems. The picture changes slightly when we consider quantum systems which may not be closed. An example of a quantum system which is not closed would be a single photon that is entangled with another, spatially separated, photon. We would still like to be able to say something about operations and measurements that could be done on this single photon.

To consider such cases, we adopt the density operator formalism. The density operator formalism will also allow us to very efficiently describe an unknown quantum state sampled from a known probability distribution.

2.2.6.1 Trace Operator

Key to the density operator formalism is a particular linear operator called the trace.

Definition 2.2.19 (Trace)**.**
Let $\mathcal{H}$ be a Hilbert space. The trace $\mathrm{Tr} \in \mathcal{L}(\mathcal{L}(\mathcal{H}), \mathbb{C})$ *is the unique linear operator which satisfies*

$$\mathrm{Tr}\left[\, |\psi\rangle\langle\phi| \,\right] = \langle\psi|\phi\rangle \tag{2.2.33}$$

for all vectors $|\psi\rangle, |\phi\rangle \in \mathcal{H}$.

The trace has a particular property which we will call *cyclicity*.

Lemma 2.2.20.
Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces. Let $L \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$ and $M \in \mathcal{L}(\mathcal{H}_B, \mathcal{H}_A)$ be operators. Then,

$$\mathrm{Tr}\left[ML\right] = \mathrm{Tr}\left[LM\right] \tag{2.2.34}$$

Note that $ML \in \mathcal{L}(\mathcal{H}_A)$ and $LM \in \mathcal{L}(\mathcal{H}_B)$. So, it may be better to write

$$\mathrm{Tr}_A\left[ML\right] = \mathrm{Tr}_B\left[LM\right] \tag{2.2.35}$$

to highlight the fact that $\mathrm{Tr}_A \in \mathcal{L}(\mathcal{L}(\mathcal{H}_A), \mathbb{C})$ and $\mathrm{Tr}_B \in \mathcal{L}(\mathcal{L}(\mathcal{H}_B), \mathbb{C})$ are, technically, different operators.

If $\mathcal{H}_A$ and $\mathcal{H}_B$ are Hilbert spaces, then $\mathbb{1}_A \otimes \mathrm{Tr}_B \in \mathcal{L}(\mathcal{L}(\mathcal{H}_A)\otimes\mathcal{L}(\mathcal{H}_B), \mathcal{L}(\mathcal{H}_A)\otimes\mathbb{C})$ is often called the *partial trace*. Applying this operator is often described as tracing out the B subsystem.

For any Hilbert space $\mathcal{H}$, we have that $\mathcal{H}\otimes\mathbb{C}$ is isomorphic to $\mathcal{H}$. This follows from the fact that for every elementary tensor in $\mathcal{H}\otimes\mathbb{C}$, we may write $|\psi\rangle\otimes s = (s \cdot |\psi\rangle)\otimes 1$. Thus, we will consider partial trace $\mathbb{1}_A \otimes \mathrm{Tr}_B$ as a linear operator form $\mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ to $\mathcal{L}(\mathcal{H}_A)$.

Note that the trace of a tensor product is the product of the traces, which is to say that $\mathrm{Tr}[M \otimes L] = \mathrm{Tr}[M] \cdot \mathrm{Tr}[L]$, and that if $\mathcal{H}_C = \mathcal{H}_A \otimes \mathcal{H}_B$, then $\mathrm{Tr}_C = \mathrm{Tr}_A \otimes \mathrm{Tr}_B$.

2.2.6.2 Motivating the Density Operator

We can motivate the usefulness of the density operator formalism with the following example.

We are presented with a machine which produces, with equal probability, a quantum state in either the $|0\rangle$ or $|+\rangle$ state. If we immediately measure the quantum state we are given with the projective measurement $\{P_0, P_1\}$, what is the probability of obtaining 0 as the measurement result?

According to the fourth postulate and the properties of the trace, we can compute this as probability as

$$\begin{aligned}
\frac{1}{2}\left(\|P_0|0\rangle\|^2 + \|P_0|+\rangle\|^2\right) &= \frac{1}{2}\left(\langle 0|P_0^\dagger P_0|0\rangle + \langle +|P_0^\dagger P_0|+\rangle\right) \\
&= \frac{1}{2}\left(\langle 0|P_0|0\rangle + \langle +|P_0|+\rangle\right) \\
&= \frac{1}{2}\left(\mathrm{Tr}\left[\langle 0|P_0|0\rangle\right] + \mathrm{Tr}\left[\langle +|P_0|+\rangle\right]\right) \\
&= \frac{1}{2}\left(\mathrm{Tr}\left[P_0|0\rangle\langle 0|\right] + \mathrm{Tr}\left[P_0|+\rangle\langle +|\right]\right) \\
&= \mathrm{Tr}\left[P_0\left(\frac{|0\rangle\langle 0| + |+\rangle\langle +|}{2}\right)\right].
\end{aligned} \tag{2.2.36}$$

So, it seems that

$$\frac{|0\rangle\langle 0| + |+\rangle\langle +|}{2} \tag{2.2.37}$$

correctly represents, in a certain sense, the quantum state we received from the machine. Note, however, that this is not a vector. It is a *density operator*.

2.2.6.3 Density Operators

Definition 2.2.21 (Density Operator)**.**
Let $\mathcal{H}$ be a Hilbert space. A linear operator $\rho \in \mathcal{L}(\mathcal{H})$ is said to be a density operator if and only if $\rho \in \mathcal{P}(\mathcal{H})$ and $\mathrm{Tr}[\rho] = 1$. The set of all density operators on $\mathcal{H}$ is denoted by $\mathcal{D}(\mathcal{H})$.

We note that to every unit vector $|\psi\rangle \in \mathcal{H}$ in some Hilbert space, we can associate a density operator on this Hilbert space by the map

$$|\psi\rangle \mapsto |\psi\rangle\langle\psi|. \tag{2.2.38}$$

If a density operator ρ may be expressed as $|\psi\rangle\langle\psi|$ for some unit vector $|\psi\rangle \in \mathcal{H}$, we say that ρ is a *pure state*. Else, we say that ρ is *mixed state*.

We note that for any two states $\rho_0, \rho_1 \in \mathcal{D}(\mathcal{H})$ and any two reals $p_0, p_1 \in \mathbb{R}_0^+$ such that $p_0 + p_1 = 1$, we have that $p_0\rho_0 + p_1\rho_1 \in \mathcal{D}(\mathcal{H})$. This can generalized to any finite collection of density operators and real coefficients.

In particular, every mixed state can be seen as a linear combination of pure states.

Lemma 2.2.22.
Let $\rho \in \mathcal{D}(\mathcal{H})$ be a density operator. Then, there exists a finite set I, a collection of positive reals $\{p_i\}_{i\in I} \subseteq \mathbb{R}^+$, and a collection of unit vectors $\{|\psi_i\rangle\}_{i\in I} \subseteq \mathcal{H}$ such that

$$\rho = \sum_{i\in I} p_i \, |\psi_i\rangle\langle\psi_i| \, . \tag{2.2.39}$$

Since $\mathrm{Tr}[\rho] = 1$, the p_i's in the above lemma must satisfy $\sum_{i\in I} p_i = 1$. This allows us to interpret mixed states as a distribution over pure states. We sometimes call $\{(p_i, |\psi_i\rangle)\}_{i\in I}$ an *ensemble* of states.

2.2.6.4 Completely Positive Trace Preserving Maps

If pure states evolve according to unitary operators, what are the maps that quantum mechanics allow on density operators? Recall that mixed states are operators, not vectors. So, instead of having linear maps $L \in \mathcal{L}(\mathcal{H})$, we will be considering linear maps of linear operators: $\Phi \in \mathcal{L}(\mathcal{L}(\mathcal{H}_A), \mathcal{L}(\mathcal{H}_B))$. These are sometimes called *superoperators*.

We recall that $\mathbb{1} \in \mathcal{L}(\mathcal{H})$ was defined as the identity operator. We will overload the notation of $\mathbb{1}$ and also use it to denote the identity in $\mathcal{L}(\mathcal{L}(\mathcal{H}), \mathcal{L}(\mathcal{H}))$.

For a superoperator to be permissible in quantum mechanics, it has to satisfy two criteria. These criteria ensure that density operators, which represent the state of a quantum system, are mapped to density operators.

Definition 2.2.23 (Positive Map)**.**
A linear operator $\Phi : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ is positive *if and only if*

$$P \in \mathcal{P}(\mathcal{H}_A) \implies \Phi(P) \in \mathcal{P}(\mathcal{H}_B). \tag{2.2.40}$$

Definition 2.2.24 (Completely Positive Trace Preserving Maps)**.**
Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two Hilbert spaces. A map $\Phi : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ is said to be completely positive trace preserving (CPTP) if

1. *it is completely positive, which is to say that*

$$\Phi \otimes \mathbb{1}_C : \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_C) \to \mathcal{L}(\mathcal{H}_B \otimes \mathcal{H}_C) \tag{2.2.41}$$

   is a positive map for any Hilbert space $\mathcal{H}_C$, and

2. *it is trace preserving, which is to say that*

$$\mathrm{Tr}(\Phi(L)) = \mathrm{Tr}(L) \tag{2.2.42}$$

   for all $L \in \mathcal{L}(\mathcal{H}_A)$.

In the same way that unitary operators characterized the allowed operations on quantum states in the pure formalism, CPTP maps characterize the allowed operations in the mixed formalism. In particular, it can be seen that if $\Phi : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ is a CPTP map, then $\rho \in \mathcal{D}(\mathcal{H}_A) \implies \Phi(\rho) \in \mathcal{D}(\mathcal{H}_B)$. Thus, we will sometimes write CPTP maps as $\Phi : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_B)$, instead of $\Phi : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$, when we are working with the density states of quantum systems.

Even if they are superoperators, CPTP maps remain linear operators on vector spaces. As such, all our remarks on linear operators and their tensor products also hold for CPTP maps.

The identity map $\mathbb{1} \in \mathcal{L}(\mathcal{L}(\mathcal{H}))$ is a CPTP map, as is the trace. The tensor product of two CPTP maps remains a CPTP map and the composition of two CPTP maps remains a CPTP map. Unitary operators also naturally give rise to CPTP maps.

Lemma 2.2.25.
Let $\mathcal{H}$ be a Hilbert space and $U \in \mathcal{U}(\mathcal{H})$ be a unitary operator. Then, the mapping

$$L \mapsto ULU^\dagger \tag{2.2.43}$$

is a CPTP map.

The convex combinations of CPTP maps are also CPTP maps.

Lemma 2.2.26.
Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces. Let $\Phi, \Psi : \mathcal{L}(H_A) \to \mathcal{L}(H_B)$ be two CPTP maps and $p_0, p_1 \in \mathbb{R}_0^+$ be two reals such that $p_0 + p_1 = 1$. Then, $p_0\Phi + p_1\Psi : \mathcal{L}(H_A) \to \mathcal{L}(H_B)$ is also a CPTP map.

This is quite useful since the CPTP map of a process which may apply the CPTP map Φ_i with probability p_i can be described by $\sum_{i\in I} p_i\Phi_i$.

CPTP maps also characterize the notion of state preparation. In quantum information, it is common to read a sentence of the form "Alice prepares, or generates, an EPR pair". We can model this generation is given by the CPTP map $\Phi : \mathcal{D}(\mathbb{C}) \to \mathcal{D}(\mathcal{Q}(2))$ defined by

$$1 \mapsto |\mathrm{EPR}\rangle\langle\mathrm{EPR}| \,. \tag{2.2.44}$$

Indeed, $\mathcal{D}(\mathbb{C}) = \{1\}$ is a set with a single element and we can see it as the state space of no qubits. In general, we can model the action of preparing the state ρ by the CPTP map $1 \mapsto \rho$. Note that, similarly, the trace operator $\mathrm{Tr} : \mathcal{D}(\mathcal{Q}) \to \mathcal{D}(\mathbb{C})$ can be interpreted as discarding, or tracing out, a qubit.

Perhaps most importantly, CPTP maps can also be viewed as unitary operators on larger Hilbert spaces. Mathematically, this can be attributed to Stinespring's dilation theorem. We present a particular formulation of this fact for CPTP maps between qubits as given by Aharonov, Kitaev, and Nisan [AKN98].

In essence, every CPTP map $\Phi : \mathcal{D}(\mathcal{Q}(n)) \to \mathcal{D}(\mathcal{Q}(m))$ map can be implemented by the following three steps: First, append $n + m$ qubits to the system. Then, apply some unitary operator. Finally, trace out the last $2n$ qubits.

Colloquially, we refer to this as *purifying* the CPTP map.

Theorem 2.2.27 (CPTP Map on Qubits as a Unitary Operator [AKN98])**.**
Let $n, m \in \mathbb{N}^+$ be two integers and let $\Phi : \mathcal{D}(\mathcal{Q}(n)_A) \to \mathcal{D}(\mathcal{Q}(m)_B)$ be a CPTP map. Let $\mathcal{Q}(n+m)_{A'}$ and $\mathcal{Q}(2n)_{B'}$ be two Hilbert spaces such that $\mathcal{Q}(n)_A \otimes \mathcal{Q}(n+m)_{A'}$ is isomorphic to $\mathcal{Q}(m)_B \otimes \mathcal{Q}(2n)_{B'}$.

Then, there exists a unitary operator $U \in \mathcal{U}(\mathcal{Q}(2n+m))$ *such that*

$$\Phi(\rho) = \mathrm{Tr}_{B'}\left[U\left(\rho_A \otimes |\mathbf{0}\rangle\langle\mathbf{0}|_{A'}\right)U^\dagger\right] \tag{2.2.45}$$

for all $\rho \in \mathcal{D}(\mathcal{Q}(n)_A)$ *and where* $|\mathbf{0}\rangle\langle\mathbf{0}|_{A'}$ *is the density operator corresponding to* $n+m$ *qubits in the* $|0\rangle$ *state.*

The four Hilbert spaces in Theorem 2.2.27 can be visualized as the tensor product

$$\underbrace{\overbrace{\mathcal{Q}\otimes\ldots\otimes\mathcal{Q}}^{\mathcal{Q}(n)_A}}_{\mathcal{Q}(m)_B} \otimes \underbrace{\overbrace{\mathcal{Q}\otimes\ldots\otimes\mathcal{Q}}^{\mathcal{Q}(n+m)_{A'}}}_{\mathcal{Q}(2n)_{B'}}. \tag{2.2.46}$$

2.2.6.5 Measurements on Density Operators

As was saw in our motivating example, measurements can be expressed very well in the density operator formalism. If $\mathcal{M} = \{M_i\}_{i\in I}$ is a measurement on the Hilbert space $\mathcal{H}$ and $\rho \in \mathcal{D}(\mathcal{H})$ is some state on this space, then the probability of obtaining the outcome $i \in I$ when measuring ρ with $\mathcal{M}$ is given by

$$\mathrm{Tr}\left[M_i^\dagger M_i \rho\right]. \tag{2.2.47}$$

If we see the state being measured as an ensemble of pure states, $\rho = \sum_{j\in J} p_j |\psi_j\rangle\langle\psi_j|$, we may use the linearity and cyclic property of the trace to obtain

$$\begin{aligned}
\mathrm{Tr}\left[M_i^\dagger M_i \rho\right] &= \sum_{j\in J} p_j \,\mathrm{Tr}\left[M_i^\dagger M_i |\psi_j\rangle\langle\psi_j|\right] \\
&= \mathrm{Tr}\left[\langle\psi_j| M_i^\dagger M_i |\psi_j\rangle\right] \\
&= \sum_{j\in J} p_j \langle\psi_j| M_i^\dagger M_i |\psi_j\rangle \\
&= \sum_{j\in J} p_j \|M_i|\psi_j\rangle\|^2.
\end{aligned} \tag{2.2.48}$$

Note that measurement $\mathcal{M}_A = \{M_{A,i}\}_{i\in I_A}$ on a Hilbert space $\mathcal{H}_A$ can naturally be extended to a measurement on $\mathcal{H}_A \otimes \mathcal{H}_B$ with $\{M_{A,i}\otimes \mathbb{1}_B\}_{i\in I_A}$. Similarly, if we have a measurement $\mathcal{H}_B = \{M_{B,j}\}_{j\in I_B}$, we can extend it to a measurement on $\mathcal{H}_A \otimes \mathcal{H}_B$. Note that $M_{A,i}\otimes\mathbb{1}_B$ commutes with $\mathbb{1}_A \otimes M_{B,j}$ and so it can be shown that the order

of the measurements has no effect on the outcomes.

In fact, we can see measurements as CPTP maps. Let $\mathcal{M} = \{M_i\}_{i\in I}$ be a measurement on a Hilbert space $\mathcal{H}$. Let $\mathcal{H}_I$ be the Hilbert space spanned by the orthonormal basis $\{|i\rangle\}_{i\in I}$. Then, the map $\mathcal{M} : \mathcal{D}(\mathcal{H}) \to \mathcal{D}(\mathcal{H} \otimes \mathcal{H}_I)$ defined by

$$\mathcal{M}(\rho) \mapsto \sum_{i\in I} M_i \rho M_i^\dagger \otimes |i\rangle\langle i| \tag{2.2.49}$$

is a CPTP map. We may write any particular summand in the right-hand side as

$$\mathrm{Tr}\left[M_i^\dagger M_i \rho\right] \cdot \left(\frac{M_i \rho M_I^\dagger}{\mathrm{Tr}\left[M_i^\dagger M_i \rho\right]} \otimes |i\rangle\langle i|\right) \tag{2.2.50}$$

which has a nice interpretation. The scalar given by the trace is the probability of obtaining outcome i upon measuring ρ, the first element in the tensor product is the post-measurement state, and the second term in the tensor product represents the measurement outcome. If only the measurement outcome interests us, we can trace out post-measurement state.

2.2.7 No-Cloning Theorem

We conclude this chapter with the no-cloning theorem. We base this formulation on the one found in the works of Dieks, Wooters, and Zurek [Die82, WZ82].

Theorem 2.2.28 (No-Cloning)**.**
There is no Hilbert space $\mathcal{H}$, state $|ready\rangle \in \mathcal{H}$, and unitary $U \in \mathcal{U}(\mathcal{Q} \otimes \mathcal{Q} \otimes \mathcal{H})$ such that

$$U\big(\,|\psi\rangle\,|0\rangle\,|ready\rangle\,\big) = |\psi\rangle\,|\psi\rangle\,|done_\psi\rangle \tag{2.2.51}$$

for all states $|\psi\rangle \in \mathcal{Q}$.

Note that $|\mathrm{done}_\psi\rangle$ may depend on the input state $|\psi\rangle$. We can think of $\mathcal{H}$ as the "workspace" of our unitary operator and we pose no restrictions on this space except that its initial state must not depend on the input state.

Our proof will be more verbose then necessary. However, it will be a good exercise in the application of the mathematical formalism developed so far. It is inspired by the one found in Nielsen and Chuang's textbook [NC10].

Proof: We proceed by contradiction. Suppose there exists such a Hilbert space, state, and unitary operator. By assumption, we have that

$$U\big(\,|0\rangle\,|0\rangle\,|\text{ready}\rangle\,\big) = |0\rangle\,|0\rangle\,|\text{done}_0\rangle \tag{2.2.52}$$

and

$$U\big(\,|1\rangle\,|0\rangle\,|\text{ready}\rangle\,\big) = |1\rangle\,|1\rangle\,|\text{done}_1\rangle\,. \tag{2.2.53}$$

We consider now the case $|\psi\rangle = |+\rangle$. Using our assumption, we have that

$$U\big(\,|+\rangle\,|0\rangle\,|\text{ready}\rangle\,\big) = |+\rangle\,|+\rangle\,|\text{done}_+\rangle \tag{2.2.54}$$

or, we can use the linearity of U and the definition of $|+\rangle$ to obtain

$$\begin{aligned} U\big(\,|+\rangle\,|0\rangle\,|\text{ready}\rangle\,\big) &= U\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\,|0\rangle\,|\text{ready}\rangle\right) \\ &= \frac{1}{\sqrt{2}}\,|0\rangle\,|0\rangle\,|\text{done}_0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,|1\rangle\,|\text{done}_1\rangle\,. \end{aligned} \tag{2.2.55}$$

We claim that these two states are not equal. It suffices to show that their inner product is not one. Noting that

$$\big(\,\langle+|\,\langle+|\,\big)\big(\,|0\rangle\,|0\rangle\,\big) = \langle+|0\rangle\,\langle+|0\rangle = \frac{1}{\sqrt{2}}\cdot\frac{1}{\sqrt{2}} = \frac{1}{2} \tag{2.2.56}$$

and similarly if $|00\rangle$ is replaced by $|11\rangle$, we may write:

$$\begin{aligned} &\langle+|\,\langle+|\,\langle\text{done}_+|\left(\frac{1}{\sqrt{2}}\,|0\rangle\,|0\rangle\,|\text{done}_0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,|1\rangle\,|\text{done}_1\rangle\right) \\ &\qquad = \frac{1}{2\sqrt{2}}\big(\,\langle\text{done}_+|\text{done}_0\rangle + \langle\text{done}_+|\text{done}_1\rangle\,\big) \end{aligned} \tag{2.2.57}$$

So, it suffices to show that:

$$\langle\text{done}_+|\text{done}_0\rangle + \langle\text{done}_+|\text{done}_1\rangle \neq 2\sqrt{2} \tag{2.2.58}$$

Taking the absolute value, we may write

$$|\langle\text{done}_+|\text{done}_0\rangle + \langle\text{done}_+|\text{done}_1\rangle| \leq |\langle\text{done}_+|\text{done}_0\rangle| + |\langle\text{done}_+|\text{done}_1\rangle| \leq 2 \tag{2.2.59}$$

where the last inequality follows from the fact that $\| |\text{done}_b\rangle \| = 1$ (since U must preserve the norm) and Theorem 2.1.19. ∎

We emphasize, however, that the no-cloning theorem does not mean that no quantum state can be copied. In particular, for any orthonormal basis $B = \{|b_i\rangle\}_{i \in I}$ of a Hilbert space $\mathcal{H}$, there is an auxiliary state $|a\rangle \in \mathcal{H}$ and a unitary operator U_B such that

$$U_B \left(|b_i\rangle \, |a\rangle \right) = |b_i\rangle \, |b_i\rangle \tag{2.2.60}$$

for all $|b_i\rangle \in B$.

Chapter 3

Quantum Computing

In this chapter, we present the tools from quantum information processing which we will use. In Section 3.1, we introduce the notion of quantum circuits and efficient quantum computations. We say a few words on oracle computations in Section 3.2. Quantum-secure pseudorandom functions are introduced in Section 3.3 and, finally, we discuss monogamy-of-entanglement games in Section 3.4.

3.1 Computational Model

In general, any quantum computation can be modelled by a CPTP map from n qubits to m qubits for $n, m \in \mathbb{N}$. However, this does not capture the *complexity* of the computation. For this, we use the notion of *quantum circuits*. We sketch out the relevant details here and refer the reader to Watrous' more comprehensive introduction to this subject [Wat09].

Central to the notion of a quantum circuit is a *universal gate set*. A universal gate set a finite collection of CPTP maps $\mathcal{G} = \{\Phi_i\}_{i \in I}$. From this finite collection of CPTP maps, a more complex map can be built. An abstract example can be given by the map

$$\Phi = \Phi_2 \circ (\Phi_1 \otimes \Phi_3) \circ (\Phi_4 \otimes \Phi_1)\,. \tag{3.1.1}$$

Without getting into the details, the gate set is universal in the sense that any CPTP map $\Phi : \mathcal{D}(\mathcal{Q}(n)) \to \mathcal{D}(\mathcal{Q}(m))$ can be approximated to any arbitrarily high degree of precision by the composition of elements from the gate set. One may think of the elements of the universal gate set as the simple and basic building blocks from

which a more complex computation is built. A common example of a universal gate set, as given by Watrous [Wat09], contains five gates, none of which act on more than three qubits. Three of the gates implement maps of the form $\rho \to U\rho U^\dagger$ for a unitary operator U. The last two maps are the single qubit trace $\mathrm{Tr} : \mathcal{D}(\mathcal{Q}) \to \mathcal{D}(\mathbb{C})$ and the auxiliary state preparation $Aux : \mathcal{D}(\mathbb{C}) \to \mathcal{D}(\mathcal{Q})$ defined by $1 \mapsto |0\rangle\langle 0|$.

A *quantum circuit* $\mathtt{C}$ from the universal gate set $\mathcal{G}$ is a finite length bit string which encodes a valid composition of gates from $\mathcal{G}$. The specifics of the encoding will not be a concern to us, except that we assume that the length of the bit string encoding a certain circuit cannot be smaller than the number of gates in that circuit. In other words, we do not allow "compression" in our encoding.

We note that it is sometimes convenient to distinguish between a quantum circuit and the overall CPTP map that it implements. For example, there are many different circuits that implement the same CPTP map. We remark that it is also sometimes convenient to distinguish between a circuit and its description. We do not need to do this and identify these two notions.

A common measure of the complexity of a circuit $\mathtt{C}$ is its *size* which is simply the number of gates it contains.

One of the drawbacks of quantum circuits is that a single circuit can only process inputs of a single specific size. However, we are often interested in a computational task that scales with some parameter $\lambda \in \mathbb{N}^+$. To treat this task, we then consider a family of quantum circuits $\{\mathtt{C}_\lambda\}_{\lambda\in\mathbb{N}^+}$ with one circuit to treat each individual case arising from the different values of λ.

Specifically, we often require that the whole family can be described by a single deterministic polynomial-time Turing machine. We refer the reader to any standard textbook on the theory of computation or complexity theory (*e.g.*: [AB09]) for a formal definition of a Turing machine. For our needs, we can view a deterministic Turing machine $\mathtt{T}$ as a mathematical model for a classical computer which computes a certain map $f_\mathtt{T} : \{0,1\}^* \to \{0.1\}^*$. The complexity of the function $f_\mathtt{T}$ which the Turing machine $\mathtt{T}$ computes can be measured in the number of "steps" that the machine takes to produce the answer on any input. Specifically, we say that $\mathtt{T}$ is a polynomial-time Turing machine if there exists a polynomial $p_\mathtt{T}$ such that for any input s, $\mathtt{T}$ produces the bit string $f_\mathtt{T}(s)$ in at most $p_\mathtt{T}(|s|)$ steps.

