# QUANTUM ENCRYPTION WITH CERTIFIED DELETION

Rabib Islam

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

Department of Mathematics and Statistics
Faculty of Science
University of Ottawa



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

# Abstract

In the context of classical information, every message is composed of 0s and 1s; these messages can generally be copied at will. However, when quantum phenomena are used to model information, this guarantee no longer exists. This difference gives rise to a range of cryptographic possibilities when one considers encoding certain messages as quantum information. In our case, we analyze a potential benefit of encoding part of an encryption scheme's ciphertext as quantum information. We call this type of ciphertext a *quantum ciphertext*.

In particular, quantum ciphertexts are useful when one wants to be able to prove the *deletion* of the plaintext underlying a ciphertext. Since classical ciphertexts can be copied, clearly such feat is impossible using classical information alone. However, we show that quantum encodings allow such *certified deletion*. More precisely, we show that it is possible to encrypt classical data into a quantum ciphertext such that the recipient of the ciphertext can produce a *classical* string which proves to the originator that the recipient has relinquished any chance of recovering the plaintext, should the decryption key be revealed. Our scheme is feasible with current quantum technology: the honest parties only require quantum devices for single-qubit preparation and measurements, and the scheme is robust against noise in these devices. Furthermore, we provide a proof of security which requires only a finite amount of communication, and which therefore avoids the common technique of relying on the analysis of an asymptotic case.

# Acknowledgements

I would like to thank my supervisor, Professor Anne Broadbent. Were it not for her patience, wisdom, and insight, I would not have been able to make it as far as I have.

I would like to thank my colleagues in Ottawa for all of our engaging and fruitful discussions.

I would like to thank the members of my Thesis Advisory Committee, Professors Jason Crann and Hadi Salmasian, for their comments and revisions.

Finally, I would like to thank my parents. They have supported me every step of the way, and I could not have done this, nor could I have accomplished anything else, without them.

# Contents

# Chapter 1

# Introduction

Consider the following scenario: Alice sends a ciphertext to Bob, but in addition, she wants to encode the data in a way such that Bob can prove to her that he *deleted* the information contained in the ciphertext. Such a deletion should prevent Bob from retrieving any information on the encoded plaintext once the decryption key is revealed. We call this *certified deletion*.

Informally, this functionality stipulates that Bob should not be able to do the following two things simultaneously: (1) Convince Alice that he has deleted the ciphertext; and (2) Given the key, recover information about the encrypted message. To better understand this concept, consider an analogy to certified deletion in the physical world: "encryption" would correspond to locking information into a keyed safe, the "ciphertext" comprising of the locked safe. In this case, "deletion" may simply involve returning the safe in its original state. This "deletion" is intrinsically certified since, without the safe (and having never had access to the key and the safe at the same time), Bob is relinquishing the possibility of gaining access to the information (even in the future when the key may be revealed) by returning the safe. However, in the case that encryption is digital, Bob may retain a copy of the ciphertext; there is therefore no meaningful way for him to certify "deletion" of the underlying information, since clearly a copy of the ciphertext is just as good as the original ciphertext when it comes time to use the key to decrypt the data.

While certain cryptographic tasks seem plainly impossible when considering only the use of classical information, they may become achievable when one uses *quantum information* as well. Whereas a classical bit can only exist as either a 0 or a 1, a quantum bit, or *qubit*, can exist in a continuous-valued superposition of 0 and 1. Also, while two classical bits at a physical distance from one another may not be able to affect one another, two quantum systems can be correlated at a distance, which is a phenomenon known as *entanglement*. Moreover, whereas a classical bit can be copied from one register to another, this is not possible for quantum states. This latter restriction is known as the *no-cloning principle* [Die82, Par70, WZ82]. This quantum

feature has been explored in many cryptographic applications, including unforgeable money [Wie83], quantum key distribution (QKD) [BB84], and more (for a survey, see [BS16]).