Polynomial-time Turing machines give a formal definition for the otherwise intuitive notion of "efficient computation".

Definition 3.1.1 (Polynomial-Time Uniform Quantum Circuit)**.**
A polynomial-time uniform quantum circuit *is a collection of quantum circuits* $\{\mathsf{C}_\lambda\}_{\lambda\in\mathbb{N}^+}$ *such that there exists a deterministic polynomial-time Turing machine* T *which, on input of the bit string composed of* λ 1*'s, outputs a description of* C_λ*.*

Since the only type of circuits that we consider are polynomial-time uniform quantum circuits, we allow ourselves to shorten their name to simply *polynomial-time circuits*.

In the same way that we identify "efficient classical computation" with polynomial-time Turing machines, polynomial-time circuit families capture the idea of efficient quantum computations.

We also emphasize that if $\{\mathtt{C}_\lambda\}_{\lambda\in\mathbb{N}^+}$ is a polynomial-uniform family of circuits, then there is a polynomial p such that the number of gates in $\mathtt{C}_\lambda$ is bounded by $p(\lambda)$ for all $\lambda \in \mathbb{N}^+$. This follows from the fact that there exists a Turing machine $\mathtt{T}$ which generates the description $\mathtt{C}_\lambda$ and does not take more then $p_\mathtt{T}(\lambda)$ do to so. Since $\mathtt{T}$ takes at most $p_\mathtt{T}(\lambda)$ steps, it cannot produce more than $p_\mathtt{T}(\lambda)$ bits as an output. Since our encoding of quantum circuits does not allow compression, this bounds the number of gates in the circuit.

Finally, we note that via standard methods all the auxiliary state preparation gates in a circuit $\mathtt{C}$ may be moved to the start of the circuit and all trace gates at the end of the circuit. Considering that all the other gates are unitary, this allows us to naturally represent the CPTP map implemented by the circuit in manner similar to the one given in Theorem 2.2.27.

3.2 Oracles

What is an oracle? An oracle can be seen as a gate added to the chosen universal gate set which computes an arbitrary but fixed Boolean function. A circuit with access to this oracle is a circuit built from a gate set which includes this new gate.

Definition 3.2.1 (Circuits with Oracles)**.**
Let $H \in \mathrm{Bool}(n, m)$ *be a function. Let* $O^H \in \mathcal{U}(\mathcal{Q}(n)\otimes\mathcal{Q}(m))$ *be the unitary operator defined on the computational basis by the mapping:*

$$|a\rangle\,|b\rangle \mapsto |a\rangle\,|b \oplus H(a)\rangle \tag{3.2.1}$$

A quantum circuit with oracle access to H, denoted by $\mathtt{C}^H$, is a quantum circuit with gate set $\mathcal{G} \cup \{\Phi_{O^H}\}$ where $\Phi_{O^H} : \mathcal{DQ}(n+m) \to \mathcal{DQ}(n+m)$ is the CPTP map defined by

$$\rho \mapsto O^H \rho \left(O^H\right)^\dagger. \tag{3.2.2}$$

We note that if $H \in \mathrm{Bool}(n,m)$ is a Boolean function and $\mathtt{C}^H$ is a quantum circuit with oracle access to H, we can pick another function $H' \in \mathrm{Bool}(n,m)$ with the same input and output sizes and consider the circuit $\mathtt{C}^{H'}$. This circuit is the same as $\mathtt{C}^H$, except we replace every instance of the O^H gate with an instance of the $O^{H'}$ gate.

3.2.1 Quantum Oracle Computations for Pure States

Quantum computations with access to an oracle have been studied in the literature, for example in [BBC+01], [BDF+11] and [Unr15]. In these works, the computation was modelled by multiple unitary transformations on a pure state.

In this context, we can model a quantum computation querying $q \in \mathbb{N}^+$ times an oracle O^H implementing a function $H \in \mathrm{Bool}(n,m)$ by the unitary operator

$$U_q \left(\mathbb{1}_S \otimes O^H\right) U_{q-1} \left(\mathbb{1}_S \otimes O^H\right) \cdots U_1 \left(\mathbb{1}_S \otimes O^H\right) U_0 \in \mathcal{U}(\mathcal{H}) \tag{3.2.3}$$

where $\mathcal{H}$ is a Hilbert space of the form

$$\mathcal{H} = \mathcal{Q}(k)_S \otimes \mathcal{Q}(n)_Q \otimes \mathcal{Q}(m)_R \tag{3.2.4}$$

and $O^H \in \mathcal{U}(\mathcal{Q}(n)_Q \otimes \mathcal{Q}(m)_R)$ is as defined in Definition 3.2.1. The collection of unitary operators $\{U_i\}_{i \in [q]_0}$, each an element of $\mathcal{U}(\mathcal{H})$, represent all computations that the party carries out prior, between and after the queries to the oracle. We give a visual representation of this type of computation in Figure 3.1.

We note that $\mathcal{H}$ has three registers. The first, $\mathcal{Q}(k)_S$, represents the workspace of the party and its memory between queries. We call it the "state register". We will call the second register, $\mathcal{Q}(n)_Q$, the "query register". It is in this register that the party will submit a query to the oracle. Finally, we call the third, $\mathcal{Q}(m)_R$, the "response register". It is in this register that the oracle will place its response.

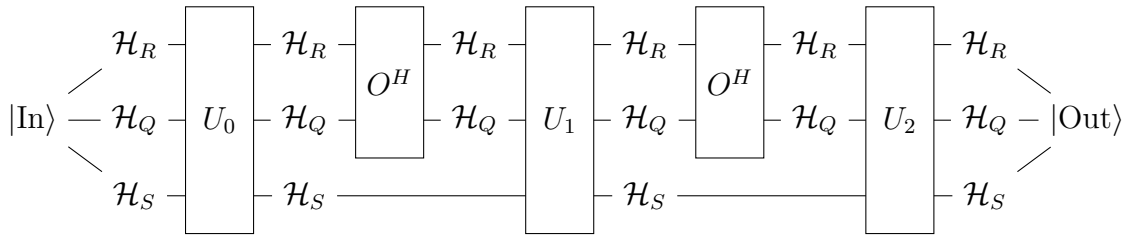


Figure 3.1: Schematic representation of an oracle computation with two queries, proceeding from left to right. We have $|\text{Out}\rangle = (U_2 O^H U_1 O^H U_0)\,|\text{In}\rangle$.

In general, there is no requirements for any of the unitary operators $\{U_i\}_{i\in[q]_0}$ to be the same. But, with about $s = log_2(q)$ extra qubits in the state register, we can use a single unitary U to simulate all $q+1$ unitary operators U_i. Indeed, we can define this operator $U \in \mathcal{U}(\mathcal{H} \otimes \mathcal{Q}(s)_C)$ by the mapping

$$|\psi\rangle\,|i\rangle \mapsto \begin{cases} (U_i\,|\psi\rangle)\,|i+1\rangle & \text{if } i \in [q]_0 \\ |\psi\rangle\,|i\rangle & \text{else.} \end{cases} \tag{3.2.5}$$

on all basis states and extended linearly to all other vectors. In essence, $\mathcal{Q}(s)_C$ acts as a "counter register" which keeps track of which unitary operator needs to be applied next. This allows us to write

$$(U_q U_{q-1} \cdots U_1 U_0\,|\psi\rangle)\,|q\rangle = U^{q+1}\,|\psi\rangle\,|0\rangle \tag{3.2.6}$$

for any $|\psi\rangle \in \mathcal{H}$.

Keeping in mind the above discussion, we now define a notion of "oracle computation". This is mostly be a notational convenience.

Definition 3.2.2 (Oracle computation)**.**
Let $n, m \in \mathbb{N}^+$. An oracle computation is a unitary operator $\mathcal{O} \in \mathcal{U}(\mathcal{H})$ on a Hilbert space of the form

$$\mathcal{H} = \mathcal{H}_S \otimes \mathcal{Q}(n)_Q \otimes \mathcal{Q}(m)_R. \tag{3.2.7}$$

It is parametrized by an integer $q \in \mathbb{N}^+$, a unitary operator $U \in \mathcal{U}(\mathcal{H})$, and a boolean function $H : \{0,1\}^n \to \{0,1\}^m$. We define it as

$$\mathcal{O}^{U,H,q} = \big(U\big(\mathbb{1}_S \otimes O^H\big)\big)^q \tag{3.2.8}$$

where $O^H \in \mathcal{U}(\mathcal{Q}(n) \otimes \mathcal{Q}(m))$ *is a unitary operator such that*

$$O^H |a\rangle |b\rangle = |a\rangle |b \oplus H(a)\rangle \tag{3.2.9}$$

for all computational basis elements.

Note that this definition also captures the possibility of having different unitary computations between queries as a "counter register" (as discussed above) may be present in the state register $\mathcal{H}_S$. Thus, there is no loss of generality in imposing a single unitary operator.

While $\mathcal{O}^{U,H,q}$ indeed models q queries to the oracle O^H, there is an argument to be made that there are only $q-1$ *effective* queries. This is due to the fact that we assume that the first operation in an oracle computation is a query to the oracle. There is no possible pre-processing by the party prior to submitting this query to the oracle. Note that this type of pre-processing was accounted for in [BBC+01] as can be seen by the presence of the operator U_0 in Equation (3.2.3).

We could have avoided this difference by defining $\mathcal{O}^{U,H,q}$ as $\left(U\left(\mathbb{1}_S \otimes O^H\right)\right)^q U$. We have opted not to do so primarily due to the fact that we will be interested in cases where parties have polynomially many queries to the oracle. It will be of no consequence to our analysis that a party may have to lose one query to the oracle to be able to complete its wanted pre-processing. We also justify this choice by the slightly simpler notation that it will offer later.

3.2.2 General Quantum Circuits with Oracles

The previous discussion concerned unitary computations with oracles. However, in general, our quantum circuits implement CPTP maps and not unitary operators.

However, we will assume that the CPTP maps implemented by a circuit with access to an oracle can be purified into a unitary oracle computation. This can be seen as the result of multiple applications of Theorem 2.2.27. Alternatively, it can be seen as a result of the fact that all auxiliary state preparation gates can be moved to the start of the circuit and all trace gates at the end. The resulting operations between these state preparation and trace gates is a unitary oracle computation of the form seen in the previous subsection.

Proposition 3.2.3.
Let $C^H : \mathcal{D}(\mathcal{Q}(a)_A) \to \mathcal{D}(\mathcal{Q}(b)_B)$ be the CPTP map implemented by a quantum circuit $\mathcal{C}^H$ with oracle access to a function $H \in \mathrm{Bool}(\lambda, n)$. Then, there exists Hilbert spaces $\mathcal{H}_{A'}$, $\mathcal{H}_{B'}$, and $\mathcal{H}_S$ satisfying

$$\mathcal{Q}(a)_A \otimes \mathcal{H}_{A'} \simeq \mathcal{Q}(b)_B \otimes \mathcal{H}_{B'} \simeq \mathcal{H}_S \otimes \mathcal{Q}(\lambda)_Q \otimes \mathcal{Q}(n)_R \tag{3.2.10}$$

and a unitary operator $U \in \mathcal{U}(\mathcal{H}_S \otimes \mathcal{Q}(\lambda)_Q \otimes \mathcal{Q}(n)_R)$ with a state $|aux\rangle\langle aux| \in \mathcal{D}(\mathcal{H}_A)$ such that

$$C^H(\rho) = \mathrm{Tr}_B \left[\left(\mathcal{O}^{U,H,q}\right) \left(\rho_A \otimes |aux\rangle\langle aux|_{A'}\right) \left(\mathcal{O}^{U,H,q}\right)^\dagger \right] \tag{3.2.11}$$

for all $\rho \in \mathcal{D}(\mathcal{Q}(a)_A)$.

3.3 Quantum-Secure Pseudorandom Functions

In this section, we define and discuss the notion of pseudorandom functions. Pseudorandom functions were introduced by Goldwasser, Goldreich, and Micali [GGM84].

3.3.1 Motivating Example

A standard way to motivate the notion of pseudorandom functions is to consider a classical private-key encryption scheme build from truly random functions. We walk through this scheme as it also resembles our upcoming uncloneable encryption scheme (Scheme 4.4.1).

Consider a classical private-key encryption scheme where the secret key shared by Alice and Bob is the description, or index, of a function $f \in \mathrm{Bool}(\lambda, n)$. To encrypt a message $m \in \{0,1\}^n$, Alice picks a random $r \in \{0,1\}^\lambda$ and sends $(f(r) \oplus m, r)$ as the ciphertext to Bob. An eavesdropping Eve is unable to learn m from this ciphertext if f is indeed sampled uniformly at random from $\mathrm{Bool}(\lambda, n)$.

Intuitively, the security of this scheme follows from the following ideas:

1. Being able to learn m from $(f(r) \oplus m, r)$ is equivalent to being able to learn $f(r)$ from $(f(r) \oplus m, r)$. Indeed, it suffices to compute $m \oplus (f(r) \oplus m) = f(r)$.

2. The message m is uncorrelated to f or r. Thus, being able to learn $f(r)$ from the ciphertext $(f(r) \oplus m, r)$ is equivalent to being able to learn $f(r)$ from r.

3. For any fixed string $r \in \{0,1\}^\lambda$, $f(r)$ is uniformly distributed over $\{0,1\}^n$ if f is uniformly distributed over $\mathrm{Bool}(\lambda, n)$.

So, Eve's task of guessing m given $f(r) \oplus m$ and r is equivalent to guessing the value of a random bit string of length n.

But, there is a bit of a problem. Sampling a function f uniformly at random from the set $\mathrm{Bool}(\lambda, n)$, the set of all functions $f : \{0,1\}^\lambda \to \{0,1\}^n$, is easier said than done. The key issue is that $|\mathrm{Bool}(\lambda, n)| = 2^{n2^\lambda}$ and so there does not exist a way to specify any arbitrary function from $\mathrm{Bool}(\lambda, n)$ using less than $n2^\lambda$ bits.

In other words, if Alice and Bob share some function $f \in \mathrm{Bool}(\lambda, n)$ as a secret key, then Alice and Bob are, effectively, sharing a key that is exponentially long.

Pseudorandom functions are a tool that allows us to overcome this problem. The idea is to consider only a subset $\mathcal{F} \subseteq \mathrm{Bool}(\lambda, n)$, which may be indexed by a polynomial number of bits, such that any efficient adversary may not distinguish between a function drawn from $\mathcal{F}$ or one drawn from $\mathrm{Bool}(\lambda, n)$.

3.3.2 Definition

In short, a quantum-secure pseudorandom function is a family of functions which may be described and computed efficiently, but which appears to behave like a random function to any efficient quantum adversary if we may only observe its input-output behaviour. We formalize this in the definition bellow, which was slightly adapted from [Zha12].

Definition 3.3.1 (Quantum-Secure Pseudorandom Function)**.**
A quantum-secure pseudorandom function $\mathcal{F}$ *is a collection of functions*

$$\mathcal{F} = \left\{ f_\lambda : \{0,1\}^\lambda \times \{0,1\}^{\ell_{In}(\lambda)} \to \{0,1\}^{\ell_{Out}(\lambda)} \right\}_{\lambda \in \mathbb{N}^+} \tag{3.3.1}$$

where $\ell_{In}, \ell_{Out} : \mathbb{N}^+ \to \mathbb{N}^+$ *satisfying the following properties.*

1. *There is a polynomial-time circuit* $\{\mathsf{F}_\lambda\}_{\lambda \in \mathbb{N}^+}$ *such that* F_λ *implements the CPTP map* $F_\lambda(\rho) = U_\lambda \rho U_\lambda^\dagger$ *where* $U_\lambda \in \mathcal{U}(\mathcal{Q}(\lambda) \otimes \mathcal{Q}(\ell_{In}(\lambda)) \otimes \mathcal{Q}(\ell_{Out}(\lambda)))$ *is defined by*

$$U_\lambda\big(|k\rangle |a\rangle |b\rangle \big) = |k\rangle |a\rangle |b \oplus f_\lambda(k,a)\rangle . \tag{3.3.2}$$

2. *For all polynomial-time circuit* $\{\mathcal{D}_\lambda^H\}_{\lambda\in\mathbb{N}^+}$ *having oracle access to a function of the form* $H \in \mathrm{Bool}(\ell_{In}(\lambda), \ell_{Out}(\lambda))$*, each implementing a CPTP map of the form* $D_\lambda^H : \mathcal{D}(\mathbb{C}) \to \mathcal{D}(\mathcal{Q})$*, there is a negligible function* $\eta_{\mathcal{D}}$ *such that*

$$\left| \Pr_{k\leftarrow\{0,1\}^\lambda} \mathrm{Tr}\left[|0\rangle\langle 0| \, D_\lambda^{f_\lambda(k,\cdot)}(1)\right] - \Pr_{H\leftarrow\mathrm{Bool}(\ell_{In}(\lambda),\ell_{Out}(\lambda))} \mathrm{Tr}\left[|0\rangle\langle 0| \, D_\lambda^{H}(1)\right] \right| \leq \eta_{\mathcal{D}}(\lambda). \tag{3.3.3}$$

We should think of $\{\mathtt{D}_\lambda\}_{\lambda\in\mathbb{N}^+}$ as circuits which attempt to distinguish two different cases: are they given oracle access to an instance of the pseudorandom function, which is to say $f(k,\cdot) : \{0,1\}^{\ell_{\mathrm{In}}(\lambda)} \to \{0,1\}^{\ell_{\mathrm{Out}}(\lambda)}$ for a randomly sampled $k \in \{0,1\}^\lambda$? Or to a function that was sampled truly at random, $H \in \mathrm{Bool}(\ell_{\mathrm{In}}(\lambda), \ell_{\mathrm{Out}}(\lambda))$?

The circuit takes no input and produces a single bit of output, via measuring a single qubit in the computational basis. The bound given in the definition ensures that the probability distribution of the output does not change by much in both scenarios.

We note that when Golwasser, Goldreich, and Micali first defined pseudorandom functions [GGM84], they did so with respect to classical adversaries. There are two main considerations which do not allow us to directly state that any pseudorandom function secure against classical adversaries is also secure against quantum adversaries:

1. The quantum adversary may be more powerful than the classical adversary.

2. A quantum adversary may query the function *in superposition*.

The first point reflects the belief that quantum computation may indeed be strictly stronger than classical computation. The second point tells us that, in general, a quantum adversary may apply the oracle of $f_\lambda(k,\cdot)$ or H to a superposition of basis states. For example, they may compute

$$U_f \left(\frac{1}{\sqrt{2^{\ell_{\mathrm{In}}(\lambda)}}} \sum_{s\in\{0,1\}^{\ell_{\mathrm{In}}(\lambda)}} |s\rangle \right) |0\rangle = \frac{1}{\sqrt{2^\lambda}} \sum_{s\in\{0,1\}^\lambda} |s\rangle \, |f(s)\rangle \tag{3.3.4}$$

where f is either H or $f_\lambda(k,\cdot)$. In fact, this ability to query in superposition was used by Zhandry [Zha12] to show that from a pseudorandom function secure against

classical adversary we can construct a pseudorandom function secure against classical adversaries but insecure against quantum adversaries.

Fortunately, Zhandry also showed that some common constructions of pseudorandom functions, such as the one given in [GGM84] when it uses quantum-secure pseudorandom generator, are also quantum-secure pseudorandom functions.

3.4 Monogamy-of-Entanglement Games

Monogamy-of-entanglement games were introduced and studied by Tomamichel, Fehr, Kaniewski, and Wehner [TFKW13]. They form a crucial element of the proof of security of our uncloneable encryption scheme. We review here their key definitions and also reformulate their main result in the form of a corollary that will be useful to us.

3.4.1 Monogamy-of-Entanglement

A full and rigorous treatment of the topic of monogamy-of-entanglement is beyond the scope of this work. In a nutshell, monogamy-of-entanglement states that if subsystems A and B have "a lot of entanglement" between them, then neither A nor B can have "a lot of entanglement" with some other subsystem C. We illustrate this situation in Figure 3.2.

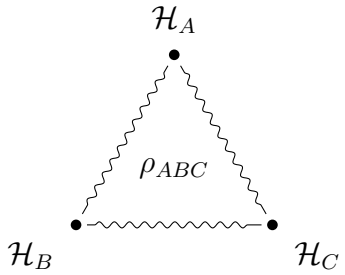


Figure 3.2: Tripartite quantum state $\rho \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$.

Quantifying entanglement between three of more subsystems is a non-trivial problem and may be done via a quantity called the *concurrence* or the *tangle* between the different subsystems of the quantum state. A formal analysis of these

quantities may be found in the works of Coffman, Kundu, and Wooters [CKW00] and Osborne and Verstraete [OV06], among others.

A simpler example will suffice to understand the concept studied in [TFKW13]. As mentioned in Section 2.2.5, one of the signatures of entanglement is that measurements on subsystems may produce correlated results. For example, consider an EPR pair shared between Alice and Bob,

$$|\text{EPR}\rangle\langle\text{EPR}|_{AB} \in \mathcal{D}(\mathcal{Q}_A \otimes \mathcal{Q}_B). \tag{3.4.1}$$

If Alice and Bob both measure in the computational basis, they will always obtain the same result. The same will also hold if they both measure in the Hadamard basis. This follows due to the fact that

$$|\text{EPR}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|{+}{+}\rangle + |{-}{-}\rangle}{\sqrt{2}}. \tag{3.4.2}$$

Is there a three qubit state that could be shared among Alice, Bob and Charlie such that all three will always obtain the same result if they all measure in the computational or Hadamard basis? As the results from [TFKW13] show, no.

The intuitive appeal to the monogamy-of-entanglement is that if Alice and Bob shared enough entanglement to always get the same results, then Charlie could not be sufficiently entangled with Alice and Bob to also obtain perfectly correlated results.

The monogamy-of-entanglement games study these type of situations. Alice will do one of many possible measurements on some state shared with Bob and Charlie and the probability of all three parties obtaining the same result will be bounded.

3.4.2 Defining Monogamy-of-Entanglement Games

We formally define the games, their strategies and how they are played. These definitions come directly from [TFKW13].

Definition 3.4.1 (Monogamy-of-Entanglement Game)**.**
Let X and Θ be finite sets and let $\mathcal{H}$ be a Hilbert space. For every $\theta \in \Theta$, we define a POVM $\mathcal{M}^\theta = \{M_x^\theta\}_{x\in X}$ on $\mathcal{H}$. Then, $G = \{\mathcal{M}^\theta\}_{\theta\in\Theta}$ is a monogamy-of-entanglement game (MoEG) on the Hilbert space $\mathcal{H}$.

We call G a "game" since it can be played "played" in the following fashion.

Game 1 (Monogamy-of-Entanglement Game)**.**
Let $G = \{\mathcal{M}^\theta\}_{\theta\in\Theta}$ be a monogamy-of-entanglement game on a Hilbert space $\mathcal{H}_A$. We define the following game between a referee (Alice) and two adversaries (Bob and Charlie) who begin the game together.

1. Bob and Charlie generate a quantum state $\rho \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$. They give the A subsystem of ρ to Alice, while Bob and Charlie keep the B and C subsystems, respectively. Bob and Charlie are then separated.

2. Alice samples $\theta \leftarrow \Theta$ at random. She then executes the $\mathcal{M}^\theta$ measurement on her subsystem of ρ and records the result as $x_A \in X$.

3. Alice broadcasts θ to Bob and Charlie.

4. Bob and Charlie, without communicating, perform some measurement which may depend on θ on their respective subsystems. They record $x_B, x_C \in X$, respectively, as results.

5. Bob and Charlie win if and only if $x_A = x_B = x_C$.

In other words, given a known collection of possible POVMs $\{\mathcal{M}^\theta\}_{\theta\in\Theta}$ and a shared quantum state, are Bob and Charlie able to guess the outcome of a measurement picked at random from a known set on Alice's subsystem? We formalize strategies for Bob and Charlie in the following definition.

Definition 3.4.2 (Strategy for a MoEG)**.**
Let $G = \{\mathcal{M}^\theta\}_{\theta\in\Theta}$ be a monogamy-of-entanglement game. A strategy for this game is given by a tuple

$$S = \left(\rho, \{\mathcal{B}^\theta = \{B_x^\theta\}_{x\in X}\}_{\theta\in\Theta}, \{\mathcal{C}^\theta = \{C_x^\theta\}_{x\in X}\}_{\theta\in\Theta}\right) \tag{3.4.3}$$

where

1. *$\mathcal{H}_B$, $\mathcal{H}_C$ are two Hilbert spaces and $\rho \in \mathcal{D}(\mathcal{H} \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ and*

2. *for all $\theta \in \Theta$, $\mathcal{B}^\theta$ and $\mathcal{C}^\theta$ are POVMs on $\mathcal{H}_B$ and $\mathcal{H}_C$, respectively.*

Definition 3.4.3 (Winning Probability of a MoEG)**.**
Let G be a monogamy-of-entanglement game as described in Definition 3.4.1 and S a

strategy for this game as described in Definition 3.4.2. Then, the winning probability of this strategy is given by

$$\omega_G(S) = \frac{1}{|\Theta|} \sum_{\theta \in \Theta} \sum_{x \in X} \mathrm{Tr}\left[\left(M_x^\theta \otimes B_x^\theta \otimes C_x^\theta \right) \rho \right] \tag{3.4.4}$$

and the winning probability of this game is given by

$$\omega_G = \sup_S \omega_G(S) \tag{3.4.5}$$

where the supremum is over all possible strategies.

3.4.3 The BB84 Game

One of the main results of [TFKW13] is an upper bound on the winning strategy for a particular game. In this game, Alice measures λ qubits each randomly in either the computational or Hadamard basis.

Theorem 3.4.4 ([TFKW13])**.**
Let $\lambda \in \mathbb{N}^+$ and define the following monogamy-of-entanglement game on $\mathcal{Q}(\lambda)$:

$$G_{BB84}^\lambda = \left\{ \left\{ M_x^\theta = |x^\theta\rangle\langle x^\theta| \right\}_{x \in \{0,1\}^n} \right\}_{\theta \in \{0,1\}^\lambda} \tag{3.4.6}$$

Then:

$$\omega_{G_{BB84}^n} = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}} \right)^\lambda < 0.86^\lambda \tag{3.4.7}$$

We note that the bound in Theorem 3.4.4 can be saturated, or met, by a strategy requiring no entanglement between Bob and Charlie. We define the state

$$|b_0\rangle = \cos\left(\frac{\pi}{8}\right)|0\rangle + \sin\left(\frac{\pi}{8}\right)|1\rangle = \cos\left(\frac{\pi}{8}\right)|+\rangle - \sin\left(\frac{\pi}{8}\right)|-\rangle \tag{3.4.8}$$

and note that:

$$|\langle b_0|0\rangle|^2 = |\langle b_0|+\rangle|^2 = \cos^2\left(\frac{\pi}{8}\right) = \frac{1}{2} + \frac{1}{2\sqrt{2}} \tag{3.4.9}$$

In a sense, $|b_0\rangle$ can be thought of as being halfway between $|0\rangle$ (corresponding to an angle of 0) and $|+\rangle$ (corresponding to an angle of $\pi/4$). So, to saturate the bound, Bob and Charlie send λ times the state $|b\rangle\langle b|$ to Alice and will guess that she obtained

the result corresponding to the all 0 bit string.

Note that we can also define the state

$$|b_1\rangle = \cos\left(\frac{-3\pi}{8}\right)|0\rangle + \sin\left(\frac{-3\pi}{8}\right)|1\rangle \tag{3.4.10}$$

so that $\{|b_0\rangle, |b_1\rangle\}$ forms an orthonormal basis of $\mathcal{Q}$ which we call the *Breidbart basis*. This basis can be thought of as being "midway" between the computational and Hadamard bases. We illustrate this in Figure 3.3.

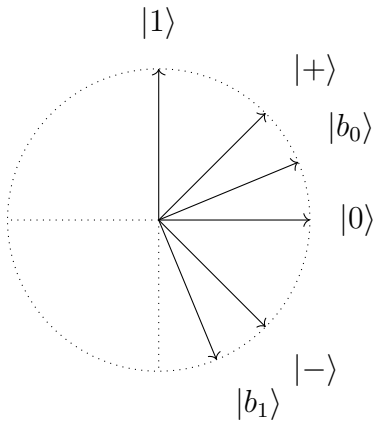


Figure 3.3: Representation of the computational, Hadamard, and Breidbart bases.

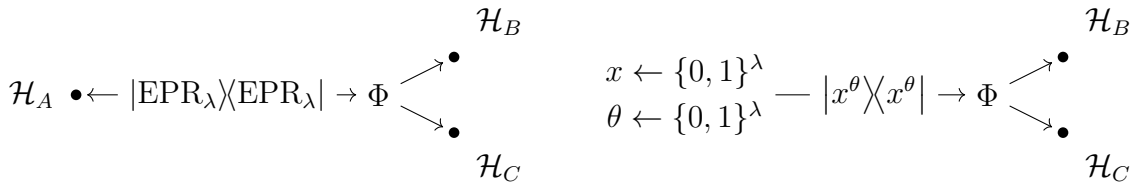
We now consider a different game. In this game, instead of sharing a tripartite entangled state, Alice will generate a Wiesner state and will send it to Bob and Charlie.

Game 2 (Guessing Wiesner States)**.**
Let $\lambda \in \mathbb{N}^+$ be an integer. We define the following game between a referee (Alice) and two adversaries (Bob and Charlie). Note that Bob and Charlie begin the game together.

1. Alice samples $\theta \leftarrow \{0,1\}^\lambda$ and $x \leftarrow \{0,1\}^\lambda$ uniformly at random.
2. Alice prepares the state $\rho = \left|x^\theta\right\rangle\!\left\langle x^\theta\right|$ and sends it to Bob and Charlie.
3. Bob and Charlie may communicate and perform arbitrary computations on ρ.

4. Bob and Charlie are then separated and may no longer communicate.
5. Alice announces θ to both Bob and Charlie.
6. Bob and Charlie then each produce a guess for x. Let $x_B, x_C \in \{0,1\}^\lambda$ be these guesses.
7. Bob and Charlie win if and only if $x = x_A = x_B$.

We can relate the winning probability of this game to the winning probability of the BB84 monogamy-of-entanglement game. We do this in the following corollary and illustrate the two scenarios in Figure 3.4.



(a) A quantum state for a MoEG is created by generating EPR pairs and giving one half of each pair to a CPTP map.

(b) A randomly chosen Wiesner state is sent into a CPTP map and the result is shared by two adversaries.

Figure 3.4: Illustration of the two scenarios related in Corollary 3.4.1.

Corollary 3.4.1.
Let $\lambda \in \mathbb{N}^+$. Then, for any Hilbert spaces $\mathcal{H}_B$ and $\mathcal{H}_C$, any families of POVMs

$$\left\{\left\{\mathcal{B}^\theta = \{B_x^\theta\}_{x\in\{0,1\}^\lambda}\right\}_{\theta\in\{0,1\}^\lambda}\right\} \qquad \left\{\left\{\mathcal{C}^\theta = \{C_x^\theta\}_{x\in\{0,1\}^\lambda}\right\}_{\theta\in\{0,1\}^\lambda}\right\} \tag{3.4.11}$$

on $\mathcal{H}_B$ and $\mathcal{H}_C$ (respectively), and any CPTP map $\Phi : \mathcal{D}(\mathcal{Q}(\lambda)) \to \mathcal{D}(\mathcal{H}_B \otimes \mathcal{H}_C)$ we have that

$$\mathop{\mathbb{E}}_x \mathop{\mathbb{E}}_\theta \mathrm{Tr}\left[\left(B_x^\theta \otimes C_x^\theta\right) \Phi\left(|x^\theta\rangle\langle x^\theta|\right)\right] \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^\lambda. \tag{3.4.12}$$

Proof: The idea for this proof is that the measurements and the CPTP map can be used to define a strategy for the monogamy-of-entanglement game in Theorem 3.4.4.

The state used for this strategy is given by

$$(\mathbb{1} \otimes \Phi) \left|\mathrm{EPR}_\lambda\right\rangle\!\left\langle\mathrm{EPR}_\lambda\right| \in \mathcal{D}(\mathcal{Q}(\lambda) \otimes \mathcal{H}_B \otimes \mathcal{H}_C). \tag{3.4.13}$$

Theorem 3.4.4 then gives us the bound:

$$\frac{1}{2^\lambda} \sum_{\theta \in \{0,1\}^\lambda} \sum_{x \in \{0,1\}^\lambda} \mathrm{Tr}\left[\left(\left|x^\theta\right\rangle\!\left\langle x^\theta\right| \otimes B_x^\theta \otimes C_x^\theta\right) (\mathbb{1} \otimes \Phi) \left|\mathrm{EPR}_\lambda\right\rangle\!\left\langle\mathrm{EPR}_\lambda\right|\right] \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^\lambda. \tag{3.4.14}$$

It then suffices to show that the left hand side of this inequality is equal to the quantity we wish to bound.

Observe that, for any fixed $\theta \in \{0,1\}^\lambda$, we have

$$\left|\mathrm{EPR}_\lambda\right\rangle\!\left\langle\mathrm{EPR}_\lambda\right| = \frac{1}{2^\lambda} \sum_{s \in \{0,1\}^\lambda} \sum_{r \in \{0,1\}^\lambda} \left|s^\theta\right\rangle\!\left\langle r^\theta\right| \otimes \left|s^\theta\right\rangle\!\left\langle r^\theta\right|. \tag{3.4.15}$$

Thus, for any fixed values of $x, \theta \in \{0,1\}^n$, we have that

$$\mathrm{Tr}\left[\left(\left|x^\theta\right\rangle\!\left\langle x^\theta\right| \otimes B_x^\theta \otimes C_x^\theta\right) (\mathbb{1} \otimes \Phi) \left|\mathrm{EPR}_\lambda\right\rangle\!\left\langle\mathrm{EPR}_\lambda\right|\right] \tag{3.4.16}$$

$$= \mathrm{Tr}\left[\left(\left|x^\theta\right\rangle\!\left\langle x^\theta\right| \otimes B_x^\theta \otimes C_x^\theta\right) (\mathbb{1} \otimes \Phi) \left(\frac{1}{2^\lambda} \sum_s \sum_r \left|s^\theta\right\rangle\!\left\langle r^\theta\right| \otimes \left|s^\theta\right\rangle\!\left\langle r^\theta\right|\right)\right] \tag{3.4.17}$$

and, using the linearity of the operators, we may bring the sums outside of the trace to obtain

$$= \frac{1}{2^\lambda} \sum_s \sum_r \mathrm{Tr}\left[\left(\left|x^\theta\right\rangle\!\left\langle x^\theta\right| \otimes B_x^\theta \otimes C_x^\theta\right) (\mathbb{1} \otimes \Phi) \left(\left|s^\theta\right\rangle\!\left\langle r^\theta\right| \otimes \left|s^\theta\right\rangle\!\left\langle r^\theta\right|\right)\right] \tag{3.4.18}$$

so that when we apply our operators, we obtain

$$= \frac{1}{2^\lambda} \sum_s \sum_r \mathrm{Tr}\left[\left(\left|x^\theta\right\rangle \left\langle x^\theta | s^\theta\right\rangle \left\langle r^\theta\right|\right) \otimes \left(\left(B_x^\theta \otimes C_x^\theta\right) \Phi\left(\left|s^\theta\right\rangle\!\left\langle r^\theta\right|\right)\right)\right] \tag{3.4.19}$$

and, recalling that the trace of a tensor product is the product of the traces yields

$$= \frac{1}{2^\lambda} \sum_s \sum_r \mathrm{Tr}\left[\left|x^\theta\right\rangle \left\langle x^\theta | s^\theta\right\rangle \left\langle r^\theta\right|\right] \cdot \mathrm{Tr}\left[\left(B_x^\theta \otimes C_x^\theta\right) \Phi\left(\left|s^\theta\right\rangle\!\left\langle r^\theta\right|\right)\right]. \tag{3.4.20}$$

Note that, using the cyclic property of the trace, $\mathrm{Tr}\left[\left|x^\theta\right\rangle\left\langle x^\theta\right|s^\theta\right\rangle\left\langle r^\theta\right|\right] = \left\langle x^\theta\right|s^\theta\left\rangle\left\langle r^\theta\right|x^\theta\right\rangle$ and that this product is 1 if $x = r = s$ and 0 otherwise as these are all elements of the same orthonormal basis for $\mathcal{Q}(\lambda)$. Thus,

$$\mathrm{Tr}\left[\left(\left|x^\theta\right\rangle\!\left\langle x^\theta\right| \otimes B_x^\theta \otimes C_x^\theta\right)(\mathbb{1}\otimes\Phi)\left|\mathrm{EPR}_\lambda\right\rangle\!\left\langle\mathrm{EPR}_\lambda\right|\right] = \frac{1}{2^\lambda}\,\mathrm{Tr}\left[\left(B_x^\theta \otimes C_x^\theta\right)\Phi\left(\left|x^\theta\right\rangle\!\left\langle x^\theta\right|\right)\right]. \tag{3.4.21}$$

which implies that

$$\begin{aligned}\frac{1}{2^\lambda}\sum_{\theta\in\{0,1\}^\lambda}\sum_{x\in\{0,1\}^\lambda} &\mathrm{Tr}\left[\left(\left|x^\theta\right\rangle\!\left\langle x^\theta\right| \otimes B_x^\theta \otimes C_x^\theta\right)(\mathbb{1}\otimes\Phi)\left|\mathrm{EPR}_\lambda\right\rangle\!\left\langle\mathrm{EPR}_\lambda\right|\right] \\ &= \mathop{\mathbb{E}}_x \mathop{\mathbb{E}}_\theta \mathrm{Tr}\left[\left(B_x^\theta \otimes C_x^\theta\right)\Phi\left(\left|x^\theta\right\rangle\!\left\langle x^\theta\right|\right)\right]\end{aligned} \tag{3.4.22}$$

which concludes the proof. ∎

We emphasize that the correspondence between "sending random Wiesner states" and "sharing EPR pairs which will be later measured" is not new. This technique was popularized by the Shor-Preskill proof of security of the BB84 protocol [SP00]. In their proof, Shor and Preskill relate the security of the BB84 protocol (which sends Wiesner states) to the security of a protocol with shared EPR pairs.

Chapter 4

Uncloneable Encryption

In this chapter, we describe *quantum encryptions of classical messages* (Definition 4.1.1) and define a few security notions for them, including the notions which formalize uncloneable encryption (Definitions 4.1.3 and 4.1.4).

We then present two concrete schemes for the quantum encryption of classical messages. The first, Scheme 4.3.1, is a simple protocol which will not be a good uncloneable encryption scheme. We will use it to explore our definitions and to justify looking for something better. Our second proposal, Scheme 4.4.1, can be seen as a way to construct an uncloneable encryption scheme from any quantum-secure pseudorandom function.

Our main original contributions in this chapter are the security notions given in Definitions 4.1.3 and 4.1.4 and the remarks concerning them, specifically Theorems 4.2.1 and 4.2.2. The remaining definitions, Definitions 4.1.1 and 4.1.2, are slight variations of concepts already known which have been restated and adapted for our context. One of the encryption schemes that we give, Scheme 4.4.1, is novel but the other, Scheme 4.3.1, has already appeared implicitly in the literature.

4.1 Formal Definitions

4.1.1 Quantum Encryption of Classical Messages Schemes

Succinctly, a quantum encryption of classical messages scheme is an encryption protocol for classical messages which produces quantum ciphertexts. Our formal definition can be seen as a generalization of definition 5.1.1 of [Gol04] which allows quantum

ciphertexts with classical keys and classical plaintexts. We add the restriction, also mentioned in [Gol04], of fixed plaintext lengths for any given value of the security parameter λ.

Definition 4.1.1 (Quantum Encryption of Classical Messages)**.**
Let $\ell : \mathbb{N}^+ \to \mathbb{N}^+$. An $\ell(\lambda)$-quantum encryption of classical messages ($\ell(\lambda)$-QECM) scheme $\mathcal{S}$ is composed of three polynomial-time circuits,

$$\mathcal{S} = \left(\{K_\lambda\}_{\lambda\in\mathbb{N}^+}, \{E_\lambda\}_{\lambda\in\mathbb{N}^+}, \{D_\lambda\}_{\lambda\in\mathbb{N}^+}, \right). \tag{4.1.1}$$

For any fixed value of $\lambda \in \mathbb{N}^+$, the corresponding circuits implicitly define three Hilbert spaces:

1. *A key space $\mathcal{H}_{K,\lambda} = \mathcal{Q}(p_K(\lambda))$.*
2. *A plaintext space $\mathcal{H}_{M,\lambda} = \mathcal{Q}(\ell(\lambda))$.*
3. *A ciphertext space $\mathcal{H}_{T,\lambda} = \mathcal{Q}(p_T(\lambda))$.*

The functions p_K and p_T are polynomially bounded functions and give, respectively, the key size and the cipher text size for any given λ. Finally, $\ell(\lambda)$ gives the length of the messages that can be encrypted.

Assuming that the value of λ is fixed and omitted for clarity, we require the following:

1. *K, called the key-generation circuit, implements a CPTP map of the form*

$$K : \mathcal{D}(\mathbb{C}) \to \mathcal{D}(\mathcal{H}_K). \tag{4.1.2}$$

2. *E, called the encryption circuit, implements a CPTP map of the form*

$$E : \mathcal{D}(\mathcal{H}_K \otimes \mathcal{H}_M) \to \mathcal{D}(\mathcal{H}_T). \tag{4.1.3}$$

3. *D, called the decryption circuit, implements a CPTP map of the form*

$$D : \mathcal{D}(\mathcal{H}_K \otimes \mathcal{H}_T) \to \mathcal{D}(\mathcal{H}_M). \tag{4.1.4}$$

We will also require that for all $\lambda \in \mathbb{N}^+$*, all* $m \in \{0,1\}^{\ell(\lambda)}$*, and all* $k \in \{0,1\}^{p_K(\lambda)}$ *such that*

$$\mathrm{Tr}\left[\, |k\rangle\langle k|\, K_\lambda(1)\right] > 0 \tag{4.1.5}$$

we have

$$\mathrm{Tr}\left[\, |m\rangle\langle m|\, D_\lambda\big(\, |k\rangle\langle k| \otimes E_\lambda\left(|k\rangle\langle k| \otimes |m\rangle\langle m|\right)\big)\right] = 1 \tag{4.1.6}$$

which is to say that our scheme is correct.

A few remarks on the key-generation circuits are in order. First, the key-generation circuits takes no input. This is represented by having $\mathcal{D}(\mathbb{C})$ as domain. Recall that $\mathbb{C}$ may be thought of as the state space of a system of zero qubit. In particular, there is a single density operator on $\mathbb{C}$: $\mathcal{D}(\mathbb{C}) = \{1\}$.

Second, the keys in a QECM can be thought of as classical bit strings and not quantum states. To obtain a key, a party runs the circuit $\mathtt{K}_\lambda$, *i.e.*, evaluates $K_\lambda(1)$, and measures the resulting state in the computation basis. The result of the measurement is the key.

Using a polynomial-time circuit for key-generation, instead of a classical probabilistic polynomial-time algorithm, allows us to describe this procedure in the same language as the encryption and decryption procedures. Moreover, if we allow our honest users to have access to quantum circuits for encryption and decryption, it is reasonable to expect them to have access to quantum circuits for key generation.

The fact that the scheme is correct guaranteed that any message encrypted with the scheme will be correctly decrypted when the same key is used.

4.1.2 Security Notions

We define three security notions.

- Definition 4.1.2: Indistinguishable security, abbreviated as IND-security.
- Definition 4.1.3: Uncloneable security, abbreviated as UNC-security.
- Definition 4.1.4: Uncloneable-indistinguishable security, abbreviated as UNC-IND-security.

Each of these definitions will be preceded by a game describing interactions between a referee and some adversaries. These games are *not* our formal definitions of security, but rather tools to help illustrate and interpret the formal definitions.

We emphasize that the first notion, IND-security, is not new and has been previously studied, both in the classical and quantum contexts. However, it is essentially the weakest security notion that an encryption scheme should satisfy. Thus, we introduce it here to highlight that our implementation of an uncloneable encryption scheme is also an encryption scheme.

The last two security notions are new.

4.1.2.1 Indistinguishable Security

Our definition of indistinguishable security for an $\ell(\lambda)$-QECM scheme is a reformulation of the standard indistinguishable security notion for private-key encryption schemes. In the purely classical case, *i.e.*, encrypting classical messages into classical ciphertexts, a version of this security notion can be found in definition 5.2.14 of [Gol04]. In the purely quantum case, *i.e.*, encrypting quantum states into quantum ciphertexts, a version of this security notion can be found in definition 7 of [ABF+16].

Our particular definition will be a slightly modified version of the one given in [ABF+16]. Our modifications will account for the fact that this is a private-key and not a public-key encryption scheme as well as the fact that the plaintexts must be classical bit strings and not arbitrary quantum states.

Conceptually, we can think of indistinguishable security via the following game.

Game 3 (Indistinguishable Security as a Game)**.**
Let $\mathcal{S}$ be an $\ell(\lambda)$-QECM. Let $\lambda \in \mathbb{N}^+$ and define $n = \ell(\lambda)$. We consider the following game played by a referee, Alice, against a single adversary, Eve.

1. Eve generates a classical message $m \in \{0,1\}^n$ and sends it to Alice.
2. Alice gets a key k by measuring $K_\lambda(1)$ in the computational basis.
3. Alice samples a bit $b \leftarrow \{0,1\}$ uniformly at random.
4. Depending on the value of b, Alice does one of two things:
   (a) If $b = 0$, Alice encrypts the all zero bit string $\mathbf{0}$ with k and obtains the state $\rho = E_\lambda(|k\rangle\langle k| \otimes |\mathbf{0}\rangle\langle\mathbf{0}|)$
   (b) If $b = 1$, Alice encrypts m with k and obtains $\rho = E_\lambda(|k\rangle\langle k| \otimes |m\rangle\langle m|)$.
5. Alice sends ρ to Eve.

6. Eve outputs a bit b' and wins if and only if $b' = b$.

We formalize this game and the possible strategies for the adversary in the following definition. We sketch the relation between all Hilbert spaces and CPTP maps given from Definition 4.1.2 in Figure 4.1.

Definition 4.1.2 (Indistinguishable Security)**.**
Let $\mathcal{S}$ be an $\ell(\lambda)$-QECM scheme as described in Definition 4.1.1. An IND-attack on this scheme is defined by two polynomial-time quantum circuits

$$\mathcal{A} = \left\{ \{\mathtt{A}_\lambda\}_{\lambda\in\mathbb{N}^+}, \{\mathtt{G}_\lambda\}_{\lambda\in\mathbb{N}^+} \right\} \tag{4.1.7}$$

such that, for every fixed λ, $\mathtt{G}$ implements a CPTP map of the form

$$G : \mathcal{D}(\mathbb{C}) \to \mathcal{D}(\mathcal{H}_S \otimes \mathcal{H}_M) \tag{4.1.8}$$

and $\mathtt{A}$ implements a CPTP map of the form

$$A : \mathcal{D}(\mathcal{H}_S \otimes \mathcal{H}_T) \to \mathcal{D}(\mathcal{Q}) \tag{4.1.9}$$

where $\mathcal{H}_{S,\lambda} = \mathcal{Q}(p_S(\lambda))$ and p_S is a polynomially bounded function.

For $b \in \{0,1\}$ and $k \in \{0,1\}^{p_K(\lambda)}$, define the CPTP map $E_k^b : \mathcal{D}(\mathcal{H}_M) \to \mathcal{D}(\mathcal{H}_T)$ by

$$E_k^0(\rho) = E_k\big(|\mathbf{0}\rangle\langle\mathbf{0}| \big) \tag{4.1.10}$$

and

$$E_k^1(\rho) = E_k\left(\sum_{m\in\{0,1\}^{\ell(\lambda)}} \mathrm{Tr}\left[|m\rangle\langle m| \, \rho \right] |m\rangle\langle m| \right) \tag{4.1.11}$$

where $E_k(\rho) = E(|k\rangle\langle k| \otimes \rho)$. Then, the success probability of this attack is defined by

$$\omega_{\mathcal{A}}^{IND}(\lambda) = \mathop{\mathbb{E}}_{b} \mathop{\mathbb{E}}_{k\leftarrow\mathcal{K}} \mathrm{Tr}\left[|b\rangle\langle b| \, A\left(\mathbb{1}_S \otimes E_k^b \right) G(1) \right] \tag{4.1.12}$$

where λ is implicit on the right-hand side and $\mathcal{K}$ is the random variable satisfying

$$\Pr[\mathcal{K} = k] = \mathrm{Tr}\left[|k\rangle\langle k| \, K(1) \right]. \tag{4.1.13}$$

We say that $\mathcal{S}$ is IND-secure if for all IND-attacks $\mathcal{A}$ there exists a negligible function $\eta_{\mathcal{A}}$ such that

$$\omega_{\mathcal{A}}^{IND}(\lambda) \leq \frac{1}{2} + \eta_{\mathcal{A}}(\lambda). \tag{4.1.14}$$

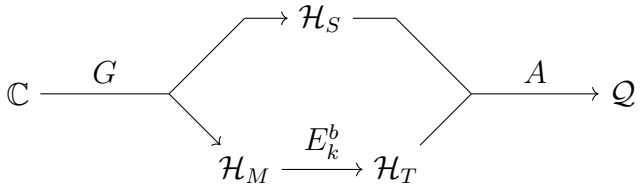


Figure 4.1: Relation between the CPTP maps and Hilbert spaces considered in an indistinguishable attack as described in Definition 4.1.2.

If the CPTP map E_k^0 naturally corresponds to the behaviour of the referee in Game 3 in the case of $b = 0$, it is little less clear how E_k^1 corresponds to their behaviour in the case of $b = 1$. We think of E_k^1 as of first measuring a state $\rho \in \mathcal{DQ}(\ell(\lambda))$ in the computational basis and then encrypting the resulting classical bit string with the key k.

The reason we impose this measurement on E_k^1 is two fold. First, QECM schemes are used to encrypt classical messages, not arbitrary quantum states. Second, it is easier in our formalism to place the measurement in the hands of the referee instead of the adversary. Indeed, this lets us define the adversaries as polynomial-time quantum circuits with less restrictions on their outputs. Even if we did require $\mathtt{G}_\lambda$ to produce strictly classical messages, these could still be seen as the result of a measurement in the computational basis of some quantum state.

Finally, we note that the register $\mathcal{H}_S$ is used by the adversary to hold any information it wishes between the task of generating a message and the task of generating its output.

4.1.2.2 Uncloneable Security

Uncloneable security is our first novel security notion. It captures what we believe to be the simplest notion of uncloneable encryptions.

Conceptually, this security definition is described by the following game.

Game 4 (Uncloneable Security as a Game)**.**
Let $\mathcal{S}$ be an $\ell(\lambda)$-QECM scheme. Let $\lambda \in \mathbb{N}^+$ and define $n = \ell(\lambda)$. We consider the following game played by a referee, Alice, against two collaborating adversaries who begin the game together, Bob and Charlie.