## 1.1 Summary of Contributions

In this work, we add to the repertoire of functionalities that are classically impossible, but that quantum information allows to achieve with unconditional security. We give the first formal definition of certified deletion encryption (which is a type of scheme) and certified deletion security (which is a security notion). Moreover, we construct an encryption scheme which, as we demonstrate, satisfies these definitions (in addition, our proofs are applicable in the finite-key regime, which unlike many analyses, does not rely on a case with asymptotic communication). Furthermore, our scheme is technologically simple since it can be implemented by honest parties who have access to rudimentary quantum devices (that is, they only need to prepare single-qubit quantum states, and perform single-qubit measurements); we also show that our scheme is robust against noise in these devices. We now elaborate on these contributions.

### Definitions

Our first contribution is in the area of definitions (see Chapter 3). We build on the *quantum encryption of classical messages* (QECM) framework [BL19] in order to explicate our notion of encryption (for simplicity, our work is restricted to the single-use, private-key setting). Here, we specify both a *decryption key* and an *auxiliary key*: The decryption key is used for decrypting a ciphertext, whereas both the decryption and auxiliary keys are used for encryption. To the QECM, we add a *delete* circuit, used by Bob if he wishes to delete his ciphertext and generate a corresponding verification state, and a *verify* circuit, which uses both the auxiliary and decryption keys, and is used by Alice to determine whether Bob really deleted the ciphertext.

Next, we define the notion of certified deletion security for a QECM scheme (See Fig. 1.1 and Definition 3.2.3). The starting point for this definition is the indistinguishability experiment, here played between an adversary $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2)$ and a challenger. After running the Key Generation procedure, the adversary $\mathcal{A}_0$ submits an $n$-bit plaintext $\mathsf{msg}_0$ to the challenger. Based on a random bit $b$, the challenger either encrypts $\mathsf{msg}_0$ or a dummy plaintext $0^n$, and sends the ciphertext to $\mathcal{A}_1$. The adversary $\mathcal{A}_1$ then produces a candidate "deletion certificate", $y$. Next, the decryption key is sent to the adversary $\mathcal{A}_2$, who produces a guess $b' \in \{0,1\}$. A scheme is deemed *secure* if the probability that *both* $y$ is accepted *and* $b = b'$ is negligibly close to $\frac{1}{2}$. We note that certified deletion security does not necessarily

imply indistinguishability, and hence these two properties are defined and proved separately.

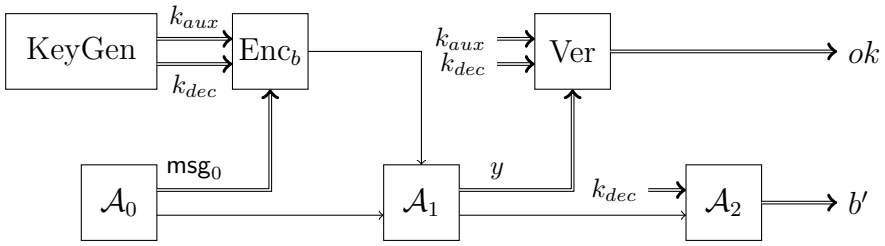


Figure 1.1: Schematic representation of the security notion for certified deletion security. The game is parametrized by $b \in \{0,1\}$ and $\mathrm{Enc}_0$ outputs an encryption of $0^n$ while $\mathrm{Enc}_1$ encrypts its input, $\mathsf{msg}_0$. An adversary $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2)$ *wins* the game if the verification output is *ok and* $b' = b$

## Scheme

In Chapter 4, we present our scheme. Our encoding is based on the well-known Wiesner encoding [Wie83]. Informally, the message is encoded by first generating $m$ random Wiesner states, $|r\rangle^{\theta}$ $(r, \theta \in \{0,1\}^m)$ (for notation, see Section 2.3 and Table 4.1). We let $r|_{\mathcal{I}}$ be the substring of $r$ where qubits are encoded in the computational basis, and we let $r|_{\bar{\mathcal{I}}}$ be the remaining substring of $r$ (where qubits are encoded in the Hadamard basis). Then, in order to create a *proof of deletion*, Bob measures the entire ciphertext in the Hadamard basis. The result is a classical string, and Alice accepts the deletion if all the bits corresponding to positions encoded in the Hadamard basis are correct according to $r|_{\bar{\mathcal{I}}}$. As for the message $\mathsf{msg}$, it is encoded into $x' = \mathsf{msg} \oplus H(r|_{\mathcal{I}}) \oplus u$, where $H$ is a two-universal hash function and $u$ is a fresh, random string. The use of the hash function is required, intuitively, in order to prevent that *partial* information retained by Bob could be useful in distinguishing the plaintext, whereas the random $u$ is used to guarantee security in terms of an encryption scheme. Robustness of the protocol is achieved by using an error correcting code and including an encrypted version of the error syndrome. We note that while our definitions do not require it, our scheme provides a further desirable property, namely that the proof of deletion is a classical string only.

## Proof

In Chapter 5, we present the security analysis of our scheme and give concrete security parameters (Theorem 5.4.2 and its proof). First, the fact that the scheme is an encryption scheme is relatively straightforward; it follows via the uniformity

of the expected ciphertext state to an observer with no key (see Section 5.1). Next, correctness and robustness (Section 5.2) follow from the properties of the encoding and of the error correcting mechanism.

Next, the proof of security for certified deletion has a number of key steps. First, we apply the security notion of certified deletion (Definition 3.2.3) to our concrete scheme (Scheme 4.0.1). This yields a "prepare-and-measure" security game (see Game 5.3.1). However, for the purposes of the analysis, it is convenient to consider instead an entanglement-based game (this is a common proof technique for quantum protocols that include the preparation of random states [LC99, SP00]). In this game (Game 5.3.2), the adversary, Bob, creates an initial entangled state, from which Alice derives (via measurements in a random basis $\theta$ of her choosing) the value of $r \in \{0,1\}^m$. Interestingly, we show that without loss of generality, in this game, Bob can produce the proof of deletion, $y$, *before* he receives any information from Alice (this is due, essentially, to the fact that the ciphertext is uniformly random from Bob's point of view). Averaging over Alice's choice of basis $\theta$, we arrive at a very powerful intuition: in order for Bob's probability of creating an acceptable proof of deletion $y$ (*i.e.*, he produces a string, where the positions corresponding to $\theta = 1$ match with $r|_{\bar{\mathcal{I}}}$) to be high, he must unavoidably have a low probability of correctly guessing $r|_{\mathcal{I}}$. The above phenomenon is embodied in the following *entropic uncertainty relation* for smooth entropies [TR11, TLGR12], where we consider the scenario of Eve preparing a tripartite state $\rho_{ABE}$, with Alice, Bob and Eve receiving the $A$, $B$ and $E$ systems, respectively (here, $A$ and $B$ contain $n$ qubits). Next, Alice either measures all of her qubits in the computational basis to obtain string $X$, or she measures all of her qubits in the Hadamard basis to obtain string $Z$, whereas Bob measures his qubits in the Hadamard basis to obtain $Z'$. We then have the relation:

$$H^{\epsilon}_{\min}(X \mid E) + H^{\epsilon}_{\max}(Z \mid Z') \geq n, \tag{1.1.1}$$

In the above, $\epsilon \leq 0$ is a smoothing parameter which represents a probability of failure, and the smooth min-entropy $H^{\epsilon}_{\min}(X \mid E)$ characterizes the average probability that Eve guesses $X$ correctly, using her optimal strategy, and given her quantum register $E$, while the smooth max-entropy, $H^{\epsilon}_{\max}(Z \mid Z')$ corresponds to the number of bits that are needed in order to reconstruct $Z$ from $Z'$, up to a failure probability $\epsilon$ (for details, see Section 2.5).

Our proof technique thus consists in formally analysing the entanglement-based game and applying the appropriate uncertainty relation in the spirit of the one above.

Finally, we combine the bound on Bob's min-entropy with a universal$_2$ hash function, which, together with the Leftover Hashing Lemma of [Ren05], are used to prove indistinguishability between the cases $b = 0$ and $b = 1$ after Alice has been convinced of deletion.

## 1.2 Related Work

To the best of our knowledge, the first use of a quantum encoding to certify that a ciphertext is completely "returned" was developed by Unruh [Unr14] in the context of *revocable timed-release encryption*.