1. Alice samples, uniformly at random, a message $m \leftarrow \{0,1\}^n$.
2. Alice gets a key k by measuring $K_\lambda(1)$ in the computational basis.
3. Alice encrypts m with k by generating the state $\rho = E_\lambda(|k\rangle\langle k| \otimes |m\rangle\langle m|)$.
4. Alice sends ρ to Bob and Charlie.
5. Bob and Charlie complete some computations which may use ρ. They are then separated and may no longer communicate.
6. Alice broadcasts k to both Bob and Charlie.
7. Bob outputs some $m_B \in \{0,1\}^n$ and Charlie outputs some $m_C \in \{0,1\}^n$.
8. Bob and Charlie win if and only if $m = m_B = m_C$.

Note that there is a strategy for Bob and Charlie that always wins with probability 2^{-n}: always guess the all zero bit string as the message. Alternatively, one of Bob or Charlie could keep the complete and unchanged ciphertext and decrypt it correctly when they receive the key. The other player would then have a probability of 2^{-n} to correctly guess the plaintext.

We will say that the QECM scheme $\mathcal{S}$ is $t(n)$-uncloneable secure if Bob and Charlie's probability of winning is always bounded by $t(n) \cdot 2^{-n} + \eta(\lambda)$ for some negligible function η.

We formalize this game, its strategies, and its winning probability in the following definition. We sketch the relation between all CPTP maps and Hilbert spaces given in Definition 4.1.3 in Figure 4.2.

Definition 4.1.3 (Uncloneable Security)**.**
Let $\mathcal{S}$ be an $\ell(\lambda)$-QECM scheme as described in Definition 4.1.1 and let $n = \ell(\lambda)$ implicitly depend on λ. An UNC-attack $\mathcal{A}$ on this scheme is defined by three polynomial-

time quantum circuits,

$$\mathcal{A} = \big(\{\mathtt{A}_\lambda\}_{\lambda\in\mathbb{N}^+}, \{\mathtt{B}_\lambda\}_{\lambda\in\mathbb{N}^+}, \{\mathtt{C}_\lambda\}_{\lambda\in\mathbb{N}^+}\big). \tag{4.1.15}$$

For any fixed value of $\lambda \in \mathbb{N}^+$, we require that

1. $\mathtt{A}$ *implements a CPTP map for the form*

$$A : \mathcal{D}(\mathcal{H}_T) \to \mathcal{D}(\mathcal{H}_B \otimes \mathcal{H}_C) \tag{4.1.16}$$

2. *and* $\mathtt{B}$ *and* $\mathtt{C}$ *implement CPTP maps of the form*

$$B : \mathcal{D}(\mathcal{H}_K \otimes \mathcal{H}_B) \to \mathcal{D}(\mathcal{H}_M) \qquad C : \mathcal{D}(\mathcal{H}_K \otimes \mathcal{H}_C) \to \mathcal{D}(\mathcal{H}_M) \tag{4.1.17}$$

for some Hilbert spaces $\mathcal{H}_B = \mathcal{Q}(p_B(\lambda))$ and $\mathcal{H}_C = \mathcal{Q}(p_C(\lambda))$ where p_B and p_C are polynomially bounded functions.

We define the success probability of this attack by

$$\omega_{\mathcal{A}}^{UNC}(\lambda) = \mathop{\mathbb{E}}_{m}\mathop{\mathbb{E}}_{k\leftarrow\mathcal{K}} \mathrm{Tr}\left[\Big(\,|m\rangle\langle m| \otimes |m\rangle\langle m|\,\Big)\Big(B_k \otimes C_k\Big)A\Big(E_k(|m\rangle\langle m|)\Big)\right] \tag{4.1.18}$$

where $\mathcal{K}$ is the random variable satisfying

$$\Pr[\mathcal{K} = k] = \mathrm{Tr}\left[|k\rangle\langle k|\, K(1)\right] \tag{4.1.19}$$

and B_k, C_k, and E_k are the CPTP maps defined by:

$$B_k(\rho) = B(|k\rangle\langle k| \otimes \rho) \qquad C_k(\rho) = C(|k\rangle\langle k| \otimes \rho) \qquad E_k(\rho) = E(|k\rangle\langle k| \otimes \rho) \tag{4.1.20}$$

We say that $\mathcal{S}$ is $t(n)$-uncloneable secure if, for every attack $\mathcal{A}$, there is a negligible function $\eta_{\mathcal{A}}$ such that:

$$\omega_{\mathcal{A}}^{UNC}(\lambda) \leq t(n) \cdot 2^{-n} + \eta_{\mathcal{A}}(\lambda) \tag{4.1.21}$$

If $\mathcal{S}$ is 1-uncloneable secure, we simply say that it is uncloneable secure.

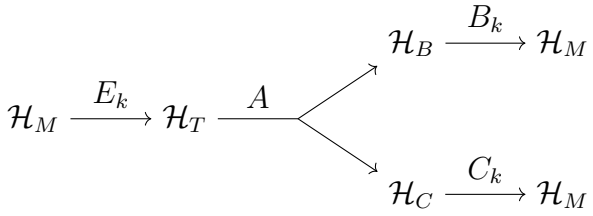


Figure 4.2: Relation between the CPTP maps and Hilbert spaces considered in an uncloneable attack as described in Definition 4.1.3.

We emphasize that whenever $t(n) < 2^n$, the QECM scheme achieves something that is simply impossible for classical encryption schemes. Indeed, for any encryption scheme which produces classical ciphertexts, there is an UNC-attack which succeeds with certainty. It suffices for $\mathtt{A}_\lambda$ to make two copies of the ciphertext and $\mathtt{B}_\lambda$ and $\mathtt{C}_\lambda$ to behave as honest receivers. This translates to $\eta_{\mathcal{A}}(\lambda) = 0$ and $t(n) = 2^n$.

4.1.2.3 Uncloneable-Indistinguishable Secure

Uncloneable-indistinguishable security can be seen as a combination of the standard indistinguishable security and the novel uncloneable security notions.

Game 5 (Uncloneable-Indistinguishable Security as a Game)**.**
Let $\mathcal{S}$ be an $\ell(\lambda)$-QECM scheme. Let $\lambda \in \mathbb{N}^+$ and define $n = \ell(\lambda)$. We consider the following game played by a referee, Alice, against collaborating adversaries who begin the game together, Bob and Charlie.

1. Bob and Charlie pick a message $m \in \{0,1\}^n$ and sent it to Alice.
2. Alice gets a key k by measuring $K_\lambda(1)$ in the computational basis.
3. Alice samples a bit $b \leftarrow \{0,1\}$ uniformly at random.
4. Depending on the value of b, Alice does one of two things:
   (a) If $b = 0$, Alice encrypts the all zero bit string $\mathbf{0}$ with k and obtains the state $\rho = E_\lambda(|k\rangle\langle k| \otimes |\mathbf{0}\rangle\langle\mathbf{0}|)$
   (b) If $b = 1$, Alice encrypts m with k and obtains $\rho = E_\lambda(|k\rangle\langle k| \otimes |m\rangle\langle m|)$.
5. Alice sends ρ to Bob and Charlie.

6. Bob and Charlie complete some computations which may use ρ. They are then separated and may no longer communicate.

7. Alice broadcasts k to both Bob and Charlie.

8. Bob and Charlie each outputs a bit $b_B, b_C \in \{0,1\}$.

9. Bob and Charlie win if and only if $b = b_B = b_C$.

We now formalize this game and the possible strategies that Bob and Charlie may implement. We sketch all Hilbert spaces and CPTP maps defined here in Figure 4.3.

Definition 4.1.4 (Uncloneable-Indistinguishable Security)**.**
Let $\mathcal{S}$ be a $\ell(\lambda)$-QECM scheme as described in Definition 4.1.1 and let $n = \ell(\lambda)$ implicitly depend on λ. An UNC-IND-attack $\mathcal{A}$ on this scheme is defined by four polynomial-time circuits,

$$\mathcal{A}' = \left(\{\mathtt{G}_\lambda\}_{\lambda\in\mathbb{N}^+}\{\mathtt{A}_\lambda\}_{\lambda\in\mathbb{N}^+}\{\mathtt{B}_\lambda\}_{\lambda\in\mathbb{N}^+}\{\mathtt{C}_\lambda\}_{\lambda\in\mathbb{N}^+}\right). \tag{4.1.22}$$

For any fixed value of $\lambda \in \mathbb{N}^+$, we require that

1. *$\mathtt{G}$ implements a CPTP map of the form*

$$G : \mathcal{D}(\mathbb{C}) \to \mathcal{D}(\mathcal{H}_S \otimes \mathcal{H}_M), \tag{4.1.23}$$

2. *$\mathtt{A}$ implements a CPTP map of the form*

$$A : \mathcal{D}(\mathcal{H}_S \otimes \mathcal{H}_T) \to \mathcal{D}(\mathcal{H}_B \otimes \mathcal{H}_C), \tag{4.1.24}$$

3. *and $\mathtt{B}$ and $\mathtt{C}$ implement CPTP maps of the form*

$$B : \mathcal{D}(\mathcal{H}_K \otimes \mathcal{H}_B) \to \mathcal{D}(\mathcal{Q}) \qquad C : \mathcal{D}(\mathcal{H}_K \otimes \mathcal{H}_C) \to \mathcal{D}(\mathcal{Q}) \tag{4.1.25}$$

for some Hilbert spaces $\mathcal{H}_S = \mathcal{Q}(p_S(\lambda))$, $\mathcal{H}_B = \mathcal{Q}(p_B(\lambda))$, and $\mathcal{H}_C = \mathcal{Q}(p_C(\lambda))$ where the function p_S, p_B, and p_C are polynomially bounded.

For each value of $b \in \{0,1\}$ and all possible keys $k \in \{0,1\}^{p_K(\lambda)}$, we define the CPTP maps $E_k^b : \mathcal{D}(\mathcal{H}_M) \to \mathcal{D}(\mathcal{H}_T)$ as in Definition 4.1.2.

We define the success probability of this attack by

$$\omega_{\mathcal{A}'}^{\textit{UNC-IND}}(\lambda) = \mathop{\mathbb{E}}_{b} \mathop{\mathbb{E}}_{k\leftarrow\mathcal{K}} \operatorname{Tr}\left[\Big(|b\rangle\langle b| \otimes |b\rangle\langle b|\Big)\Big(B_k \otimes C_k\Big) A\left(\mathbb{1}_S \otimes E_k^b\right) G(1)\right] \tag{4.1.26}$$

where k is distributed according to the random variable $\mathcal{K}$ defined by

$$\Pr[\mathcal{K} = k] = \operatorname{Tr}[|k\rangle\langle k|\, K(1)] \tag{4.1.27}$$

and B_k, C_k, and E_k are the CPTP maps defined by

$$B_k(\rho) = B(|k\rangle\langle k| \otimes \rho) \qquad C_k(\rho) = C(|k\rangle\langle k| \otimes \rho) \qquad E_k(\rho) = E(|k\rangle\langle k| \otimes \rho). \tag{4.1.28}$$

We say that $\mathcal{S}$ is $t(n)$-uncloneable-indistinguishable secure if for every UNC-IND-attack $\mathcal{A}$ there is a negligible function $\eta_{\mathcal{A}}$ such that

$$\omega_{\mathcal{A}}^{\textit{UNC-IND}}(\lambda) \leq t(n) \cdot \frac{1}{2} + \eta_{\mathcal{A}}(\lambda). \tag{4.1.29}$$

If $\mathcal{S}$ is 1-uncloneable-indistinguishable secure, we simply say that it is uncloneable-indistinguishable secure.

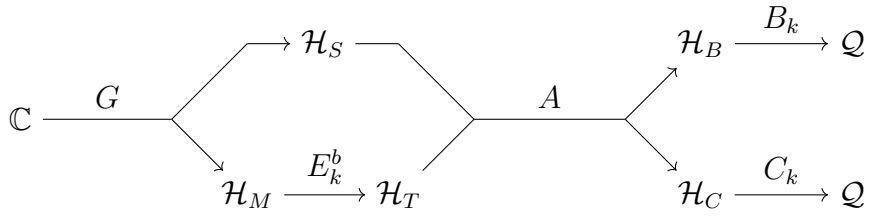


Figure 4.3: Relation between the CPTP maps and Hilbert spaces considered in an uncloneable-indistinguishable attack as described in Definition 4.1.4.

4.2 Relations Among Security Notions

A natural question to ask is if there exists any relations between our different notions of uncloneable security. We give two such relations.

4.2.1 UNC-IND-Security Implies IND-Security

UNC-IND-security is a strictly stronger notion then IND-security. Indeed, if an adversary is able to distinguish without the key, there is no need to wait until the key is revealed.

Theorem 4.2.1.
Let $\mathcal{S}$ be an $\ell(\lambda)$-QECM scheme that is UNC-IND-secure. Then, $\mathcal{S}$ is IND-secure.

Formally, any IND-attack naturally gives rise to an IND-UNC attack where the `B` and `C` circuits do nothing but carryover the answer given by the `A` circuit. That is to say that they do not use their knowledge of the key in any way. We can then use the bound on the winning probability of an UNC-IND-attack to obtain a bound on the winning probability of the IND-attack.

Proof: Let

$$\mathcal{A} = \big(\{\mathtt{G}_\lambda\}_{\lambda\in\mathbb{N}^+}, \{\mathtt{A}_\lambda\}_{\lambda\in\mathbb{N}^+}\big)$$

be an IND-attack on $\mathcal{S}$. We construct an IND-UNC-attack

$$\mathcal{A}' = \big(\{\mathtt{G'}_\lambda\}_{\lambda\in\mathbb{N}^+}, \{\mathtt{A'}_\lambda\}_{\lambda\in\mathbb{N}^+}, \{\mathtt{B'}_\lambda\}_{\lambda\in\mathbb{N}^+}, \{\mathtt{C'}_\lambda\}_{\lambda\in\mathbb{N}^+}\big)$$

from $\mathcal{A}$ in the following way:

1. There is no change to the message generation circuit, so $\mathtt{G'}_\lambda = \mathtt{G}_\lambda$.

2. We obtain the $\mathtt{A'}_\lambda$ circuit from $\mathtt{A}_\lambda$ by adding a measurement in the computational basis at the end and making two copies of the result. In other words,

$$A'_\lambda(\rho) = \sum_{b\in\{0,1\}} \mathrm{Tr}\left[\,|b\rangle\langle b|\,A(\rho)\right]|b\rangle\langle b|\otimes|b\rangle\langle b|\,. \tag{4.2.1}$$

   One of these copies will be sent to the $\mathtt{B'}_\lambda$ circuit and the other to $\mathtt{C'}_\lambda$.

3. Both $\mathtt{B'}_\lambda$ and $\mathtt{C'}_\lambda$ circuits do nothing with the key, and so $B' = C' = \big(\mathrm{Tr}_K \otimes \mathbb{1}_{\mathcal{Q}}\big)$.

Since $\mathcal{S}$ is UNC-IND secure, we have the existence of a negligible function $\eta_{\mathcal{A}'}$ such that for any $\lambda \in \mathbb{N}^+$

$$\mathop{\mathbb{E}}_{k\leftarrow\mathcal{K}} \mathop{\mathbb{E}}_{b} \mathrm{Tr}\left[\big(\,|b\rangle\langle b|\otimes|b\rangle\langle b|\,\big)\big(B'_k\otimes C'_k\big)A'\big(\mathbb{1}_S\otimes E^b_k\big)G'(1)\right] \leq \frac{1}{2} + \eta_{\mathcal{A}'}(\lambda). \tag{4.2.2}$$

Let us examine the trace on the left-hand side for fixed values of b and k. Since B'_k and C'_k are the identity, G' is exactly G, and recalling the definition of A' we rewrite this trace as

$$\begin{aligned}
&\mathrm{Tr}\left[\left(|b\rangle\langle b|\otimes|b\rangle\langle b|\right)\left(\sum_{b'\in\{0,1\}}\mathrm{Tr}\left[|b'\rangle\langle b'|\,A\left(\left(\mathbb{1}_S\otimes E_k^b\right)G(1)\right)\right]|b'\rangle\langle b'|\otimes|b'\rangle\langle b'|\right)\right]\\
&=\sum_{b'\in\{0,1\}}\mathrm{Tr}\left[|b'\rangle\langle b'|\,A\left(\left(\mathbb{1}_S\otimes E_k^b\right)G(1)\right)\right]\mathrm{Tr}\left[(|b\rangle\langle b|\otimes|b\rangle\langle b|)(|b'\rangle\langle b'|\otimes|b'\rangle\langle b'|)\right]\\
&=\mathrm{Tr}\left[|b\rangle\langle b|\,A\left(\left(\mathbb{1}_S\otimes E_k^b\right)G(1)\right)\right]
\end{aligned}\tag{4.2.3}$$

where the first equality comes form the fact that the trace is a linear operator and the second equality comes from the fact that

$$\mathrm{Tr}\left[(|b\rangle\langle b|\otimes|b\rangle\langle b|)(|b'\rangle\langle b'|\otimes|b'\rangle\langle b'|)\right]=\langle b|b'\rangle^2\cdot\langle b|b'\rangle^2=\begin{cases}0 & \text{if } b\neq b'\\ 1 & \text{if } b=b'.\end{cases}\tag{4.2.4}$$

So, we may write

$$\mathop{\mathbb{E}}_{k\leftarrow\mathcal{K}}\mathop{\mathbb{E}}_{b}\mathrm{Tr}\left[|b\rangle\langle b|\,A\left(\mathbb{1}_S\otimes E_k^b\right)G(1)\right]\leq\frac{1}{2}+\eta_{\mathcal{A}'}(\lambda).\tag{4.2.5}$$

Noting that the left-hand side of this equation is precisely the winning probability of the IND-attack $\mathcal{A}$ gives us our result. ∎

4.2.2 UNC Implies UNC-IND-Secure for Short Messages

A second implication is that a QECM scheme that is $t(n)$-UNC-secure is also $t(n)$-UNC-IND-secure if the allowed message size does not grow too quickly with λ.

Theorem 4.2.2.
Let $\ell:\mathbb{N}^+\to\mathbb{N}^+$ be a function such that there exists two integers $\lambda',k\in\mathbb{N}^+$ which satisfy $\lambda\geq\lambda'\implies\ell(\lambda)\leq k\log_2(\lambda)$. Then, a $\ell(\lambda)$-QECM scheme which is $t(n)$-UNC secure is also $t(n)$-UNC-IND secure.

Proof: The proof technique is similar to the proof of Theorem 4.2.1. From any

IND-UNC-attack $\mathcal{A}$, we can construct an UNC-attack $\mathcal{A}'$ and by hypothesis bound its success probability. Then, relating the success probabilities of $\mathcal{A}$ and $\mathcal{A}'$ will conclude the proof.

Let

$$\mathcal{A} = \left(\{\mathtt{G}_\lambda\}_{\lambda\in\mathbb{N}^+}, \{\mathtt{A}_\lambda\}_{\lambda\in\mathbb{N}^+}, \{\mathtt{B}_\lambda\}_{\lambda\in\mathbb{N}^+}, \{\mathtt{C}_\lambda\}_{\lambda\in\mathbb{N}^+}\right)$$

be an UNC-IND-attack against $\mathcal{S}$. We give a high level description of the induced UNC-attack $\mathcal{A}'$ and we will compute its winning probability in Game 4, the interpretation of our formal notion of uncloneable security. We fix λ and $n = \ell(\lambda)$.

`A'`: Run the `G` circuit to generate the state $G(1) \in \mathcal{D}(\mathcal{H}_S \otimes \mathcal{H}_M)$. Measure the $\mathcal{H}_M$ subsystem in the computational basis to obtain a result $m \in \{0,1\}^n$. For any particular string m, this occurs with probability

$$p_m = \mathrm{Tr}\left[\left(\mathbb{1}_S \otimes |m\rangle\langle m|\right) G(1)\right] \tag{4.2.6}$$

and the resulting post-measurement state is given by

$$G_m = \frac{1}{p_m}\left(\mathbb{1}_S \otimes |m\rangle\langle m|_M\right) G(1) \left(\mathbb{1}_S \otimes |m\rangle\langle m|_M\right) \in \mathcal{D}(\mathcal{H}_S \otimes \mathcal{H}_M). \tag{4.2.7}$$

Discard the $\mathcal{H}_M$ subsystem and call the resulting state σ_m. In other words,

$$\sigma_m = \mathrm{Tr}_M\left(G_m\right) \in \mathcal{D}(\mathcal{H}_S). \tag{4.2.8}$$

Obtain the state $\rho \in \mathcal{D}(\mathcal{H}_T)$ which was given as input and output the state given by

$$A(\sigma_m \otimes \rho)_{BC} \otimes |m\rangle\langle m|_{B'} \otimes |m\rangle\langle m|_{C'}\,. \tag{4.2.9}$$

Send the $\mathcal{H}_B$, $\mathcal{H}_{B'}$ subsystems to `B'` and the $\mathcal{H}_C$, $\mathcal{H}_{C'}$ subsystems to `C'`. Formally, $\mathtt{A}'$ implements the CPTP map given by

$$A'(\rho) = \sum_{m\in\{0,1\}^n} p_m \cdot A(\sigma_m \otimes \rho)_{BC} \otimes |m\rangle\langle m|_{B'} \otimes |m\rangle\langle m|_{C'}\,. \tag{4.2.10}$$

`B'`: Receive the $\mathcal{H}_B$ and $\mathcal{H}_{B'}$ subsystems. Run the `B` circuit on the $\mathcal{H}_B$ subsystem and receive a single qubit. Measure the qubit in the computational basis. If the result is 1, output the state found in the $\mathcal{H}_{B'}$ subsystem. If the result is 0,

output $|\mathbf{0}\rangle\langle\mathbf{0}|$, where $\mathbf{0}$ is the all 0 bit string.

`C'`: Analogous to `B'`.

In short, the induced UNC-attack $\mathcal{A}'$ described above simply hopes that the random message that the referee decided to encrypt is the same that it would have given to the referee in the UNC-IND game.

In a single execution of the UNC-attack $\mathcal{A}'$ as described above, there are three measurements and two random choices. The choices are the random message m' that is chosen to be encrypted by the referee and the random key k that is used for that encryption. The three measurements are when `A'` measures the $\mathcal{H}_M$ register of the state $G(1)$ to obtain some string m and when `B'` and `C'` measure the qubit given by their execution of the `B` and `C` circuits.

Looking at the result of these three measurements and the random choice of message m' is sufficient to determine if $\mathcal{A}'$ succeeded or not, which is to say if the circuits `B'` and `C'` have both produced the correct bit.

Indeed, let $\mathcal{B}$ and $\mathcal{C}$ be the random variables which model the result of the measurements made by `B'` and `C'`. Let $\mathcal{M}$ be the random variable which models the result of the measurement `A'` makes. Let $\mathcal{E}$ be the random variable which models the message to be encrypted and $\mathcal{K}$ be the random variable that models the key to be used.

The conditions for the attack being successful are the following.

1. $\mathcal{B} = \mathcal{C} = 1$ and $\mathcal{E} = \mathcal{M}$, since if $\mathcal{B} = \mathcal{C} = 1$, `B'` and `C'` will output the message measured by `A'`, which was the same that was encrypted since $\mathcal{A} = \mathcal{M}$.

2. Or, for similar reasons, $\mathcal{B} = \mathcal{C} = 0$ and $\mathcal{E} = \mathbf{0}$.

3. Or, for similar reasons, $\mathcal{B} \neq \mathcal{C}$ and $\mathcal{E} = \mathcal{M} = \mathbf{0}$.

It can be seen that the random variables $\mathcal{M}$, $\mathcal{E}$, and $\mathcal{K}$ are all independent of each other, but that $\mathcal{B}$ and $\mathcal{C}$ depend on the values of the other random variables. Indeed, the values of $\mathcal{M}$, $\mathcal{E}$, and $\mathcal{K}$ dictate the state that the `B` and `C` circuits will receive and that the `B'` and `C'` circuits will eventually measure. Specifically, we observe that for any $b \in \{0,1\}$, any $m, m' \in \{0,1\}^n$, and any key k, we have that

$$\begin{aligned} &\Pr\left[\mathcal{B} = b \wedge \mathcal{C} = b | \mathcal{M} = m \wedge \mathcal{E} = m' \wedge \mathcal{K} = k\right] \\ &\qquad = \mathrm{Tr}\left[\big(\,|b\rangle\langle b| \otimes |b\rangle\langle b|\,\big)\big(B_k \otimes C_k\big) A\big(\sigma_m \otimes E_k(|m'\rangle\langle m'|)\big)\right]. \end{aligned} \tag{4.2.11}$$

We can then express the winning probability of the UNC-attack $\mathcal{A}'$ by:

$$\begin{aligned}\Bigg(\sum_m \Pr\left[\mathcal{B}=1\wedge\mathcal{C}=1\wedge\mathcal{M}=m\wedge\mathcal{E}=m\right]\Bigg)\\ +\Pr\left[\mathcal{B}=0\wedge\mathcal{C}=0\wedge\mathcal{E}=\mathbf{0}\right]\\ +\Pr\left[\mathcal{B}=1\wedge\mathcal{C}=0\wedge\mathcal{M}=\mathbf{0}\wedge\mathcal{E}=\mathbf{0}\right]\\ +\Pr\left[\mathcal{B}=0\wedge\mathcal{C}=1\wedge\mathcal{M}=\mathbf{0}\wedge\mathcal{E}=\mathbf{0}\right] \quad \leq t(n)\cdot 2^{-n}+\eta(\lambda)\end{aligned} \tag{4.2.12}$$

where the upper bound is provided by our assumption that the scheme is $t(n)$-UNC secure. By removing two terms, this implies that

$$\begin{aligned}\Bigg(\sum_m \Pr\left[\mathcal{B}=1\wedge\mathcal{C}=1\wedge\mathcal{M}=m\wedge\mathcal{E}=m\right]\Bigg)\\ +\Pr\left[\mathcal{B}=0\wedge\mathcal{C}=0\wedge\mathcal{E}=\mathbf{0}\right] \quad \leq t(n)\cdot 2^{-n}+\eta(\lambda)\end{aligned} \tag{4.2.13}$$

so, noting that $\Pr[\mathcal{M}=m]=p_m$ and $\Pr[\mathcal{E}=m]=2^{-n}$ for any m, we may write

$$\begin{aligned}\Bigg(\sum_m \frac{1}{2^n}p_m\Pr\left[\mathcal{B}=1\wedge\mathcal{C}=1|\mathcal{M}=m\wedge\mathcal{E}=m\right]\Bigg)\\ +\frac{1}{2^n}\Pr\left[\mathcal{B}=0\wedge\mathcal{C}=0|\mathcal{E}=\mathbf{0}\right] \quad \leq t(n)\cdot 2^{-n}+\eta(\lambda)\end{aligned} \tag{4.2.14}$$

and

$$\begin{aligned}\frac{1}{2}\Bigg(\sum_m p_m\Pr\left[\mathcal{B}=1\wedge\mathcal{C}=1|\mathcal{M}=m\wedge\mathcal{E}=m\right]\Bigg)\\ +\frac{1}{2}\Pr\left[\mathcal{B}=0\wedge\mathcal{C}=0|\mathcal{E}=\mathbf{0}\right] \quad \leq t(n)\cdot\frac{1}{2}+2^{n-1}\eta(\lambda).\end{aligned} \tag{4.2.15}$$

It then suffices to note the left-hand side of the above equation is precisely the success probability of the UNC-IND attack.