Fu and Miller [FM18] gave the first evidence that quantum information could be used to prove *deletion* of information, and that this could be verified using classical interaction only: they showed that, via a two-party nonlocality game (involving classical interaction), Alice can become convinced that Bob has *deleted* a single-bit ciphertext (in the sense that the deleted state is unreadable even if Bob were to learn the decryption key). Their results are cast in the device-independent setting (meaning that security holds against arbitrarily malicious quantum devices).

Further related work (that is independent from ours) by Coiteux-Roy and Wolf [CW19] touches on the question of provable deletion using quantum encodings. However, their paper is not concerned with encryption schemes, and therefore does not consider leaking of the key. By contrast, we are explicitly concerned with what it would mean to delete a quantum ciphertext. However, our techniques are closely related to the scheme which they outline.

**Relationship with Quantum Key Distribution.** It can be instructive to compare our results to the ones obtained in the analysis of QKD [TL17]. Firstly, our adversarial model appears different, since in certified deletion, we have one honest party (Alice, the sender) and one cheating party (Bob, the receiver), whereas QKD involves two honest parties (Alice and Bob) and one adversary (Eve). Next, the interaction model is different, since certified deletion is almost non-interactive, whereas QKD involves various rounds of interaction between Alice and Bob. However, the procedures and proof techniques for certified deletion are close to the ones used in QKD: we use similar encodings into Wiesner states, similar privacy amplification and error correction, and the analysis via an entanglement-based game uses similar entropic uncertainty relations, leading to a security parameter that is very similar to the one in [TL17]. While we are not aware of any direct reduction from the security of a QKD scheme to certified deletion, we note that, as part of our proof technique, we manage to essentially map the adversarial model for certified deletion to one similar to the QKD model, since we *split* the behaviour of our adversarial Bob into multiple phases: preparation of the joint state $\rho_{ABE}$, measurement of a register $B$ in a determined basis, and finally bounding the advantage that the adversary has in *simultaneously* making Alice accept the outcome of the measurement performed on $B$, *and* predicting some measurement outcome on register $A$, given quantum side-information $E$. This scenario is similar to QKD, although we note that the measurement bases are not chosen randomly, but are instead consistently in the Hadamard basis (for Bob's measurement), and Eve's challenge is to predict Alice's

measurement in the computational basis only (this situation is reminiscent of the *single-basis parameter estimation* technique [TL17, PLWC16]).

## 1.3 Potential Applications

While the main focus of this work is on the foundations of certified deletion, we can nevertheless envisage potential applications, which we briefly discuss below (we leave the formal analyses for future work).

**Protection against data retention.** In 2016, the European Union adopted a regulation on the processing and free movement of personal data [The16]. Included is a clause on the "right to be forgotten": a person should be able to have their data erased whenever its retention is no longer necessary. Certified deletion encryption might help facilitate this scenario in the following way: if a party were to provide their data to an organization via a certified deletion encryption, the organization would be able to certify deletion of the data using the deletion circuit included in the scheme.

**Encryption with classical revocation.** The concept of *ciphertext revocation* allows a recipient to provably *return* a ciphertext (in the sense that the sender can confirm that the ciphertext is returned, and that the recipient will *not* be able to decrypt, even if the decryption key is leaked in the future); such a functionality is unachievable with classical information alone, but is known to be achievable using quantum ciphertexts [Unr14]. In a sense, our contribution is an extension of revocation, since from the point of view of the recipient, whether quantum information is deleted or returned, the end result is similar: the recipient is unable to decrypt, even given the decryption key. Our scheme, however, has the advantage of using classical information only for the deletion.

As a use case for classical revocation, consider a situation where Bob loans Alice an amount of money. Alice agrees to pay back the full amount in time $T$ plus 15% interest if Bob does not recall the loan within that time. To implement this scheme, Alice uses a certified deletion encryption scheme to send Bob an encrypted cheque, and schedules her computer to send Bob the key at time $T$. If Bob wishes to recall the loan within time $T$, he sends Alice the deletion string. Another possible application is *timed-release encryption* [Unr14], where the decryption key is included in the ciphertext, but encoded in a classical timed-release encryption.