So, the success probability of $\mathcal{A}$ is upper bounded by $t(n)\cdot\frac{1}{2}+2^{n-1}\eta(\lambda)$. By assumption on $n=\ell(\lambda)$, we have that $2^{n-1}\eta(\lambda)$ is eventually bounded by $\frac{1}{2}k\lambda\eta(\lambda)$, which is a negligible function of λ. ∎

4.3 Uncloneable Encryption via Conjugate Coding

As we saw in Section 3.4, specifically with Corollary 3.4.1, a conjugate encoding offers a source of "uncloneability" for classical strings, even when the basis chosen for the encoding is later revealed. We can use this property to obtain a simple uncloneable encryption scheme.

This type of scheme, which combines Wiesner's conjugate encoding and a one-time pad has already appeared in the literature (*e.g.*, [Got03, BBB14]). Those versions are also a little bit more sophisticated and also add a layer of error-correction. We do not add this component.

We emphasize that this will *not* be a good uncloneable encryption scheme. However, it will be an instructive toy example with which we can start comparing concrete schemes against our definitions. It will also justify looking for something better and offer an introduction to some of the proof techniques that are used later.

Scheme 4.3.1 (Conjugate Encryption)**.**
Let $\ell : \mathbb{N}^+ \to \mathbb{N}^+$ be the function defined by $\lambda \mapsto \lambda$. Let $n = \ell(\lambda) = \lambda$. Recall that for all strings $s, \theta \in \{0,1\}^n$, $\left|s^\theta\right\rangle = \bigotimes_{i=1}^n H^{\theta_i} |s_i\rangle$. The conjugate encryption scheme is defined by the following circuits.

Algorithm 1 The key generation circuit.

procedure $\mathtt{K}_\lambda()$
  Sample $\theta \leftarrow \{0,1\}^\lambda$ uniformly at random.
  Sample $r \leftarrow \{0,1\}^\lambda$ uniformly at random.
  Output $|\theta\rangle\langle\theta| \otimes |r\rangle\langle r|$.
end procedure

Algorithm 2 The encryption circuit.

procedure $\mathtt{E}_\lambda(\theta, r, m)$
  Generate $\rho = \left|(m \oplus r)^\theta\right\rangle\!\left\langle(m \oplus r)^\theta\right|$.
  Output ρ.
end procedure

Algorithm 3 The decryption circuit.

procedure $\mathtt{D}_\lambda(\theta, r, \rho)$
Compute $\rho' = H^\theta \rho H^\theta$.
Measure ρ' in the computational basis and call the result c.
Compute $m' = c \oplus r$.
Output m'.
end procedure

It fairly simple to see that this scheme is correct. The encryption of any message m with the key (θ, r) produces the state $\left|(m \oplus r)^\theta\right\rangle\!\left\langle(m \oplus r)^\theta\right|$. When given to the decryption circuit with the same key, we first compute

$$\rho' = H^\theta \left|(m \oplus r)^\theta\right\rangle\!\left\langle(m \oplus r)^\theta\right| H^\theta = |m \oplus r\rangle\langle m \oplus r| \tag{4.3.1}$$

and so the measurement in the computational basis gives $m \oplus r$. The final exclusive-or with r then gives us m.

The above scheme is also IND-secure. At a high level this is true due to the "one-time pad" nature of this scheme. In particular, we can see that averaged over all keys the ciphertext is independent of the plain text. We formally demonstrate this bellow. The proof is novel in the sense that this protocol has not been studied in our framework before. However, the main ideas of the proof are not new and fall back very directly to the proof of security of the one-time pad.

Theorem 4.3.2.
The conjugate encryption scheme (Scheme 4.3.1) is IND-secure.

Proof: Let $\mathcal{A} = \left(\{\mathtt{G}_\lambda\}_{\lambda\in\mathbb{N}^+}, \{\mathtt{A}_\lambda\}_{\lambda\in\mathbb{N}^+}\right)$ be an IND-attack. Recall that, for a fixed and implicit $\lambda \in \mathbb{N}^+$, the success probability of this attack is given by

$$\omega = \mathop{\mathbb{E}}_{\theta}\mathop{\mathbb{E}}_{r}\mathop{\mathbb{E}}_{b} \mathrm{Tr}\left[\, |b\rangle\langle b|\, A\big(\mathbb{1}_S \otimes E^b_{r,\theta}\big) G(1)\right]. \tag{4.3.2}$$

We claim that $\omega = 1/2$, which implies IND-security.

Using the linearity of the trace and expending the expectation over r, we have

that

$$\omega = \mathop{\mathbb{E}}_{\theta} \mathop{\mathbb{E}}_{b} \operatorname{Tr}\left[|b\rangle\langle b| \, A \left(\mathbb{1}_S \otimes \frac{1}{2^n} \sum_{r \in \{0,1\}^n} E^b_{r,\theta} \right) \rho \right]. \tag{4.3.3}$$

We will show that for any fixed θ, the CPTP maps $E^0_{r,\theta}$ and $E^1_{r,\theta}$ are identical when averaged over the values of r, which is to say that

$$\frac{1}{2^n} \sum_{r \in \{0,1\}^n} E^0_{r,\theta} = \frac{1}{2^n} \sum_{r \in \{0,1\}^n} E^1_{r,\theta}. \tag{4.3.4}$$

By definition of $E^0_{\theta,r}$ and for any $\rho \in \mathcal{D}(\mathcal{H}_M)$, we have that

$$\frac{1}{2^n} \sum_{r \in \{0,1\}^n} E^0_{r,\theta}(\rho) = \frac{1}{2^n} \sum_{r \in \{0,1\}^n} E_{\theta,r}(|\mathbf{0}\rangle\langle\mathbf{0}|) = \frac{1}{2^n} \sum_{r \in \{0,1\}^n} \left| r^\theta \right\rangle\!\left\langle r^\theta \right|. \tag{4.3.5}$$

We claim that the same holds for $E^1_{\theta,r}$. We first show this for states of the form $|s\rangle\langle s|$ for any $s \in \{0,1\}^n$. We may write

$$\begin{aligned}
\frac{1}{2^n} \sum_{r \in \{0,1\}^n} E^0_{r,\theta}(|s\rangle\langle s|) &= \frac{1}{2^n} \sum_{r \in \{0,1\}^n} E_{r,\theta} \left(\sum_{m \in \{0,1\}^n} \operatorname{Tr}\left[|m\rangle\langle m| \, |s\rangle\langle s| \right] |m\rangle\langle m| \right) \\
&= \frac{1}{2^n} \sum_{r \in \{0,1\}^n} E_{r,\theta} \left(|s\rangle\langle s| \right) \\
&= \frac{1}{2^n} \sum_{r \in \{0,1\}^n} \left| (s \oplus r)^\theta \right\rangle\!\left\langle (s \oplus r)^\theta \right| \\
&= \frac{1}{2^n} \sum_{r \in \{0,1\}^n} \left| r^\theta \right\rangle\!\left\langle r^\theta \right|.
\end{aligned} \tag{4.3.6}$$

Then, for any state $\rho \in \mathcal{D}(\mathcal{H}_M)$ and using the linearity of CPTP maps, we have that

$$\begin{aligned}\frac{1}{2^n}\sum_{r\in\{0,1\}^n} E^0_{r,\theta}(\rho) &= \sum_{m\in\{0,1\}^n} \mathrm{Tr}\left[\,|m\rangle\langle m|\,\rho\right]\left(\frac{1}{2^n}\sum_{r\in\{0,1\}^n} E^0_{r,\theta}(|m\rangle\langle m|)\right)\\ &= \sum_{m\in\{0,1\}^n} \mathrm{Tr}\left[\,|m\rangle\langle m|\,\rho\right]\left(\frac{1}{2^n}\sum_{r\in\{0,1\}^n} \left|r^\theta\right\rangle\!\left\langle r^\theta\right|\right)\\ &= \frac{1}{2^n}\sum_{r\in\{0,1\}^n} \left|r^\theta\right\rangle\!\left\langle r^\theta\right|\end{aligned} \tag{4.3.7}$$

where the last equality comes from the fact that

$$\sum_{m\in\{0,1\}^n} \mathrm{Tr}\left[\,|m\rangle\langle m|\,\rho\right] = \mathrm{Tr}\left[\left(\sum_{m\in\{0,1\}^n} |m\rangle\langle m|\right)\rho\right] = \mathrm{Tr}\left[\rho\right] = 1. \tag{4.3.8}$$

In fact, we note that $\frac{1}{2^n}\sum_{r\in\{0,1\}^n} \left|r^\theta\right\rangle\!\left\langle r^\theta\right| = \frac{1}{2^n}\mathbb{1}$ is also independent of θ. It then follows that

$$A\left(\mathbb{1}_S \otimes \frac{1}{2^n}\sum_{r\in\{0,1\}^n} E^b_{r,\theta}\right) G(1) \tag{4.3.9}$$

does not depend on the value of b or θ. So, we denote the above quantity by ρ and may then write

$$\omega = \mathop{\mathbb{E}}_{\theta}\frac{1}{2}\,\mathrm{Tr}\left[\left(\sum_{b\in\{0,1\}} |b\rangle\langle b|\right)\rho\right] = \mathop{\mathbb{E}}_{\theta}\frac{1}{2} = \frac{1}{2} \tag{4.3.10}$$

which concludes the proof. ∎

We can give an upper bound on the UNC-security of the above scheme.

Theorem 4.3.3.
The conjugate encryption scheme (Scheme 4.3.1) is $\left(1+\frac{1}{\sqrt{2}}\right)^n$*-UNC-secure.*

Proof: Let

$$\mathcal{A} = \left(\{\mathtt{A}_\lambda\}_{\lambda\in\mathbb{N}^+}, \{\mathtt{B}_\lambda\}_{\lambda\in\mathbb{N}^+}, \{\mathtt{C}_\lambda\}_{\lambda\in\mathbb{N}^+}\right) \tag{4.3.11}$$

be an UNC-attack on the conjugate encryption scheme. We claim that for any fixed and implicit value of $\lambda \in \mathbb{N}^+$, the winning probability of this attack

$$\omega = \mathop{\mathbb{E}}_{\theta} \mathop{\mathbb{E}}_{r} \mathop{\mathbb{E}}_{m} \operatorname{Tr}\left[\left(|m\rangle\langle m| \otimes |m\rangle\langle m|\right)\left(B_{\theta,r} \otimes C_{\theta,r}\right) A\left(\left|(m \oplus r)^{\theta}\right\rangle\left\langle(m \oplus r)^{\theta}\right|\right)\right] \tag{4.3.12}$$

can be upper bounded by $\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n$. This value will be coming in from Corollary 3.4.1. Indeed, using Proposition 2.1.10 with the expectation over m and noting that $s \mapsto r \oplus s$ is a permutation, we have

$$\omega = \mathop{\mathbb{E}}_{\theta} \mathop{\mathbb{E}}_{r} \mathop{\mathbb{E}}_{m} \operatorname{Tr}\left[\left(|m \oplus r\rangle\langle m \oplus r| \otimes |m \oplus r\rangle\langle m \oplus r|\right)\left(B_{\theta,r} \otimes C_{\theta,r}\right) A\left(\left|m^{\theta}\right\rangle\left\langle m^{\theta}\right|\right)\right]. \tag{4.3.13}$$

Suppose, for a contradiction, that $\omega > \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n$. Then, there must be one particular value of $r' \in \{0,1\}^n$ such that

$$\mathop{\mathbb{E}}_{\theta} \mathop{\mathbb{E}}_{m} \operatorname{Tr}\left[\left(\pi^m \otimes \pi^m\right)\left(B_{\theta,r'} \otimes C_{\theta,r'}\right) A\left(\left|m^{\theta}\right\rangle\left\langle m^{\theta}\right|\right)\right] > \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n \tag{4.3.14}$$

where $\pi^m = |m \oplus r'\rangle\langle m \oplus r'|$.

Now, using Theorem 2.2.27, we can purify the actions of $B_{\theta,r'}$ and $C_{\theta,r'}$. For both values $L \in \{B, C\}$, let $\mathcal{H}_{L'}$ and $\mathcal{H}_{L''}$ be Hilbert spaces such that

$$\mathcal{H}_L \otimes \mathcal{H}_{L''} \simeq \mathcal{H}_M \otimes \mathcal{H}_{L'}. \tag{4.3.15}$$

Let $U_L^{\theta,r'} \in \mathcal{U}(\mathcal{H}_L \otimes \mathcal{H}_{L''})$ be a unitary operator and $|\text{aux-}L\rangle\langle\text{aux-}L| \in \mathcal{D}(\mathcal{H}_{L''})$ be a state such that

$$L_{\theta,r'}(\rho) = \operatorname{Tr}_{L'}\left(U_L^{\theta,r'}\left(\rho \otimes |\text{aux-}L\rangle\langle\text{aux-}L|\right)\left(U_L^{\theta,r'}\right)^{\dagger}\right) \tag{4.3.16}$$

for all $\rho \in \mathcal{D}(\mathcal{H}_L)$. Note that Theorem 2.2.27 guaranties that $\mathcal{H}'_L$, $\mathcal{H}_{L''}$, and $|\text{aux-}L\rangle$ are independent of θ and r'. Indeed, they depend only on the dimensions of the input and output spaces.

Defining the CPTP maps Φ by

$$\Phi(\rho) = A(\rho)_{BC} \otimes |\text{aux-}B\rangle\langle\text{aux-}B|_{B''} \otimes |\text{aux-}C\rangle\langle\text{aux-}C|_{C''} \tag{4.3.17}$$

lets us write

$$\begin{aligned}
&\left(\pi^m \otimes \pi^m\right)\left(B_{\theta,r'} \otimes C_{\theta,r'}\right) A\left(\left|m^\theta\right\rangle\!\left\langle m^\theta\right|\right) \\
&= \left(\pi^m \otimes \pi^m\right) \mathrm{Tr}_{B'C'}\left(\left(U_B^{\theta,r'} \otimes U_C^{\theta,r'}\right) \Phi(\left|m^\theta\right\rangle\!\left\langle m^\theta\right|) \left(U_B^{\theta,r'} \otimes U_C^{\theta,r'}\right)^\dagger\right) \\
&= \mathrm{Tr}_{B'C'}\left(\left(\pi_B^m \otimes \mathbb{1}_{B'} \otimes \pi_C^m \otimes \mathbb{1}_{C'}\right)\left(U_B^{\theta,r'} \otimes U_C^{\theta,r'}\right) \Phi(\left|m^\theta\right\rangle\!\left\langle m^\theta\right|) \left(U_B^{\theta,r'} \otimes U_C^{\theta,r'}\right)^\dagger\right).
\end{aligned} \tag{4.3.18}$$

This implies that

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\theta}\mathop{\mathbb{E}}_{m} \mathrm{Tr}_{BC}\left[\left(\pi^m \otimes \pi^m\right)\left(B_{\theta,r'} \otimes C_{\theta,r'}\right) A\left(\left|m^\theta\right\rangle\!\left\langle m^\theta\right|\right)\right] \\
&= \mathop{\mathbb{E}}_{\theta}\mathop{\mathbb{E}}_{m} \mathrm{Tr}_{BB'CC'}\left[\left(\pi_B^m \otimes \mathbb{1}_{B'} \otimes \pi_C^m \otimes \mathbb{1}_{C'}\right)\left(U_B^{\theta,r'} \otimes U_C^{\theta,r'}\right) \Phi(\left|m^\theta\right\rangle\!\left\langle m^\theta\right|) \left(U_B^{\theta,r'} \otimes U_C^{\theta,r'}\right)^\dagger\right] \\
&= \mathop{\mathbb{E}}_{\theta}\mathop{\mathbb{E}}_{m} \mathrm{Tr}_{BB'CC'}\left[\left(U_B^{\theta,r'} \otimes U_C^{\theta,r'}\right)^\dagger \left(\pi_B^m \otimes \mathbb{1}_{B'} \otimes \pi_C^m \otimes \mathbb{1}_{C'}\right)\left(U_B^{\theta,r'} \otimes U_C^{\theta,r'}\right) \Phi(\left|m^\theta\right\rangle\!\left\langle m^\theta\right|)\right] \\
&= \mathop{\mathbb{E}}_{\theta}\mathop{\mathbb{E}}_{m} \mathrm{Tr}_{BB'CC'}\left[\left(U_B^{\theta,r'}\left(\pi_B^m \otimes \mathbb{1}_{B'}\right)\left(U_B^{\theta,r'}\right)^\dagger\right) \otimes \left(U_C^{\theta,r'}\left(\pi_C^m \otimes \mathbb{1}_{C'}\right)\left(U_C^{\theta,r'}\right)^\dagger\right) \Phi(\left|m^\theta\right\rangle\!\left\langle m^\theta\right|)\right].
\end{aligned} \tag{4.3.19}$$

We then note that for any value of θ, the set

$$\left\{\left(U_B^{\theta,r'}\left(\pi^m \otimes \mathbb{1}_{B'}\right)\left(U_B^{\theta,r'}\right)^\dagger\right)\right\}_{m\in\{0,1\}^n} \tag{4.3.20}$$

is a POVM, in fact it is a projective measurement. Thus, Corollary 3.4.1 gives an upper bound of $\left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right)^n$ on the above value, which is a contradiction.

Thus,

$$\omega \leq \left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right)^n \tag{4.3.21}$$

which completes the proof. ∎

We note that there is an UNC-attack which gives the adversary a winning probability of precisely $\left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right)^n$.

If the A circuits measures each qubit received in the Breidbart basis given by

$$|b_0\rangle = \cos\left(\frac{\pi}{8}\right)|0\rangle + \sin\left(\frac{\pi}{8}\right)|1\rangle \quad \text{and} \quad |b_1\rangle = \cos\left(\frac{-3\pi}{8}\right)|0\rangle + \sin\left(\frac{-3\pi}{8}\right)|1\rangle \tag{4.3.22}$$

then it can be shown that A will obtain the string $m \oplus r$ with probability $\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n$. Recall that this basis also appeared in the optimal strategy for the BB84 monogamy-of-entanglement game in Section 3.4.3. Indeed, let c_i be the i^{th} bit of $m \oplus r$ which was encoded in the basis designated by θ_i. The probability that A obtains the correct value of c_i if $\theta_i = 0$, which is to say that c_i was sent in the computational basis, is given by

$$|\langle b_{c_i}|c_i\rangle|^2 = \begin{cases} |\langle b_0|0\rangle|^2 = \cos^2(\pi/8) = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) & \text{if } c_i = 0 \\ |\langle b_1|1\rangle|^2 = \sin^2(-3\pi/8) = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) & \text{if } c_i = 1 \end{cases} \tag{4.3.23}$$

and if $\theta_i = 1$, which is to say that c_i was sent in the Hadamard basis, is given by

$$|\langle b_{c_i}|c_i\rangle|^2 = \begin{cases} |\langle b_0| H |0\rangle|^2 = \left(\frac{\cos(\pi/8)+\sin(\pi/8)}{\sqrt{2}}\right)^2 = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) & \text{if } c_i = 0 \\ |\langle b_1| H |1\rangle|^2 = \left(\frac{\cos(-3\pi/8)-\sin(-3\pi/8)}{\sqrt{2}}\right)^2 = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) & \text{if } c_i = 1. \end{cases} \tag{4.3.24}$$

Thus, A obtains each bit of $m \oplus r$ correctly with probability $\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)$.

The circuit A then passes the string it obtained to B and C who wait to receive r as part of the key to try to obtain the message m.

4.4 Our New Protocol

Our first attempt at a QECM scheme which offers uncloneable or even uncloneable-indistinguishable security was not quite optimal. We now offer a better QECM scheme.

Scheme 4.4.1 ($\mathcal{F}$-Conjugate Encryption)**.**
Let $\ell : \mathbb{N}^+ \to \mathbb{N}^+$ be a function. Let

$$\mathcal{F} = \left\{ f_\lambda : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^{\ell(\lambda)} \right\}_{\lambda \in \mathbb{N}^+} \tag{4.4.1}$$

be a quantum-secure pseudorandom function. We define the $\mathcal{F}$-uncloneable encryption scheme as the $\ell(\lambda)$-QECM given by the following algorithms.

Algorithm 4 The key generation circuit.

procedure $\mathtt{K}_\lambda()$
    Sample $\theta \xleftarrow{U} \{0,1\}^\lambda$ uniformly at random.
    Sample $s \xleftarrow{U} \{0,1\}^\lambda$ uniformly at random.
    Output $|\theta\rangle\langle\theta| \otimes |s\rangle\langle s|$.
end procedure

Algorithm 5 The encryption circuit.

procedure $\mathtt{E}_\lambda(\theta, s, m)$
    Sample $r \leftarrow \{0,1\}^\lambda$ uniformly at random.
    Generate $\rho = \left|r^\theta\right\rangle\!\left\langle r^\theta\right|$.
    Compute $c = m \oplus f_\lambda(s, r)$.
    Output $|c\rangle\langle c| \otimes \rho$.
end procedure

Algorithm 6 The decryption circuit.

procedure $\mathtt{D}_{n,\lambda}(\theta, s, c, \rho)$
    Compute $\rho' = H^\theta \rho H^\theta$.
    Measure ρ' in the computational basis and call the result r'.
    Compute $m' = c \oplus f_\lambda(s, r')$.
    Output m'.
end procedure

The above QECM scheme resembles a standard construction of a classical private-key encryption scheme, secure under chosen plaintext attacks, from any pseudorandom function. We had discussed this construction in Section 3.3. We add a conjugate encoding to the random string that is chosen during the encryption.

We also note that the role of the pseudorandom function is quite different in our scheme. In the standard construction, the use of the pseudorandom function is to allow multiples uses of the same key. In our construction, the pseudorandom function is used to "distill" the uncloneability of a string. Indeed, we saw that with Wiesner's conjugate encoding, the probability that both parties may guess a string of length λ was $\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^\lambda$. If, instead, we ask them to guess the output of the pseudorandom

function on that string, we hope to approach a probability of 2^{-n} where n is the output length.

It is simple to show that this scheme is correct.

If the message $m \in \{0,1\}^{\ell(\lambda)}$ was encrypted with the key (θ, s), then the ciphertext is the state $|f_\lambda(s,r) \oplus m\rangle\langle f_\lambda(s,r) \oplus m| \otimes |r^\theta\rangle\langle r^\theta|$.

So, during decryption with the correct key, the application of the Hadamard operators gives the state $|f_\lambda(s,r) \oplus m\rangle\langle f_\lambda(s,r) \oplus m| \otimes |r\rangle\langle r|$. Thus, the measurement in the computational basis gives the strings $f_\lambda(s,r) \oplus m$ and r. Finally, doing the necessary evaluation of the pseudorandom function and the exclusive-or gives us the correct message m.

The fact that this scheme is IND-secure essentially follows the standard proof of security of the classical analogue of this scheme. This can be found in a standard textbook, such as [Gol04], but we still give an overview of this proof.

Theorem 4.4.2.
Scheme 4.4.1 is IND-secure.

Proof: Consider an IND-attack $\mathcal{A} = \{\{\mathtt{G}_\lambda\}_{\lambda\in\mathbb{N}^+}, \{\mathtt{A}_\lambda\}_{\lambda\in\mathbb{N}^+}\}$ against this scheme.

If the quantum-secure pseudorandom function are replaced by functions truly drawn at random from $\mathrm{Bool}(\lambda, \ell(\lambda))$, then the state given by $\mathtt{A}$ to $\mathtt{B}$ and $\mathtt{C}$, averaged over the possible keys, can be shown to be identical in the cases of $b = 0$ and $b = 1$. This is done in a manner similar to the proof of Theorem 4.3.2. Thus, with random oracles, the success probability of any IND-attack is exactly $1/2$.

We can now use this IND-attack $\mathcal{A}$ to create a polynomial-time circuit $\{\mathtt{D}_\lambda\}_{\lambda\in\mathbb{N}^+}$ which tries to distinguish between being given access to the pseudorandom function or to a truly random function. To achieve this, $\mathtt{D}_\lambda$ simulates both the attack $\mathcal{A}$ and the encryption E_k^b. In other words, $\mathtt{D}_\lambda$ will act as both Alice and Eve from Game 3 and output the same bit as Alice does at the end of the game.

But, by assumption of $\mathcal{F}$ being a quantum-secure pseudorandom function, we have that

$$\left| \Pr_{s\leftarrow\{0,1\}^\lambda} \mathrm{Tr}\left[|0\rangle\langle 0|\, D_\lambda^{f_\lambda(s,\cdot)}(1)\right] - \Pr_{H\leftarrow\mathrm{Bool}(\ell_{\mathrm{In}}(\lambda),\ell_{\mathrm{Out}}(\lambda))} \mathrm{Tr}\left[|0\rangle\langle 0|\, D_\lambda^{H}(1)\right] \right| \leq \eta_{\mathtt{D}}(\lambda) \tag{4.4.2}$$

This implies that in the IND-security game, even if we use the quantum-secure

pseudorandom function instead of a truly random function, the probability that the adversary outputs 0 is essentially the same. Similarly, for 1.