## 1.4 Outline

The remainder of this thesis is structured as follows. Chapter 2 is an introduction to concepts and notation used in the rest of this work. Chapter 3 lays out the novel

security definitions which appear in this thesis. Chapter 4 is an exposition of our main scheme, while Chapter 5 provides a security analysis. Chapter 6 recapitulates the main results and discusses potential future work.

# Chapter 2

# Preliminaries

In this chapter, we introduce certain concepts and notational conventions which are used throughout the thesis.

## 2.1 Strings

Here, we introduce strings (composed of bits) and certain functions related to them.

**Definition 2.1.1** (String)**.** A *string* $x$ of length $n \in \mathbb{N}$ is a tuple $x \in \{0,1\}^n$.

In order to refer to specific bits of a string, we generally assume a string $x$ of length $n$ to be of the form $x = (x_1, x_2, \ldots, x_n)$. Further, denote $[n] = \{1, 2, \ldots, n\}$. Then, for any string $x = (x_1, \ldots, x_n)$ and any subset $\mathcal{I} \subseteq [n]$, we use $x|_{\mathcal{I}}$ to denote the substring of $x$ restricted to the bits indexed by $\mathcal{I}$, where the order of the bits is the same as that of $x$.

**Definition 2.1.2** (Exclusive or)**.** The *exclusive or* is a binary operator

$$\oplus\colon \{0,1\} \times \{0,1\} \to \{0,1\} \tag{2.1.1}$$

defined by $0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1, 1 \oplus 1 = 0$. For $n \in \mathbb{N}$, the exclusive or is a binary operator

$$\oplus\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n \tag{2.1.2}$$

defined by

$$(x_1, \ldots, x_n) \oplus (y_1, \ldots, y_n) = (x_1 \oplus y_1, \ldots, x_n \oplus y_n). \tag{2.1.3}$$

**Definition 2.1.3** (Hamming weight)**.** For any string $x \in \{0,1\}^n$, we define the Hamming weight function $\omega\colon \{0,1\}^n \to \mathbb{N}$ by

$$\omega(x) = \sum_{i=1}^{n} x_i. \tag{2.1.4}$$

## 2.2 Probability and Negligible Functions

In the context of cryptography, when certain information is given to an adversary, it may be the case that it will raise their chance of success in obtaining some information which is meant to be secret. Were this to happen, it would be important that this extra chance of success should not be so great so as to render the cryptographic scheme useless. In order to encapsulate the notion of "small probabilities of success", it is necessary to discuss negligible functions, which are functions that become very small very quickly as their arguments (typically security parameters) grow.

**Definition 2.2.1** (Negligible function)**.** We call a function $\eta\colon \mathbb{N} \to \mathbb{R}_{\geq 0}$ *negligible* if for every polynomial $p$ with $p(x) > 0$ for all $x$, there exists an integer $N$ such that, for all integers $n > N$, it is true that $\eta(n) < \frac{1}{p(n)}$.

At times, we may want to calculate the expected value of a function evaluated on a uniform random variable. However, to avoid the inconvenience of having to always make the random variable explicit, we make use of the following notation: for a function $f\colon \mathcal{X} \to \mathbb{R}$, we denote

$$\mathop{\mathbb{E}}_{x} f(x) = \frac{1}{|\mathcal{X}|} \sum_{x \in \mathcal{X}} f(x). \tag{2.2.1}$$

## 2.3 Quantum Computation and Information

This section is heavily indebted to Watrous's book [Wat18]. What follows is composed in large part of excerpts from the book which are germane to the thesis. Added to this is a certain exposition which draws a bridge from Watrous's formalism to that of the research at hand.

### 2.3.1 Linear Algebra

Certain basics in linear algebra are required to understand discussions surrounding quantum computation and information. Here, we lay out the bare necessities for the rest of this thesis.