Hence, there is a negligible function $\eta_{\mathcal{A}}$ such that the winning probability of $\mathcal{A}$ is bounded by $\frac{1}{2} + \eta_{\mathcal{A}}(\lambda)$. ∎

Chapter 5

Security Proof of Our Protocol

In this chapter, we prove the following claims:

1. Theorem 5.3.1: The QECM scheme described in Scheme 4.4.1 is 9-UNC secure if pseudorandom functions are modelled as random oracles.

2. Theorem 5.3.2: The QECM scheme described in Scheme 4.4.1 is UNC secure if pseudorandom functions are modelled as random oracles and the adversaries do not share entanglement.

When we model pseudorandom functions as random oracles, we gain two interesting tools for our proofs. First, looking at the expectation over all possible functions is simplified. Second, the adversaries can only interact with the function in a "black box" manner. Our proofs rely more on this second fact then the first.

Restricting the possibility of entanglement between adversaries may seem like an artificial limitation, but we claim that it is still a meaningful security notion. In particular, it captures all attacks where the quantum states in the ciphertext are measured prior to the key being revealed and only classical information is shared between the adversaries.

In Section 5.1, we state and prove a few technical facts, the most important of which is Proposition 5.1.4. In Section 5.2, we state prove two technical lemmas which will allow us to prove our two security claims in Section 5.3.

Essentially everything in this chapter is novel, except for the inspiration for the proof technics which were taken from [Unr15].

5.1 Some Propositions

The following propositions do not directly relate to quantum information or computation. However, they will codify a few algebraic manipulations and upper bounds which we will use in our security proofs. This will lighten the presentation of the security proofs.

5.1.1 Algebra

We formalize one algebraic manipulation.

Proposition 5.1.1.
Let $n \in \mathbb{N}^+$, R be a possibly noncommutative ring, and $a, b \in R$ with $a+b=c$. Then,

$$c^n = a^n + \sum_{k=0}^{n-1} a^{n-k-1} b c^k. \tag{5.1.1}$$

Proof: We proceed by induction on n. It is trivial to show that it is true for $n = 1$. Indeed, we have that

$$a^n + \sum_{k=0}^{n-1} a^{n-k-1} b c^k = a + \sum_{k=0}^{0} a^k b c^k = a + b = c = c^n. \tag{5.1.2}$$

Assume that the statement holds when $n = \ell$ for some $\ell \in \mathbb{N}^+$. We now show that it holds when $n = \ell + 1$. We have that

$$\begin{aligned} c^n = c^\ell c &= \left(a^\ell + \sum_{k=0}^{\ell-1} a^{\ell-k-1} b c^k \right) c \\ &= a^\ell a + a^\ell b + \sum_{k=0}^{\ell-1} a^{\ell-k-1} b c^{k+1} \\ &= a^{\ell+1} + a^{\ell-0} b c^0 + \sum_{k=1}^{\ell} a^{\ell-k} b c^k \\ &= a^{\ell+1} + \sum_{k=0}^{\ell} a^{\ell-k} b c^k \end{aligned} \tag{5.1.3}$$

which is what we want. ∎

5.1.2 Norms

We use the standard (*i.e.*: non-Dirac) notation for vectors in this subsection. This will make the numerous norms easier to read.

We first recall a standard lemma about the induced norm in inner product spaces.

Theorem 5.1.2 (Pythagoras)**.**
Let (V, f) be an inner product space. Let $a, b \in V$ such that $\langle a, b\rangle = 0$. Then,

$$\|a + b\|^2 = \|a\|^2 + \|b\|^2 \tag{5.1.4}$$

Proof: We may write

$$\|a + b\|^2 = \langle a + b, a + b\rangle = \langle a, a\rangle + \langle a, b\rangle + \langle b, a\rangle + \langle b, b\rangle = \|a\|^2 + \|b\|^2 \tag{5.1.5}$$

which concludes the proof. ∎

In our upcoming security proofs, it will be useful to have an lemma analogous to Theorem 5.1.2 to let us "split" the norm squared of a sum, even if the vectors are not orthogonal to one another.

Ultimately, we will obtain a bound of the form

$$\left\| a + \sum_{i=1}^{n} b_i \right\|^2 \leq \|a\|^2 + (5 + 2n) \sum_{i=1}^{n} \|b_i\| \tag{5.1.6}$$

when appropriate conditions are placed on the vectors. We will use this inequality to quantify the idea that for "small enough" values of $\|b_i\|$, $\|a + \sum b_i\|^2 \approx \|a\|^2$.

While it may not be possible to saturate the following inequalities, they give bounds that are good enough for our needs and it is easy to verify if they are applicable or not.

We first give a version for a single vector b_i and then generalize this to any number of b_i vectors. To our knowledge, these specific propositions do not appear elsewhere, but their proofs are fairly mechanical and no new insight is presented.

Proposition 5.1.3.
Let $\mathcal{H}$ be a Hilbert space, $c \in \mathbb{R}_0^+$ be a real, and $a, b \in \mathcal{H}$ two vectors such that $\|b\| \leq 1$ and $\|a+b\| \leq c$. Then,

$$\|a+b\|^2 \leq \|a\|^2 + (3+2c)\|b\|. \tag{5.1.7}$$

Proof: We show this by two uses of the triangle inequality. First,

$$\|a\| = \|a+b-b\| \leq \|a+b\| + \|-b\| \leq c+1. \tag{5.1.8}$$

Then, noting that $\|a+b\|^2 \leq (\|a\| + \|b\|)^2$,

$$\begin{aligned} \|a+b\|^2 &\leq \|a\|^2 + 2\|a\|\|b\| + \|b\|^2 \\ &\leq \|a\|^2 + 2\,(1+c)\,\|b\| + \|b\| \\ &\leq \|a\|^2 + (3+2c)\,\|b\| \end{aligned} \tag{5.1.9}$$

which is what we want. ∎

Proposition 5.1.4.
Let $\mathcal{H}$ be a Hilbert space and $n \in \mathbb{N}^+$ a positive integer. Let $\{a, b_1, \ldots, b_n\} \subseteq \mathcal{H}$ be a set of $n+1$ vectors such that $\|b_i\| \leq 1$ for all $i \in [n]$ and $\|a + \sum_{i=1}^n b_i\| \leq 1$. Then,

$$\left\| a + \sum_{i=1}^n b_i \right\|^2 \leq \|a\|^2 + (5+2n) \sum_{i=1}^n \|b_i\|. \tag{5.1.10}$$

Proof: We first note that for any $k \in [n]_0$ we have that

$$\left\| a + \sum_{i=1}^k b_i \right\| = \left\| a + \sum_{i=1}^n b_i - \sum_{i=k+1}^n b_i \right\| \leq \left\| a + \sum_{i=1}^n b_i \right\| + \sum_{i=k+1}^n \|b_i\| \leq 1+n. \tag{5.1.11}$$

Thus, for any $k \in [n]$ and using Proposition 5.1.3 we have that

$$\left\| a + \sum_{i=1}^k b_i \right\|^2 \leq \left\| a + \sum_{i=1}^{k-1} b_i \right\|^2 + (5+2n)\|b_k\|. \tag{5.1.12}$$

By applying n times the above inequality, essentially removing one b_i from the norm at a time, we may write

$$\left\| a + \sum_{i=1}^{n} b_i \right\|^2 \leq \|a\|^2 + (5+2n) \sum_{i=1}^{n} \|b_i\| \tag{5.1.13}$$

which is what we wanted. ∎

5.2 Two Lemmas

We now prove two useful lemmas. These lemmas are best expressed and proved in the pure formalism (*i.e.*: unitary operators on unit vectors) instead of the mixed formalism (*i.e.*: CPTP maps on density operators). These lemmas were inspired by Unruh's one-way-to-hiding lemma [Unr15]. One of the key differences between our lemmas and Unruh's is that we consider two adversaries instead of one.

These lemmas may be interpreted as follows. We consider two adversaries who have oracle access to a function $H \in \text{Bool}(\lambda, n)$ which is chosen uniformly at random. Their goal is to simultaneously guess the value $H(x)$ for some value of x. The adversaries share some quantum state which we interpret as representing all the information they may initially have on x. The lemmas relates the probability of both parties simultaneously guessing $H(x)$ to their probability of being able to both simultaneously guess x. In other words, we will bound their probability of guessing $H(x)$ by a function of their probability of guessing x.

The first of these lemmas, Lemma 5.2.1 imposes a restriction that the adversaries may not share entanglement, *i.e.*, their shared state must be separable. The second, Lemma 5.2.2, considers this problem in the most general setting.

We show that the probability that both adversaries correctly guess $H(x)$ is upper bounded by

$$\frac{1}{2^n} + Q \cdot M \qquad \text{or} \qquad 9 \cdot \frac{1}{2^n} + Q' \cdot M' \tag{5.2.1}$$

where Q and Q' are functions of the number of queries the adversaries make to the oracle and M and M' quantifies their probability of guessing x with a particular strategy. The factor of 9 is present only if we allow the adversaries to share entanglement.

5.2.1 Without Entanglement

We first state the lemma in the case where the adversaries may not share any entanglement. We begin with this lemma as its proof is simpler but conceptually similar to the case with entanglement.

Lemma 5.2.1.
Let $\lambda, n \in \mathbb{N}^+$ and let $x \in \{0,1\}^\lambda$. For $L \in \{B, C\}$, let

1. *$\mathcal{H}_L = \mathcal{H}_{L_S} \otimes \mathcal{Q}(\lambda)_{L_Q} \otimes \mathcal{Q}(n)_{L_R}$ be a Hilbert space,*
2. *$U_L \in \mathcal{U}(\mathcal{H}_L)$ be a unitary operator on $\mathcal{H}_L$,*
3. *$\{\pi_L^y\}_{y\in\{0,1\}^n}$ be a projective measurement on $\mathcal{H}_L$, and*
4. *$q_L \in \mathbb{N}^+$ be an integer.*

Then, for any separable pure state $|\psi\rangle = |\psi_B\rangle \otimes |\psi_C\rangle$ with $|\psi_L\rangle \in \mathcal{H}_L$, we have that

$$\omega = \mathop{\mathbb{E}}_{H} \left\| \left(\pi_B^{H(x)} \otimes \pi_C^{H(x)}\right) \left(\mathcal{O}^{U_B,H,q_B} \otimes \mathcal{O}^{U_C,H,q_C}\right) |\psi\rangle \right\|^2 \leq \frac{1}{2^n} + (5+2q)q\sqrt[4]{M} \quad (5.2.2)$$

where $q = q_B + q_C$ and

$$M = \mathop{\mathbb{E}}_{H} \mathop{\mathbb{E}}_{H'} \mathop{\mathbb{E}}_{k} \mathop{\mathbb{E}}_{\ell} \left\| \left(|x\rangle\langle x|_{B_Q} \otimes |x\rangle\langle x|_{C_Q}\right) \left(\mathcal{O}^{U_B,H,k} \otimes \mathcal{O}^{U_C,H',\ell}\right) |\psi\rangle \right\|^2 \quad (5.2.3)$$

with $k \in [q_B - 1]_0$, $\ell \in [q_C - 1]_0$, and $H, H' \in \mathrm{Bool}(\lambda, n)$.

We can interpret M in a manner very similar to its analogous quantity in Unruh's one-way-to-hiding lemma [Unr15]. The adversaries, instead of continuing until the end of their computation, will stop immediately before a certain (randomly chosen) query to the oracle and measure their query register in the computational basis. Then, M is the probability that this procedure succeeds at letting both adversaries simultaneously obtain x, averaged over the possible stopping points and possible functions implemented by the oracle.

Why is this lemma useful? In our security proof, we use Corollary 3.4.1 to show that M is a negligible function of λ in the scenario that we consider.

We note that, in M, the adversaries do not use the same oracle. However, this will not be an issue when we use this lemma in our upcoming security proof.

The proof proceeds in five steps. First, we argue that we only need to consider the adversary with the lowest probability of success. The reason we can easily do this is that $|\psi\rangle$ is separable. Next, we write that adversary's oracle computation as a sum of two operators. One of these operators will represent the "part" of the computation where the adversary queries the oracle on x. The other represents the "part" where the adversary does not query on x. Third, we use Proposition 5.1.4 to split the contribution of these two operators into different norms. Fourth, we show that the contribution from the "part that does query x" can be reduced to M. Lastly, we show that that the contribution from the "part that does not query x" can be reduced to 2^{-n}.

We note that this separation of the operator into two "parts", one that queries on x and one that does not, is an idea that was present in Unruh's proof of the one-way-to-hiding lemma [Unr15].

Proof: Since $|\psi\rangle$ is separable, we may write M as:

$$\begin{aligned} M &= \mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{H'}\mathop{\mathbb{E}}_{k}\mathop{\mathbb{E}}_{\ell}\left\| |x\rangle\langle x|_{B_Q}\,\mathcal{O}^{U_B,H,k}\,|\psi_B\rangle\right\|^2 \cdot \left\| |x\rangle\langle x|_{C_Q}\,\mathcal{O}^{U_C,H',\ell}\,|\psi_C\rangle\right\|^2 \\ &= \underbrace{\left(\mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{k}\left\| |x\rangle\langle x|_{B_Q}\,\mathcal{O}^{U_B,H,k}\,|\psi_B\rangle\right\|^2\right)}_{=M_B} \cdot \underbrace{\left(\mathop{\mathbb{E}}_{H'}\mathop{\mathbb{E}}_{\ell}\left\| |x\rangle\langle x|_{C_Q}\,\mathcal{O}^{U_C,H',\ell}\,|\psi_C\rangle\right\|^2\right)}_{=M_C} \end{aligned} \tag{5.2.4}$$

For the remainder of the proof, we fix $L \in \{B, C\}$ such that

$$M_L = \min\{M_B, M_C\}. \tag{5.2.5}$$

Note that $M_L \leq \sqrt{M_B M_C}$ and so $\sqrt{M_L} \leq \sqrt[4]{M_B M_C} = \sqrt[4]{M}$. It now suffices to show that

$$\omega \leq \frac{1}{2} + (5 + 2q_L)q_L\sqrt{M_L} \tag{5.2.6}$$

which will imply that

$$\omega \leq \frac{1}{2} + (5 + 2q)q\sqrt[4]{M} \tag{5.2.7}$$

since $\sqrt{M_L} \leq \sqrt[4]{M}$ and $q_L \leq q_B + q_C = q$. In particular, we do not need to consider both B and C contributions in ω. We can limit ourselves to the L contribution.

Indeed, once again using the fact that $|\psi\rangle$ is separable, we have that

$$\begin{aligned}\omega &= \mathop{\mathbb{E}}_{H}\left(\left\|\pi_B^{H(x)}\mathcal{O}^{U_B,H,q_B}\left|\psi_B\right\rangle\right\|^2\right)\cdot\left(\left\|\pi_C^{H(x)}\mathcal{O}^{U_C,H,q_C}\left|\psi_C\right\rangle\right\|^2\right)\\ &\leq \mathop{\mathbb{E}}_{H}\left\|\pi_L^{H(x)}\mathcal{O}^{U_L,H,q_L}\left|\psi_L\right\rangle\right\|^2\end{aligned} \tag{5.2.8}$$

This inequality holds since all these norms have an upper bound of 1. It now suffices to show that

$$\mathop{\mathbb{E}}_{H}\left\|\pi_L^{H(x)}\mathcal{O}^{U_L,H,q_L}\left|\psi_L\right\rangle\right\|^2 \leq \frac{1}{2^n} + (5+2q_L)q_L\sqrt{M_L}. \tag{5.2.9}$$

Suppose for a moment that H is fixed and let us examine its corresponding norm in the above bound for ω. In a manner analogue to the technique found in the proof of the one-way-to-hiding lemma from [Unr15], we can isolate "everywhere L queries H on x". We may write our oracle computation as

$$\mathcal{O}^{U_L,H,q_L} = \left(U_L\left(\mathbb{1}_S\otimes O^H\right)\right)^{q_L} = \left(U_L O^H\left(\mathbb{1}-|x\rangle\langle x|_{L_Q}\right) + U_L O^H|x\rangle\langle x|_{L_Q}\right)^{q_L} \tag{5.2.10}$$

where we omit the $\mathbb{1}_S$ for clarity. Applying Proposition 5.1.1 then yields

$$\begin{aligned}\mathcal{O}^{U_L,H,q_L} = &\overbrace{\left(U_L O^H\left(\mathbb{1}-|x\rangle\langle x|_{L_Q}\right)\right)^{q_L}}^{=V_L^H} + \\ &\sum_{k=0}^{q_L-1}\underbrace{\left(U_L O^H\left(\mathbb{1}-|x\rangle\langle x|_{L_Q}\right)\right)^{q_L-k-1}U_L O^H|x\rangle\langle x|_{L_Q}\left(U_L O^H\right)^k}_{=W_L^{H,k}}.\end{aligned} \tag{5.2.11}$$

In particular, one may verify that V_L^H is independent of the value of $H(x)$ in the sense that if $H, H' \in \mathrm{Bool}(\lambda, n)$ are two functions such that $H(s) = H'(s) \iff s \neq x$, then $V_L^H = V_L^{H'}$. This follows from the fact that

$$O^H\left(\mathbb{1}-|x\rangle\langle x|_{L_Q}\right) = O^{H'}\left(\mathbb{1}-|x\rangle\langle x|_{L_Q}\right) \tag{5.2.12}$$

since we project on a subspace where $O^H = O^{H'}$. Indeed, we are removing, with the projector $(\mathbb{1}-|x\rangle\langle x|)$, the only query on which O^H and $O^{H'}$ differ. In an intuitive manner, V_L^H is the part of $\mathcal{O}^{U_L,H,q_L}$ "which does not query H on x" and the sum of

the $W_L^{H,k}$ terms is the part "which at one point queries H on x". Note the presence of the projector $|x\rangle\langle x|_{L_Q}$ in $W_L^{H,k}$.

Then, using Proposition 5.1.4 gives us

$$\left\|\pi_L^{H(x)}\mathcal{O}^{U_L,H,q_L}|\psi_L\rangle\right\|^2 \leq \left\|\pi_L^{H(x)}V_L^H|\psi_L\rangle\right\|^2 + (5+2q_L)\sum_{k=0}^{q_L-1}\left\|\pi_L^{H(x)}W_L^{H,k}|\psi_L\rangle\right\|. \tag{5.2.13}$$

Indeed, note that

$$\left\|\pi_L^{H(x)}\mathcal{O}^{U_L,H,q_L}|\psi_L\rangle\right\| \leq \left\|\pi_L^{H(x)}\right\| \cdot \left\|\mathcal{O}^{U_L,H,q_L}\right\| \cdot \||\psi_L\rangle\| \leq 1 \tag{5.2.14}$$

and that, similarly, for any value of $k \in [q_l - 1]_0$

$$\left\|W_L^{H,k}|\psi\rangle\right\| \leq 1 \tag{5.2.15}$$

since projectors and unitary operators all have operator norms of 1. Thus, the lemma is applicable.

By properties of the operator norm, we can, in a sense, remove projectors and unitary operators from the left hand side of the operator product defining $W_L^{H,k}$ to obtain

$$\left\|\pi_L^{H(x)}W_L^{H,k}|\psi_L\rangle\right\| \leq \left\||x\rangle\langle x|_{L_Q}\left(U_L O^H\right)^k|\psi_L\rangle\right\| = \left\||x\rangle\langle x|_{L_Q}\mathcal{O}^{U_L,H,k}|\psi_L\rangle\right\|. \tag{5.2.16}$$

Thus, combining Equations (5.2.13) and (5.2.16), we have

$$\left\|\pi_L^{H(x)}\mathcal{O}^{U_L,H,q_L}|\psi_L\rangle\right\|^2 \leq \left\|\pi_L^{H(x)}V_L^H|\psi_L\rangle\right\|^2 + (5+2q_L)q_L\mathop{\mathbb{E}}_k\left\||x\rangle\langle x|_{L_Q}\mathcal{O}^{U_L,H,k}|\psi_L\rangle\right\| \tag{5.2.17}$$

where k may take values from $[q_L - 1]_0$.

It then follows that

$$\begin{aligned}
\omega &\leq \mathop{\mathbb{E}}_{H} \left\| \pi_L^{H(x)} V_L^H \left|\psi_L\right\rangle \right\|^2 + (5+2q_L) q_L \mathop{\mathbb{E}}_{H} \mathop{\mathbb{E}}_{k} \left\| \left|x\right\rangle\!\left\langle x\right|_{L_Q} \mathcal{O}^{U_L,H,k} \left|\psi_L\right\rangle \right\| \\
&= \mathop{\mathbb{E}}_{H} \left\| \pi_L^{H(x)} V_L^H \left|\psi_L\right\rangle \right\|^2 + (5+2q_L) q_L \mathop{\mathbb{E}}_{H} \mathop{\mathbb{E}}_{k} \sqrt{\left\| \left|x\right\rangle\!\left\langle x\right|_{L_Q} \mathcal{O}^{U_L,H,k} \left|\psi_L\right\rangle \right\|^2} \\
&\leq \mathop{\mathbb{E}}_{H} \left\| \pi_L^{H(x)} V_L^H \left|\psi_L\right\rangle \right\|^2 + (5+2q_L) q_L \sqrt{\mathop{\mathbb{E}}_{H} \mathop{\mathbb{E}}_{k} \left\| \left|x\right\rangle\!\left\langle x\right|_{L_Q} \mathcal{O}^{U_L,H,k} \left|\psi_L\right\rangle \right\|^2} \\
&= \mathop{\mathbb{E}}_{H} \left\| \pi_L^{H(x)} V_L^H \left|\psi_L\right\rangle \right\|^2 + (5+2q_L) q_L \sqrt{M_L}
\end{aligned} \tag{5.2.18}$$

where the first inequality is given by Equation (5.2.17) and the second is given by Jensen's inequality. It now suffices to show that

$$\mathop{\mathbb{E}}_{H} \left\| \pi_L^{H(x)} V_L^H \left|\psi_L\right\rangle \right\|^2 \leq \frac{1}{2^n}. \tag{5.2.19}$$

For all $H \in \mathrm{Bool}(\lambda, n)$ and $y \in \{0,1\}^n$, define $H_{x,y} \in \mathrm{Bool}(\lambda, n)$ by the following mapping:

$$s \mapsto \begin{cases} H(s) & \text{if } s \neq x \\ y & \text{if } s = x \end{cases} \tag{5.2.20}$$

Then, using Proposition 2.1.11, we have that

$$\mathop{\mathbb{E}}_{H} \left\| \pi_L^{H(x)} V_L^H \left|\psi_L\right\rangle \right\|^2 = \mathop{\mathbb{E}}_{H} \mathop{\mathbb{E}}_{y} \left\| \pi_L^{H_{x,y}(x)} V_L^{H_{x,y}} \left|\psi_L\right\rangle \right\|^2 = \mathop{\mathbb{E}}_{H} \mathop{\mathbb{E}}_{y} \left\| \pi_L^{y} V_L^{H_{x,y}} \left|\psi_L\right\rangle \right\|^2. \tag{5.2.21}$$

It is now sufficient to show that for any value of $H \in \mathrm{Bool}(\lambda, n)$, we have that

$$\alpha = \mathop{\mathbb{E}}_{y} \left\| \pi_L^{y} V_L^{H_{x,y}} \left|\psi_L\right\rangle \right\|^2 \leq \frac{1}{2^n}. \tag{5.2.22}$$

Since each element of $\{\pi_L^y\}_{y \in \{0,1\}^n}$ projects on mutually orthogonal subspaces, we may bring the sum from the expectation inside the norm squared to obtain

$$\alpha = \frac{1}{2^n} \left\| \sum_{y \in \{0,1\}^n} \pi_L^{y} V_L^{H_{x,y}} \left|\psi_L\right\rangle \right\|^2 \tag{5.2.23}$$

and since $V^{H_{x,y}}$ does not depend on y, we can fix a single $y' \in \{0,1\}^n$ to obtain

$$= \frac{1}{2^n} \left\| \left(\sum_{y \in \{0,1\}^n} \pi_L^y \right) V_L^{H_{x,y'}} |\psi_L\rangle \right\|^2 \tag{5.2.24}$$

$$= \frac{1}{2^n} \left\| \mathbb{1} V_L^{H_{x,y'}} |\psi_L\rangle \right\|^2 \tag{5.2.25}$$

$$\leq \frac{1}{2^n} \left(\left\| V_L^{H_{x,y'}} \right\| \cdot \| |\psi_L\rangle \| \right)^2 \tag{5.2.26}$$

finally, by hypothesis, $\| |\psi_L\rangle \| = 1$ and since $V_L^{H_{x,y}}$ is simply the product of unitary operators and projectors, we have $\left\| V_L^{H_{x,y}} \right\| \leq 1$. Thus, we obtain the upper bound of

$$\alpha \leq \frac{1}{2^n} \tag{5.2.27}$$

which completes the proof. ∎

5.2.2 With Entanglement

We may now restate essentially the same lemma as Lemma 5.2.1, but where the state shared by both adversaries may be entangled.

Lemma 5.2.2.
Let $\lambda, n \in \mathbb{N}^+$ and let $x \in \{0,1\}^\lambda$ be a string. For $L \in \{B, C\}$, let

1. *$\mathcal{H}_L = \mathcal{H}_{L_S} \otimes \mathcal{Q}(\lambda)_{L_Q} \otimes \mathcal{Q}(n)_{L_R}$ be a Hilbert space,*
2. *$U_L \in \mathcal{U}(\mathcal{H}_L)$ be a unitary operator on $\mathcal{H}_L$,*
3. *$\{\pi_L^s\}_{s \in \{0,1\}^n}$ be a projective measurement on $\mathcal{H}_L$, and*
4. *$q_L \in \mathbb{N}^+$ be an integer.*

Then, for any pure state $|\psi\rangle \in \mathcal{H}_B \otimes \mathcal{H}_C$, we have that

$$\omega = \mathop{\mathbb{E}}_H \left\| \left(\pi_B^{H(x)} \otimes \pi_C^{H(x)} \right) \left(\mathcal{O}^{U_B, H, q_B} \otimes \mathcal{O}^{U_C, H, q_C} \right) |\psi\rangle \right\|^2 \leq 9 \cdot 2^{-n} + (5 + 2q) q \sqrt{M} \tag{5.2.28}$$

where $q = q_B \cdot q_C$ *and*

$$M = \mathop{\mathbb{E}}_{H} \mathop{\mathbb{E}}_{k} \mathop{\mathbb{E}}_{\ell} \left\| \left(|x\rangle\langle x|_{B_Q} \otimes |x\rangle\langle x|_{C_Q} \right) \left(\mathcal{O}^{U_B,H,k} \otimes \mathcal{O}^{U_C,H,\ell} \right) |\psi\rangle \right\|^2 \tag{5.2.29}$$

with $k \in [q_B - 1]_0$, $\ell \in [q_C - 1]_0$, *and* $H \in \mathrm{Bool}(\lambda, n)$.

We also not the slight differences in the M here as compared with Lemma 5.2.1. First, the same oracle is used by both parties. Second, $q = q_B \cdot q_C$ and not $q_B + q_C$. Neither of these differences will substantially change our upcoming security proofs.

As mentioned, the proof follows the same ideas as the proof of Lemma 5.2.1. The complications that do arise come from the fact that $|\psi\rangle$ is not separable and so we cannot consider only a single adversary.

Thus, instead of decomposing a single oracle computation, we must decompose the $\mathcal{O}_B \otimes \mathcal{O}_C$ operator into a sum of two operators. One of these operators will represent the "part" of $\mathcal{O}_B \otimes \mathcal{O}_C$ where both adversaries query the oracle on x. The other represents the "part" where at least one adversary does not query on x. The rest of the proof follows the same steps, except that we show that that the contribution from the "part" where at least one adversary does not query on x can be reduced to a value of $9 \cdot 2^{-n}$, instead of the better 2^{-n}.

Proof: As outlined, our first task is to isolate the "part" of the oracle computations where both players will have "queried H on x". For both $L \in \{B, C\}$, recall that

$$\begin{aligned} \mathcal{O}^{U_L,H,q_L} &= \left(U_L \left(\mathbb{1}_{L_S} \otimes O^H \right) \right)^{q_L} \\ &= \left(U_L O^H \right)^{q_L} \\ &= \left(U_L O^H \left(\mathbb{1} - |x\rangle\langle x|_{L_Q} \right) + U_L O^H |x\rangle\langle x|_{L_Q} \right)^{q_L} \end{aligned} \tag{5.2.30}$$

where, for simplicity, we omit the $\mathbb{1}_{L_S}$ operator for the remainder of the proof. A bit of algebra formalized in Proposition 5.1.1 allows us to write

$$\begin{aligned} \mathcal{O}^{U_L,H,q_L} = &\overbrace{\left(U_L O^H \left(\mathbb{1} - |x\rangle\langle x|_{L_Q} \right) \right)^{q_L}}^{=V_L^H} + \\ &\sum_{k=0}^{q_L-1} \underbrace{\left(U_L O^H \left(\mathbb{1} - |x\rangle\langle x|_{L_Q} \right) \right)^{q_L-k-1} U_L O^H |x\rangle\langle x|_{L_Q} \left(U_L O^H \right)^k}_{=W_L^{H,k}}. \end{aligned} \tag{5.2.31}$$

For $L \in \{B, C\}$ and as mentioned in the proof of Lemma 5.2.1, V_L^H does not depend on the value of $H(x)$ in the sense that if $H, H' \in \mathrm{Bool}(n, \lambda)$ are any two functions such that $H(s) = H'(s) \iff s \neq x$, then $V_L^H = V_L^{H'}$.

Thus, we have that

$$\mathcal{O}^{U_B,H,q_B} \otimes \mathcal{O}^{U_C,H,q_C} = \left(V_B^H + \sum_{k=0}^{q_B-1} W_B^{H,k}\right) \otimes \left(V_C^H + \sum_{\ell=0}^{q_C-1} W_C^{H,\ell}\right) \tag{5.2.32}$$

and if, for $L \in \{B, C\}$, we define

$$X_L^H = \sum_{k=0}^{q_L-1} W_L^{H,k}. \tag{5.2.33}$$

Then,

$$\mathcal{O}^{U_B,H,q_B} \otimes \mathcal{O}^{U_C,H,q_C} = V_B^H \otimes \mathcal{O}^{U_C,H,q_B} + X_B^H \otimes V_C^H + X_B^H \otimes X_C^H. \tag{5.2.34}$$

We define one last operator, the Z^H operator, by

$$Z^H = \mathcal{O}^{U_B,H,q_B} \otimes \mathcal{O}^{U_C,H,q_C} - X_B^H \otimes X_C^H. \tag{5.2.35}$$

This lets us write

$$\mathcal{O}^{U_B,H,q_B} \otimes \mathcal{O}^{U_C,H,q_C} = Z^H + X_B^H \otimes X_C^H \tag{5.2.36}$$

where, informally, Z^H represents the part of the oracle computations where at least one of these computations will not "query H on x" and $X_B^H \otimes X_C^H$ represents the part of the oracle computations where both will, at one point or another, "query H on x".

Defining $\Pi^s = \pi_B^s \otimes \pi_C^s$ for all $s \in \{0,1\}^n$ and using the above decomposition of the oracle computations yields

$$\begin{aligned} \omega &= \mathop{\mathbb{E}}_H \left\| \Pi^{H(x)} Z^H |\psi\rangle + \Pi^{H(x)} \left(X_B^H \otimes X_C^H\right) |\psi\rangle \right\|^2 \\ &= \mathop{\mathbb{E}}_H \left\| \Pi^{H(x)} Z^H |\psi\rangle + \sum_{k=0}^{q_B-1} \sum_{\ell=0}^{q_C-1} \Pi^{H(x)} \left(W_B^{H,k} \otimes W_C^{H,\ell}\right) |\psi\rangle \right\|^2. \end{aligned} \tag{5.2.37}$$

We now claim that we can apply Proposition 5.1.4. Indeed, note that

$$\left\|\Pi^{H(x)}\left(Z^H + X_B^H \otimes X_C^H\right)|\psi\rangle\right\| \leq \left\|\Pi^{H(x)}\right\| \cdot \left\|Z^H + X_B^H \otimes X_C^H\right\| \cdot \||\psi\rangle\| = 1 \quad (5.2.38)$$

since all three terms have a norm of 1. $\Pi^{H(x)}$ since it is a projector, $Z^H + X_B^H \otimes X_C^H$ since it is a unitary operator, and $|\psi\rangle$ by definition. We also note that, for $L \in \{B, C\}$ and $k \in [q_L]$, we have that

$$\left\|W_L^{H,k}\right\| \leq 1 \quad (5.2.39)$$

since it is a product of projectors and unitary operators. Then, for any $k \in [q_B - 1]_0$ and any $\ell \in [q_C - 1]_0$, we have that

$$\left\|\Pi^{H(x)}\left(W_B^{H,k} \otimes W_C^{H,\ell}\right)|\psi\rangle\right\| \leq \left\|\Pi^{H(x)}\right\| \left(\left\|W_B^{H,k}\right\| \cdot \left\|W_C^{H,\ell}\right\|\right) \||\psi\rangle\| = 1. \quad (5.2.40)$$

The above observations confirm that Proposition 5.1.4 is applicable and yields

$$\begin{aligned}\omega &\leq \mathop{\mathbb{E}}_H \left(\left\|\Pi^{H(x)} Z^H |\psi\rangle\right\|^2 + (5 + 2q_B q_C) \sum_{k=0}^{q_B-1} \sum_{\ell=0}^{q_C-1} \left\|\Pi^{H(x)}\left(W_B^{H,k} \otimes W_C^{H,\ell}\right)|\psi\rangle\right\|\right) \\ &= \mathop{\mathbb{E}}_H \left\|\Pi^{H(x)} Z^H |\psi\rangle\right\|^2 + (5 + 2q_B q_C) q_B q_C \mathop{\mathbb{E}}_H \mathop{\mathbb{E}}_k \mathop{\mathbb{E}}_\ell \left\|\Pi^{H(x)}\left(W_B^{H,k} \otimes W_C^{H,\ell}\right)|\psi\rangle\right\|.\end{aligned} \quad (5.2.41)$$

It now suffices to bound the two norm expectations.

We first show that

$$\mathop{\mathbb{E}}_H \mathop{\mathbb{E}}_k \mathop{\mathbb{E}}_\ell \left\|\Pi^{H(x)}\left(W_B^{H,k} \otimes W_C^{H,\ell}\right)|\psi\rangle\right\| \leq \sqrt{\mathop{\mathbb{E}}_H \mathop{\mathbb{E}}_k \mathop{\mathbb{E}}_\ell \left\|P_x\left(\mathcal{O}^{U_B,H,k} \otimes \mathcal{O}^{U_C,H,\ell}\right)|\psi\rangle\right\|^2} \quad (5.2.42)$$

where $P_x = |x\rangle\langle x|_{B_Q} \otimes |x\rangle\langle x|_{C_Q}$. This is the M contribution.

Recalling the definition of the W operators, we have that

$$\begin{aligned}&W_B^{H,k} \otimes W_C^{H,\ell} = \\ &\left[\left(\left(U_B O^H\left(\mathbb{1} - |x\rangle\langle x|_{B_Q}\right)\right)^{q_B-k-1} U_B O^H\right) \otimes \left(\left(U_C O^H\left(\mathbb{1} - |x\rangle\langle x|_{C_Q}\right)\right)^{q_C-\ell-1} U_C O^H\right)\right] \\ &\cdot \left[\left(|x\rangle\langle x|_{B_Q} \otimes |x\rangle\langle x|_{C_Q}\right)\left(\mathcal{O}^{U_B,H,k} \otimes \mathcal{O}^{U_C,H,\ell}\right)\right].\end{aligned} \quad (5.2.43)$$

Note that the first factor in the above decomposition of $W_B^{H,k} \otimes W_C^{H,\ell}$ has an operator norm less than or equal to 1. It is the tensor of two operators which are simply

products of projectors and unitary operators, all of which have operator norms equal to 1. Since $\Pi^{H(x)}$ also has an operator norm of 1, then

$$\left\|\Pi^{H(x)}\left(W_B^{H,k}\otimes W_C^{H,\ell}\right)|\psi\rangle\right\| \leq \left\|\left(|x\rangle\langle x|_{B_Q}\otimes|x\rangle\langle x|_{C_Q}\right)\left(\mathcal{O}^{U_B,H,k}\otimes\mathcal{O}^{U_C,H,\ell}\right)|\psi\rangle\right\|. \tag{5.2.44}$$

This implies that

$$\begin{aligned}\mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{k}\mathop{\mathbb{E}}_{\ell}\left\|\Pi^{H(x)}\left(W_B^{H,k}\otimes W_C^{H,\ell}\right)|\psi\rangle\right\| &\leq \mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{k}\mathop{\mathbb{E}}_{\ell}\left\|P_x\left(\mathcal{O}^{U_B,H,k}\otimes\mathcal{O}^{U_C,H,\ell}\right)|\psi\rangle\right\| \\ &= \mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{k}\mathop{\mathbb{E}}_{\ell}\sqrt{\left\|P_x\left(\mathcal{O}^{U_B,H,k}\otimes\mathcal{O}^{U_C,H,\ell}\right)|\psi\rangle\right\|^2} \\ &\leq \sqrt{\mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{k}\mathop{\mathbb{E}}_{\ell}\left\|P_x\left(\mathcal{O}^{U_B,H,k}\otimes\mathcal{O}^{U_C,H,\ell}\right)|\psi\rangle\right\|^2}\end{aligned} \tag{5.2.45}$$

where the first inequality holds by Equation (5.2.44) and the second is a result of Jensen's inequality.

To complete the proof, it now suffices to show that

$$\mathop{\mathbb{E}}_{H}\left\|\Pi^{H(x)}Z^H|\psi\rangle\right\|^2 \leq 9\cdot\frac{1}{2^n}. \tag{5.2.46}$$

Using Proposition 2.1.11 and for all $H\in\mathrm{Bool}(\lambda,n)$ and $y\in\{0,1\}^n$ defining the mapping $H_{x,y}\in\mathrm{Bool}(\lambda,n)$ by

$$s\mapsto\begin{cases}H(s) & \text{if } s\neq x\\ y & \text{if } s=x\end{cases} \tag{5.2.47}$$

yields

$$\mathop{\mathbb{E}}_{H}\left\|\Pi^{H(x)}Z^H|\psi\rangle\right\|^2 = \mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{y}\left\|\Pi^{H_{x,y}(x)}Z^{H_{x,y}}|\psi\rangle\right\|^2 = \mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{y}\left\|\Pi^{y}Z^{H_{x,y}}|\psi\rangle\right\|^2. \tag{5.2.48}$$

Since $\{\Pi^y\}_{y\in\{0,1\}^n}$ all project onto mutually orthogonal subspaces, we may write:

$$\mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{y}\left\|\Pi^{y}Z^{H_{x,y}}|\psi\rangle\right\|^2 = \mathop{\mathbb{E}}_{H}\frac{1}{2^n}\left\|\sum_{y}\Pi^{y}Z^{H_{x,y}}|\psi\rangle\right\|^2 \tag{5.2.49}$$

We now claim that for any H, the value of this norm squared is upper bounded by 9.

Recalling the definition of Z^H, we have that

$$\begin{aligned}&\left\|\sum_y \Pi^y Z^{H_{x,y}} |\psi\rangle\right\|^2 \\ &= \left\|\left(\sum_y \Pi^y \left(V_B^{H_{x,y}} \otimes \mathcal{O}^{U_C,H_{x,y},q_C}\right)|\psi\rangle\right) + \left(\sum_y \Pi^y \left(X_B^{H_{x,y}} \otimes V_C^{H_{x,y}}\right)|\psi\rangle\right)\right\|^2.\end{aligned} \tag{5.2.50}$$

Defining α and β as

$$\begin{aligned}\alpha &= \left\|\sum_y \Pi^y \left(V_B^{H_{x,y}} \otimes \mathcal{O}^{U_C,H_{x,y},q_C}\right)|\psi\rangle\right\| \\ \beta &= \left\|\sum_y \Pi^y \left(X_B^{H_{x,y}} \otimes V_C^{H_{x,y}}\right)|\psi\rangle\right\|\end{aligned} \tag{5.2.51}$$

allows us to write

$$\left\|\sum_y \Pi^y Z^{H_{x,y}} |\psi\rangle\right\|^2 \leq \alpha^2 + \beta^2 + 2\alpha\beta = \alpha^2 + \beta^2 + 2\sqrt{\alpha^2\beta^2}. \tag{5.2.52}$$

Thus, it now suffices to bound α^2 and β^2.

We start by bounding α^2. Since $\{\Pi^y\}_{y\in\{0,1\}^n}$ all project on mutually orthogonal subspaces, we may bring the sum out of the norm to obtain

$$\alpha = \sum_y \left\|\left(\pi_B^y \otimes \pi_C^y\right)\left(V_B^H \otimes \mathcal{O}^{U_C,H_{x,y},q_C}\right)|\psi\rangle\right\|^2 \tag{5.2.53}$$

$$= \sum_y \left\|\left(\pi_B^y V_B^H \otimes \pi_C^y \mathcal{O}^{U_C,H_{x,y},q_C}\right)|\psi\rangle\right\|^2. \tag{5.2.54}$$

Since $\left\|\pi_C^y \mathcal{O}^{U_C,H_{x,y},q_C}\right\| \leq 1$, this implies that

$$\alpha \leq \sum_y \left\|\left(\pi_B^y V_B^{H_{x,y}} \otimes \mathbb{1}_C\right)|\psi\rangle\right\|^2 \tag{5.2.55}$$

and bringing the sum back in the norm (since $\{\pi_C^y\}_{y\in\{0,1\}^n}$ all project on orthogonal subspaces) and recalling that $V_B^{H_{x,y}} = V_B^{H_{x,y'}}$ for all $y, y' \in \{0,1\}^n$ yields

$$= \left\| \left(\left(\sum_y \pi_B^y \right) V_B^{H_{x,y'}} \otimes \mathbb{1}_C \right) |\psi\rangle \right\|^2 \tag{5.2.56}$$

$$= \left\| \left(V_B^{H_{x,y'}} \otimes \mathbb{1}_C \right) |\psi\rangle \right\|^2 \tag{5.2.57}$$

for any fixed $y' \in \{0,1\}^n$ and since $\sum_y \pi_C^y = \mathbb{1}$. Lastly, since $\left\| V_B^{H_{x,y'}} \right\| \leq 1$ as it is a product of projectors and unitary operators, we have obtain

$$\leq \||\psi\rangle\|^2 \tag{5.2.58}$$

$$= 1. \tag{5.2.59}$$

Finally, we bound β^2. The step are almost the same as when we bounded α^2, with one key difference. We have $X_B^{H_{x,y}}$ instead of $\mathcal{O}^{U_C,H_{x,y},q_C}$ and it is not clear what is the operator norm of the $X_B^{H_{x,y}}$. However, noting that

$$\left\| X_B^{H_{x,y}} \right\| = \left\| \mathcal{O}^{U_B,H_{x,y},q_B} - V_B^H \right\| \leq \left\| \mathcal{O}^{U_B,H_{x,y},q_B} \right\| + \left\| V_B^H \right\| \leq 2 \tag{5.2.60}$$

is sufficient. Keeping in mind that $\left\| \pi_B^y X_B^{H_{x,y}} \right\|^2 \leq 2^2 = 4$ and closely following the same steps as for α^2, we may write

$$\beta^2 = \left\| \sum_y \left(\pi_B^y \otimes \pi_C^y \right) \left(X_B^{H_{x,y}} \otimes V_C^{H_{x,y}} \right) |\psi\rangle \right\|^2 \tag{5.2.61}$$

$$= \sum_y \left\| \left(\pi_B^y X_B^{H_{x,y}} \otimes \pi_C^y V_C^{H_{x,y}} \right) |\psi\rangle \right\|^2 \tag{5.2.62}$$

$$\leq 4 \sum_y \left\| \left(\mathbb{1}_B \otimes \pi_C^y V_C^{H_{x,y}} \right) |\psi\rangle \right\|^2 \tag{5.2.63}$$

$$= 4 \left\| \left(\mathbb{1}_B \otimes V_C^{H_{x,y'}} \right) |\psi\rangle \right\|^2 \tag{5.2.64}$$

$$\leq 4 \||\psi\rangle\|^2 \tag{5.2.65}$$

$$= 4. \tag{5.2.66}$$

Thus,

$$\begin{aligned}\mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{y}\left\|\Pi^{y}Z^{H_{x,y}}\left|\psi\right\rangle\right\|^{2} &\leq \frac{1}{2^{n}}\mathop{\mathbb{E}}_{H}\left(\alpha^{2}+\beta^{2}+2\sqrt{\alpha^{2}\beta^{2}}\right)\\ &\leq \frac{1}{2^{n}}\mathop{\mathbb{E}}_{H}\left(1+4+2\sqrt{1}\sqrt{4}\right)\\ &= 9\cdot\frac{1}{2^{n}}\end{aligned} \tag{5.2.67}$$

which completes the proof. ∎

5.3 Security Proofs

We are now ready to prove our first security notion. But, we first recall a few facts and notations concerning Scheme 4.4.1.

Let $\mathcal{F}=\{f_\lambda:\{0,1\}^\lambda\times\{0,1\}^\lambda\to\{0,1\}^{\ell(\lambda)}\}_{\lambda\in\mathbb{N}^+}$ be a quantum-secure pseudo-random function which could be used in Scheme 4.4.1.

We briefly recall that, for a fixed λ, the key in Scheme 4.4.1 is given by a string $k\in\{0,1\}^\lambda$ used to identify an element of $\mathcal{F}$ and a string $\theta\in\{0,1\}^\lambda$ which will be used in Wiesner's conjugate coding. To encrypt a message $m\in\{0,1\}^{\ell(\lambda)}$, we sample a random $x\in\{0,1\}^\lambda$ and generate the state $\left|f_\lambda(k,x)\oplus m\right\rangle\!\left\langle f_\lambda(k,x)\oplus m\right|\otimes\left|x^\theta\right\rangle\!\left\langle x^\theta\right|$ where $\left|x^\theta\right\rangle=\bigotimes_{i=1}^{\lambda}H^{\theta_i}\left|x_i\right\rangle$ is the conjugate encoding of x in the basis θ.

When we say that we model $\mathcal{F}$ as a random oracle, we mean that instead of sampling some $k\in\{0,1\}^\lambda$ and giving it to the parties so that they may compute the function $f_\lambda(k,\cdot):\{0,1\}^\lambda\to\{0,1\}^{\ell(\lambda)}$, we instead give them oracle access to a function $H\in\mathrm{Bool}(\lambda,\ell(\lambda))$. Then, instead of taking the expectation over $k\in\{0,1\}^\lambda$, we take the expectation over all possible $H\in\mathrm{Bool}(\lambda,\ell(\lambda))$.

While this greatly simplifies the averaging over all possible functions that could be used in the encryption, the technical tool that we really gain is that we force the adversaries to treat the function as a "black box". In essence, we are assuming that the adversaries may not do anything more clever then simply evaluating the pseudorandom function when they obtain the key.

Theorem 5.3.1.
The QECM protocol described in Scheme 4.4.1 is 9-UNC-secure if pseudorandom functions are modelled as random oracles.

Proof: Let $\mathcal{A}$ be an attack on the QECM scheme $\mathcal{S}$ described in Scheme 4.4.1. Let λ and $n = \ell(n)$ are fixed and that for these values the circuits $\mathtt{B}_\lambda^H$ and $\mathtt{C}_\lambda^H$ may query the oracle implementing the random function $H \in \mathrm{Bool}(\lambda, n)$ at most q_B and q_C times, respectively. We wish to upper bound

$$\omega = \mathop{\mathbb{E}}_{x}\mathop{\mathbb{E}}_{\theta}\mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{m} \mathrm{Tr}\left[\Big(\,|m\rangle\langle m| \otimes |m\rangle\langle m|\,\Big)\Big(B_\theta^H \otimes C_\theta^H\Big) A\Big(\,|H(x)\oplus m\rangle\langle H(x)\oplus m| \otimes \left|x^\theta\right\rangle\left\langle x^\theta\right|\,\Big)\right] \tag{5.3.1}$$

where the expectation over H and θ represents the randomness of the keys and the expectation over x is the randomness of the encryption algorithm. We claim that

$$\omega \leq 9 \cdot \frac{1}{2^n} + \eta_{\mathcal{A}}(\lambda) \tag{5.3.2}$$

for a negligible function $\eta_{\mathcal{A}}$.

The outline of this proof is as follows. Our goal is to use Lemma 5.2.2 and Corollary 3.4.1 to bound this quantity.

First, we manipulate our expression for ω to make Lemma 5.2.2 applicable. To do this, we use a few simple manipulations with respect to the expectations and then purify the CPTP maps B_θ^H and C_θ^H. We will not need to purify the state given to these maps (*i.e.*: the result of the CPTP map A), it is sufficient to see it as an ensemble of pure states. After this purification, we use Lemma 5.2.2 to obtain an expression in terms of the M defined in that lemma. Finally, we use Corollary 3.4.1 to show that the value of this M is a negligible function of λ.

Recall that, for any $n \in \mathbb{N}^+$ and any fixed string y, $s \mapsto s \oplus y$ is a permutation on $\{0,1\}^n$ which is also its own inverse. Thus, we can apply Proposition 2.1.10, with respect to $\mathbb{E}_m$, to write

$$\omega = \mathop{\mathbb{E}}_{x}\mathop{\mathbb{E}}_{\theta}\mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{m} \mathrm{Tr}\left[\Big(\pi_B^{m\oplus H(x)} \otimes \pi_C^{m\oplus H(x)}\Big)\Big(B_\theta^H \otimes C_\theta^H\Big) A\Big(\,|m\rangle\langle m| \otimes \left|x^\theta\right\rangle\left\langle x^\theta\right|\,\Big)\right] \tag{5.3.3}$$

where, for each $L \in \{B, C\}$, $\pi_L^{m\oplus H(x)} = |m \oplus H(x)\rangle\langle m \oplus H(x)|$. Rearranging the expectations and defining $\rho^{m,x,\theta} = A(|m\rangle\langle m| \otimes \left|x^\theta\right\rangle\left\langle x^\theta\right|)$ yields

$$= \mathop{\mathbb{E}}_{m}\mathop{\mathbb{E}}_{x}\mathop{\mathbb{E}}_{\theta}\mathop{\mathbb{E}}_{H} \mathrm{Tr}\left[\Big(\pi_B^{m\oplus H(x)} \otimes \pi_C^{m\oplus H(x)}\Big)\Big(B_\theta^H \otimes C_\theta^H\Big)\rho^{m,x,\theta}\right]. \tag{5.3.4}$$

Inspecting the above trace with the expectation over H and assuming that the values of m, x and θ are fixed, it seems that Lemma 5.2.2 is applicable, if we could

purify our expression. This resembles the manipulation done in the proof of Theorem 4.3.3.

For each $L \in \{B, C\}$ and using Proposition 3.2.3, there exists three Hilbert spaces $\mathcal{H}_{L''}$, $\mathcal{H}_{L'''}$ and $\mathcal{H}_{L_S}$ satisfying

$$\mathcal{H}_L \otimes \mathcal{H}_{L'''} \simeq \mathcal{Q}(n)_{L'} \otimes \mathcal{H}_{L''} \simeq \mathcal{H}_{L_S} \otimes \mathcal{Q}(\lambda)_{L_Q} \otimes \mathcal{Q}(n)_{L_R} \tag{5.3.5}$$

as well as a state $|\text{aux-}L\rangle\langle\text{aux-}L| \in \mathcal{H}_{L'''}$ and unitary operators $U_L^\theta \in \mathcal{U}(\mathcal{H}_L \otimes \mathcal{H}_{L'''})$ such that

$$L_\theta^H(\rho) = (\mathbb{1}_{L'} \otimes \text{Tr}_{L''}) \left(\mathcal{O}^{U_L^\theta, H, q_L} \left(\rho \otimes |\text{aux-}L\rangle\langle\text{aux-}L| \right) \left(\mathcal{O}^{U_L^\theta, H, q_L} \right)^\dagger \right) \tag{5.3.6}$$

for all $\rho \in \mathcal{D}(\mathcal{H}_L)$ and all $\theta \in \{0,1\}^\lambda$. If we define

$$\sigma^{m,x,\theta} = \rho_{BC}^{m,x,\theta} \otimes |\text{aux-}B\rangle\langle\text{aux-}B|_{B'''} \otimes |\text{aux-}C\rangle\langle\text{aux-}C|_{C'''} \tag{5.3.7}$$

and

$$\Pi_{B'C'}^{H(x)} = \pi_{B'}^{m \oplus H(x)} \otimes \pi_{C'}^{m \oplus H(x)} \tag{5.3.8}$$

as well as $\omega^{m,x,\theta}$ as the winning probability of the attack when m, x, and θ are fixed, we have that

$$\begin{aligned}
&\omega^{m,x,\theta} \\
&= \mathop{\mathbb{E}}_H \text{Tr}_{B'C'} \left[\left(\pi_{B'}^{m \oplus H(x)} \otimes \pi_{C'}^{m \oplus H(x)} \right) \left(B_\theta^H \otimes C_\theta^H \right) \rho^{m,x,\theta} \right] \\
&= \mathop{\mathbb{E}}_H \text{Tr}_{B'C'} \left[\Pi_{B'C'}^{H(x)} \left(\mathbb{1}_{B'C'} \otimes \text{Tr}_{B''} \otimes \text{Tr}_{C''} \right) \left(\mathcal{O}^{U_B^\theta, H, q_B} \otimes \mathcal{O}^{U_C^\theta, H, q_C} \right) \sigma^{m,x,\theta} \left(\mathcal{O}^{U_B^\theta, H, q_B} \otimes \mathcal{O}^{U_C^\theta, H, q_C} \right)^\dagger \right] \\
&= \mathop{\mathbb{E}}_H \text{Tr}_{B'B''C'C''} \left[\left(\Pi_{B'C'}^{H(x)} \otimes \mathbb{1}_{B''C''} \right) \left(\mathcal{O}^{U_B^\theta, H, q_B} \otimes \mathcal{O}^{U_C^\theta, H, q_C} \right) \sigma^{m,x,\theta} \left(\mathcal{O}^{U_B^\theta, H, q_B} \otimes \mathcal{O}^{U_C^\theta, H, q_C} \right)^\dagger \right].
\end{aligned} \tag{5.3.9}$$

Finally, instead of purifying $\sigma^{m,x,\theta}$, it will suffice to view it as an ensemble of pure states. In particular, let $I_{m,x,\theta}$ be a finite set such that

$$\sigma^{m,x,\theta} = \sum_{i \in I_{m,x,\theta}} p_i^{m,x,\theta} \left| \psi_i^{m,x,\theta} \right\rangle\!\left\langle \psi_i^{m,x,\theta} \right| \tag{5.3.10}$$

for appropriate values of $p_i^{m,x,\theta}$ and $\left| \psi_i^{m,x,\theta} \right\rangle$.

Using the linearity of the trace and its relation to the norm, weh ave that

$$\omega^{m,x,\theta}$$
$$= \sum_i p_i^{m,x,\theta} \mathop{\mathbb{E}}_H \left\| \left(\left(\pi_{B'}^{m\oplus H(x)} \otimes \mathbb{1}_{B''} \right) \otimes \left(\pi_{C'}^{m\oplus H(x)} \otimes \mathbb{1}_{C''} \right) \right) \left(\mathcal{O}^{U_B^\theta, H, q_B} \otimes \mathcal{O}^{U_C^\theta, H, q_C} \right) \left| \psi_i^{m,x,\theta} \right\rangle \right\|^2 \tag{5.3.11}$$

The above norm is in a form to which we may apply Lemma 5.2.2. Thus,

$$\begin{aligned} \omega^{m,x,\theta} &\leq \sum_i p_i \left(9 \cdot 2^{-n} + (5+2q) q \sqrt{M_i^{m,x,\theta}} \right) \\ &\leq 9 \cdot 2^{-n} + (5+2q) q \sqrt{\sum_{i \in I} p_i^{m,x,\theta} M_i^{m,x,\theta}} \end{aligned} \tag{5.3.12}$$

where we used Jensen's inequality to bring the sum into the square root, $q = q_B \cdot q_C$, and $M_i^{m,x,\theta}$ is as in Lemma 5.2.2, which is to say that

$$M_i^{m,x,\theta} = \mathop{\mathbb{E}}_H \mathop{\mathbb{E}}_k \mathop{\mathbb{E}}_\ell \left\| \left(|x\rangle\langle x|_{B_Q} \otimes |x\rangle\langle x|_{C_Q} \right) \left(\mathcal{O}^{U_B^\theta, H, k} \otimes \mathcal{O}^{U_C^\theta, H, \ell} \right) \left| \psi_i^{m,x,\theta} \right\rangle \right\|^2 \tag{5.3.13}$$

for $k \in [q_B - 1]_0$ and $\ell \in [q_C - 1]_0$. If we define the projectors

$$\begin{aligned} \beta_x^{\theta,H,k} &= \left(\mathcal{O}^{U_B^\theta, H, k} \right)^\dagger \left(\mathbb{1}_{B_S} \otimes |x\rangle\langle x|_{B_Q} \otimes \mathbb{1}_{B_R} \right) \left(\mathcal{O}^{U_B^\theta, H, k} \right) \\ \gamma_x^{\theta,H,\ell} &= \left(\mathcal{O}^{U_C^\theta, H, \ell} \right)^\dagger \left(\mathbb{1}_{C_S} \otimes |x\rangle\langle x|_{C_Q} \otimes \mathbb{1}_{C_R} \right) \left(\mathcal{O}^{U_C^\theta, H, \ell} \right) \end{aligned} \tag{5.3.14}$$

we may write

$$M_i^{m,x,\theta} = \mathop{\mathbb{E}}_H \mathop{\mathbb{E}}_k \mathop{\mathbb{E}}_\ell \operatorname{Tr} \left[\left(\beta_x^{\theta,H,k} \otimes \gamma_x^{\theta,H,k} \right) \left| \psi_i^{m,x,\theta} \right\rangle\!\left\langle \psi_i^{m,x,\theta} \right| \right] \tag{5.3.15}$$

which implies that

$$\sum_i p_i^{m,x,\theta} M_i^{m,x,\theta} = \mathop{\mathbb{E}}_H \mathop{\mathbb{E}}_k \mathop{\mathbb{E}}_\ell \operatorname{Tr} \left[\left(\beta_x^{\theta,H,k} \otimes \gamma_x^{\theta,H,k} \right) \sigma^{m,x,\theta} \right] \tag{5.3.16}$$

by the linearity of the trace.

After all this work, we have that

$$\omega = \mathop{\mathbb{E}}_{m}\mathop{\mathbb{E}}_{x}\mathop{\mathbb{E}}_{\theta}\omega^{m,x,\theta} \leq 9\cdot 2^{-n} + (5+2q)q\mathop{\mathbb{E}}_{m}\mathop{\mathbb{E}}_{x}\mathop{\mathbb{E}}_{\theta}\sqrt{\mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{k}\mathop{\mathbb{E}}_{\ell}\mathrm{Tr}\left[\left(\beta_x^{\theta,H,k}\otimes\gamma_x^{\theta,H,\ell}\right)\sigma^{m,x,\theta}\right]}. \tag{5.3.17}$$

Using Jensen's inequality and changing the order of the expectations yields

$$\omega \leq 9\cdot 2^{-n} + (5+2q)q\sqrt{\mathop{\mathbb{E}}_{m}\mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{k}\mathop{\mathbb{E}}_{\ell}\mathop{\mathbb{E}}_{x}\mathop{\mathbb{E}}_{\theta}\mathrm{Tr}\left[\left(\beta_x^{\theta,H,k}\otimes\gamma_x^{\theta,H,\ell}\right)\sigma^{m,x,\theta}\right]}. \tag{5.3.18}$$

We now claim that, for any fixed values of m, H, k and ℓ, we can use Corollary 3.4.1 to obtain

$$\mathop{\mathbb{E}}_{x}\mathop{\mathbb{E}}_{\theta}\mathrm{Tr}\left[\left(\beta_x^{\theta,H,k}\otimes\gamma_x^{\theta,H,\ell}\right)\sigma^{m,x,\theta}\right] \leq \left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right)^{\lambda}. \tag{5.3.19}$$

Indeed, for any $m\in\{0,1\}^n$, we define the CPTP map

$$\Phi_m : \mathcal{D}(\mathcal{Q}(\lambda)) \to \mathcal{D}\left(\mathcal{H}_B\otimes\mathcal{H}_{B'''}\otimes\mathcal{H}_C\otimes\mathcal{H}_{C'''}\right) \tag{5.3.20}$$

by

$$\rho \mapsto A(|m\rangle\langle m|\otimes\rho)_{BC}\otimes|\text{aux-}B\rangle\langle\text{aux-}B|_{B'''}\otimes|\text{aux-}C\rangle\langle\text{aux-}C|_{C'''} \tag{5.3.21}$$

so that $\sigma^{m,x,\theta} = \Phi_m\left(|x^\theta\rangle\langle x^\theta|\right)$. Note also that $\left\{\beta_x^{\theta,H,k}\right\}_{x\in\{0,1\}^\lambda}$ and $\left\{\gamma_x^{\theta,H,k}\right\}_{x\in\{0,1\}^\lambda}$ are POVMs for any H,θ,k: they are all projectors and one may verify that they sum to the identity operator.

Thus, Corollary 3.4.1 is applicable and we obtain that

$$\omega \leq 9\cdot 2^{-n} + (5+2q)q\sqrt{\mathop{\mathbb{E}}_{m}\mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{k}\mathop{\mathbb{E}}_{\ell}\left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right)^{\lambda}} < 9\cdot 2^{-n} + p\cdot 0.93^{\lambda} \tag{5.3.22}$$

where $p=(5+2q)q$.

Finally, since $\mathtt{B}_\lambda$ and $\mathtt{C}_\lambda$ are both from polynomial-uniform circuit families, the number of queries they may each make to the oracle is bounded by some polynomials. That is to say that $q_B \leq p_B(\lambda)$ and $q_C \leq p_C(\lambda)$. Defining the polynomially bounded function $p(\lambda) = (5+p_B(\lambda)p_C(\lambda))p_B(\lambda)p_C(\lambda)$ then gives:

$$\omega \leq 9\cdot 2^{-n} + p(\lambda)\cdot 0.93^{\lambda} \tag{5.3.23}$$

Noting that $p(\lambda) \cdot 0.93^{\lambda}$ is a negligible function of λ concludes this proof. ∎

This proof can also be applied to demonstrate the following theorem.

Theorem 5.3.2.
The QECM protocol described in Scheme 4.4.1 is UNC-secure if pseudorandom functions are modelled as random oracles and if the adversaries do not share entanglement.

When we say that the adversaries may not share entanglement, we mean that we only consider UNC-attacks $\mathcal{A}$ whose `A` circuits induces a CPTP map A which, for all ρ in the domain of A, satisfies

$$A(\rho) = \sum_{i \in I} p_i \left|\psi_{B,i}\right\rangle\!\left\langle\psi_{B,i}\right| \otimes \left|\psi_{C,i}\right\rangle\!\left\langle\psi_{C,i}\right| \tag{5.3.24}$$

for suitable values of p_i, $|\psi_{B,i}\rangle$, and $|\psi_{C,i}\rangle$. Note that, among other case, this captures any scenario where `A` only gives classical information to `B` and `C`.

The proof of this theorem follows *exactly* the steps of the proof of Theorem 5.3.1 except that our condition on $A(\rho)$ allows us to use the bound given in Lemma 5.2.1 at Equation (5.3.13), which is better than the bound given by Lemma 5.2.2. Specifically, it does not have the factor of 9 with the 2^{-n} term and thus allows us to obtain UNC-security and not 9-UNC-security.

We do not write this proof as it would essentially be a rewrite of the proof of Lemma 5.2.1. However, we do offer a few clarifications on two points.

The state $\sigma^{m,x,\theta}$ is an ensemble of separable states. In Equation (5.3.10), we express

$$\sigma^{m,x,\theta} = A(|m\rangle\!\langle m| \otimes \left|x^{\theta}\right\rangle\!\left\langle x^{\theta}\right|)_{BC} \otimes |\text{aux-}B\rangle\!\langle\text{aux-}B|_{B'''} \otimes |\text{aux-}C\rangle\!\langle\text{aux-}C|_{C'''} \tag{5.3.25}$$

as an ensemble of pure states. It is with respect to those pure states that Lemma 5.2.2 was eventually used. To use the better bound offered by Lemma 5.2.1, we have to ensure that $\sigma^{m,x,\theta}$ can be expressed as an ensemble of separable states.

By our condition on A, we may write:

$$A(|m\rangle\langle m|\otimes|x^\theta\rangle\langle x^\theta|)_{BC}=\sum_{i\in I^{m,x,\theta}}p_i^{m,x,\theta}\left|\phi_i^{m,x,\theta}\right\rangle\left\langle\phi_i^{m,x,\theta}\right|_B\otimes\left|\varphi_i^{m,x,\theta}\right\rangle\left\langle\varphi_i^{m,x,\theta}\right|_C \tag{5.3.26}$$

for appropriate values of $p_i^{m,x,\theta}$, $\left|\phi_i^{m,x,\theta}\right\rangle$, and $\left|\varphi_i^{m,x,\theta}\right\rangle$. Thus, we may write

$$\begin{aligned}\sigma^{m,x,\theta}&=\left(\sum_{i\in I^{m,x,\theta}}p_i^{m,x,\theta}\left|\phi_i^{m,x,\theta}\right\rangle\left\langle\phi_i^{m,x,\theta}\right|_B\otimes\left|\varphi_i^{m,x,\theta}\right\rangle\left\langle\varphi_i^{m,x,\theta}\right|_C\right)\\&\qquad\otimes|\text{aux-}B\rangle\langle\text{aux-}B|_{B'''}\otimes|\text{aux-}C\rangle\langle\text{aux-}C|_{C'''}\\&=\sum_{i\in I^{m,x,\theta}}p_i^{m,x,\theta}\left(\left|\phi_i^{m,x,\theta}\right\rangle_B|\text{aux-}B\rangle_{B'''}\otimes\left|\varphi_i^{m,x,\theta}\right\rangle_C|\text{aux-}C\rangle_{C'''}\right)\\&\qquad\left(\left\langle\phi_i^{m,x,\theta}\right|_B\langle\text{aux-}B|_{B'''}\otimes\left\langle\varphi_i^{m,x,\theta}\right|_C\langle\text{aux-}C|_{C'''}\right)\end{aligned} \tag{5.3.27}$$

which is indeed an ensemble of separable states.

The differences between the M in Lemma 5.2.2 and in Lemma 5.2.1 do not change the proof. As mentioned prior to the proof of Lemma 5.2.1, there are two differences in the quantity M of both lemmas.

In Lemma 5.2.2's M, the value of q, representing the number of queries to the oracle the adversaries make, is given by $q=q_B\cdot q_C$ which is the product of the number of queries each respective adversary makes to the oracle. The key property of q which is used in the proof of Theorem 5.3.1 is that when both q_A and q_B are bounded by a polynomial of λ, then so is q. This facts does not change when q is given by q_A+q_B, as it is in Lemma 5.2.1.

In Lemma 5.2.2's M, the oracle computation of both adversaries has them making queries to the same boolean function. This is not the case in Lemma 5.2.1's M where the adversaries, in general, make queries to different oracles. These oracle computations appear in the definition of the β and γ projectors in Equation (5.3.14). At that point, the only important property of the oracle computation is that they are unitary operators which do not depend on x. Having the same boolean function or not is of no importance.

Finally, we obtain the following corollary.

Corollary 5.3.1.
Let $\mathcal{F}=\{f_\lambda:\{0,1\}^\lambda\times\{0,1\}^\lambda\to\{0,1\}^k\}_{\lambda\in\mathbb{N}^+}$ be a quantum-secure pseudorandom

function whose output size is fixed and does not grow with λ. Then, the k-QECM scheme induced by $\mathcal{F}$ as given in Scheme 4.4.1 is UNC-IND-secure against adversaries who do not share entanglement if pseudorandom functions are modelled by random oracles.

Proof: Apply Theorem 5.3.2 and Theorem 4.2.2. ∎

Chapter 6

Conclusion

We have formally defined two notions of uncloneable encryption (Definitions 4.1.3 and 4.1.4) and have given a simple encryption scheme (Scheme 4.4.1) which satisfies these security notions under suitable conditions (Theorems 5.3.1 and 5.3.2). This gives a partial answer to a question initially asked by Gottesman [Got03]. The "uncloneability" of our ciphertexts can be connected to the upper bound on the winning probability of certain monogamy-of-entanglement games, as studied by Tomamichel, Fehr, Kaniewksi and Wehner [TFKW13]. Our main technical lemmas (Lemmas 5.2.1 and 5.2.2), inspired by Unruh's one-way-to-hiding lemma [Unr15], are key to this connection.

There remains much to be done on the topic of quantum encryptions for classical messages and we conclude by collecting a few open questions and directions for future work.

1. Can our oracle bound be improved? We showed that our new protocol was a 9-UNC-secure uncloneable encryption scheme when pseudorandom functions were replaced by random oracles (Theorem 5.3.1). Is it possible to show that our protocol is simply UNC-secure or UNC-IND-secure under this model? If not, is there an attack that would exhibit a bound for the security of this protocol?

2. Can we omit the requirement that pseudorandom functions be modelled as random oracles? As mentioned in Chapter 5, our security proofs rely heavily on the idea that our adversaries can only interact with the pseudorandom functions in a "black box" manner when they are modelled by random oracles. At first glance,

it does not seem that our proof technique for our demonstrations of Lemmas 5.2.1 and 5.2.2 can be applied without this assumption. Would it possible to state and prove an analogues of Lemmas 5.2.1 and 5.2.2 with pseudorandom functions instead of random oracles?

3. Could Scheme 4.4.1 be made to be error resistant? We did not analyze our protocol to verify if honest parties could still correctly decrypt the message even if a few errors in the quantum state naturally occurred during transmission. In fact, it is very likely that our scheme does not tolerate any errors. Could we add an error correction code and still maintain uncloneability?

4. Are there other meaningful notions of security for uncloneable encryptions? One of our security notions (Definition 4.1.4) is a direct analogue to the existing definition of indistinguishability under a chosen plain text attack for classical private key encryption schemes. However, this is far from the only notion for such classical encryption schemes. Indeed, [KY06] defines 18 different but related definitions of security for classical private-key encryption schemes. Do any of these variations have a meaningful analogue for uncloneable encryption? What about semantic security?

5. What are the connections, if any, between tamper-evident encryption, key recycling schemes and uncloneable encryption? In Section 1.2.2.2, we briefly presented the notion of tamper-evident encryption and key-recycling schemes. These, and uncloneable encryption as we define it, are security notions which are only achievable in the quantum setting. They all seem to rely, in one way or another, on the no-cloning principle. It would be enlightening to understand the relation, if any, between these security notions. Are they incomparable? Equivalent? Or is there a hierarchy among them?

Bibliography

[AB09] S. Arora and B. Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[ABF+16] G. Alagic, A. Broadbent, B. Fefferman, T. Gagliardoni, C. Schaffner, and M. St. Jules. Computational security of quantum encryption. In *Information Theoretic Security: 9th International Conference—ICITS 2016*, pages 47–71, 2016.
DOI: 10.1007/978-3-319-49175-2_3.

[AKN98] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *30th Annual ACM Symposium on Theory of Computing—STOC 1998*, pages 20–30, 1998.
DOI: 10.1145/276698.276708.

[Bar16] E. Barker. Recommendation for key management part 1: General (revision 4). Technical Report SP 800-57, National Institute of Standards and Technology, 2016.
DOI: 10.6028/NIST.SP.800-57pt1r4.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[BBB14] C. H. Bennett, G. Brassard, and S. Breidbart. Quantum cryptography ii: How to re-use a one-time pad safely even if P=NP. *Natural Computing*, 13(4): 453–458, 2014.
DOI: 10.1007/s11047-014-9453-6.

[BBC+01] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48(4): 778–797, 2001.
DOI: 10.1145/502090.502097.

[BDF+11] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In *Advances in Cryptology—ASIACRYPT 2011*, pages 41–69, 2011.
DOI: 10.1007/978-3-642-25385-0_3.

[BS16] A. Broadbent and C. Schaffner. Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography*, 78(1): 351–382, 2016.
DOI: 10.1007/s10623-015-0157-4.

[CKW00] V. Coffman, J. Kundu, and W. K. Wootters. Distributed entanglement. 61(5): 052306, 200.
DOI: 10.1103/PhysRevA.61.052306.

[Die82] D. Dieks. Communication by EPR devices. *Physics Letters A*, 92(6): 271–272, 1982.
DOI: https://doi.org/10.1016/0375-9601(82)90084-6.

[DPS05] I. Damgård, T. B. Pedersen, and L. Salvail. A quantum cipher with near optimal key-recycling. pages 494–510, 2005.
DOI: 10.1007/11535218_30.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review Letters*, 47(10): 777–780, 1935.
DOI: 10.1103/physrev.47.777.

[FS17] S. Fehr and L. Salvail. Quantum authentication and encryption with key recycling. In *Advances in Cryptology—EUROCRYPT 2017*, pages 311–338, 2017.
DOI: 10.1007/978-3-319-56617-7_11.

[GGM84] O. Goldreich, S. Goldwasser, and S. Micali. How to construct random functions. In *25th Annual Symposium on Foundations of Computer*

Science—FOCS 1984, pages 464–479, 1984.
DOI: 10.1109/SFCS.1984.715949.

[Gol04] O. Goldreich. *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge university press, 2004.

[Got03] D. Gottesman. Uncloneable encryption. *Quantum Information & Computation*, 3(6): 581–602, 2003.

[Her82] N. Herbert. FLASH – A superluminal communicator based upon a new kind of quantum measurement. *Foundations of Physics*, 12(12): 1171–1179, 1982.
DOI: 10.1007/BF00729622.

[Jen06] J. L. W. V. Jensen. Sur les fonctions convexes et les inégalités entre les valeurs moyennes. *Acta mathematica*, 30(1): 175–193, 1906.
DOI: 10.1007/BF02418571.

[Ker83] A. Kerckhoffs. *La cryptographie militaire, ou, Des chiffres usités en temps de guerre: avec un nouveau procédé de déchiffrement applicable aux systèmes à double clef*. Librairie Militaire de L. Baudoin, 1883.

[KY06] J. Katz and M. Yung. Characterization of security notions for probabilistic private-key encryption. 19(1): 67–95, 2006.
DOI: 10.1007/s00145-005-0310-8.

[LC99] H.-K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410): 2050–2056, 1999.
DOI: 10.1126/science.283.5410.2050.

[May96] D. Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In *Advances in Cryptology—CRYPTO 1996*, pages 343–357, 1996.
DOI: 10.1007/3-540-68697-5_26.

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

[Ort18] J. Ortigoso. Twelve years before the quantum no-cloning theorem. *American Journal of Physics*, 86(3): 201–205, 2018.
DOI: 10.1119/1.5021356.

[OV06] T. J. Osborne and F. Verstraete. General monogamy inequality for bipartite qubit entanglement. *Physical Review Letters*, 96(22): 220503, 2006.
DOI: 10.1103/PhysRevLett.96.220503.

[Par70] J. L. Park. The concept of transition in quantum mechanics. *Foundations of Physics*, 1(1): 23–33, 1970.
DOI: 10.1007/BF00708652.

[Per03] A. Peres. How the no-cloning theorem got its name. *Fortschritte der Physik: Progress of Physics*, 51(4-5): 458–461, 2003.
DOI: 10.1002/prop.200310062.

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

[SC94] J. J. Sakurai and E. D. Commins. *Modern quantum mechanics*. Adison-wesley Publishing Company, revised edition, 1994.

[SP00] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2): 441–444, 2000.
DOI: 10.1103/physrevlett.85.441.

[TFKW13] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15: 103002, 2013.
DOI: 10.1088/1367-2630/15/10/103002.

[Unr15] D. Unruh. Revocable quantum timed-release encryption. *Journal of the ACM*, 62(6): 49, 2015.
DOI: 10.1145/2817206.

[Wat09] J. Watrous. Quantum computational complexity. In *Encyclopedia of complexity and systems science*, pages 7174–7201. Springer, 2009.
DOI: 10.1007/978-3-642-27737-5_428-3.

[Wat18] J. Watrous. *The Theory of Quantum Information*. Cambridge University Press, 1st edition, 2018. A draft is available at https://cs.uwaterloo.ca/~watrous/TQI/.

[Wie83] S. Wiesner. Conjugate coding. *ACM SIGACT News*, 15(1): 78–88, 1983.
DOI: 10.1145/1008908.1008920.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299: 802–803, 1982.
DOI: 10.1038/299802a0.

[Zha12] M. Zhandry. How to construct quantum random functions. In *53rd Annual Symposium on Foundations of Computer Science—FOCS 2012*, pages 679–687, 2012.
DOI: 10.1109/FOCS.2012.37.