An *alphabet* is a non-empty finite set. For any alphabet $\Sigma$, we use $\mathbb{C}^{\Sigma}$ to denote the set of all functions from $\Sigma$ to $\mathbb{C}$; this forms a vector space of dimension $|\Sigma|$ over the complex numbers, with pointwise addition and scalar multiplication. We call this kind of vector space a *complex Euclidean space*. Morever, we define $\mathbb{C}^n := \mathbb{C}^{[n]}$, and we will typically view vectors $v \in \mathbb{C}^n$ as column vectors $v = (\alpha_1, \ldots, \alpha_n)$ for $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. We notice that there is a bijection between $\mathbb{C}^{\Sigma}$ for any alphabet $\Sigma$ and $\mathbb{C}^n$ where $n = |\Sigma|$, and we therefore refer to this equivalence implicitly.

At times, we make reference to the *standard basis* of $\mathbb{C}^\Sigma$, which is given by $\{e_a : a \in \Sigma\}$, where

$$e_a(b) = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{if } a \neq b. \end{cases} \tag{2.3.1}$$

Recall the inner product of two vectors of a complex Euclidean space. For vectors $u, v \in \mathbb{C}^\Sigma$, it is defined as

$$\langle u, v \rangle = \sum_{a \in \Sigma} \overline{u(a)} v(a). \tag{2.3.2}$$

This inner product is conjugate symmetric, linear in the second argument, and positive definite.

Note that we may also use Dirac bra-ket notation. In this notation, $|\psi\rangle \in \mathcal{H}$ (known as a *ket*) represents a column vector, and $\langle\psi| = |\psi\rangle^\dagger$ (known as a *bra*) represents the conjugate transpose. The inner product of vectors $|\psi\rangle$ and $|\phi\rangle$ would be written as $\langle\psi|\phi\rangle$.

For complex Euclidean spaces $\mathcal{H}$ and $\mathcal{H}'$, we use $\mathcal{L}(\mathcal{H}, \mathcal{H}')$ to denote the collection of all linear mappings of the form

$$M : \mathcal{H} \to \mathcal{H}', \tag{2.3.3}$$

which we call *linear operators*. This set has a complex vector space structure. We say $\mathcal{L}(\mathcal{H}) \coloneqq \mathcal{L}(\mathcal{H}, \mathcal{H})$ are the *operators acting on* $\mathcal{H}$.

For complex Euclidean spaces $\mathcal{H} = \mathbb{C}^\Sigma$ and $\mathcal{H}' = \mathbb{C}^{\Sigma'}$, we may make reference to the standard basis of $\mathcal{L}(\mathcal{H}, \mathcal{H}')$, which is given by $\{E_{a,b} \in \mathcal{L}(\mathcal{H}, \mathcal{H}') : a \in \Sigma', b \in \Sigma\}$, where $E_{a,b}$ is defined as

$$E_{a,b} u = u(b) e_a \tag{2.3.4}$$

for every $u \in \mathcal{H}$.

We now list specific classes of operators which will be referred to later in this thesis.

1. An operator $M \in \mathcal{L}(\mathcal{H})$ is *Hermitian* if $M = M^\dagger$. We use $\mathrm{Herm}(\mathcal{H})$ to refer to the set of Hermitian operators on $\mathcal{H}$.

2. An operator $M \in \mathcal{L}(\mathcal{H})$ is *positive semidefinite* if $M = N^\dagger N$ for some operator $N \in \mathcal{L}(\mathcal{H})$. We use $\mathcal{P}(\mathcal{H})$ to refer to the positive semidefinite operators acting on $\mathcal{H}$. Note also that every positive semidefinite operator is Hermitian.

3. A *density operator* is a positive semidefinite operator with trace equal to 1. We typically refer to density operators with lowercase Greek letters like $\rho, \sigma$, and $\xi$. We use $\mathcal{D}(\mathcal{H})$ to refer to the collection of density operators acting on $\mathcal{H}$.

4. An operator $M \in \mathcal{L}(\mathcal{H})$ is *unitary* if $M^\dagger M = MM^\dagger = \mathbb{1}_{\mathcal{H}}$. Unitary operators are also isometries. We use $\mathcal{U}(\mathcal{H})$ to refer to the group of unitary operators acting on $\mathcal{H}$.

5. An operator $M \in \mathcal{L}(\mathcal{H})$ for a complex Euclidean space of the form $\mathcal{H} = \mathbb{C}^\Sigma$ is a *diagonal operator* if $M(a,b) = 0$ for all $a, b \in \Sigma$ such that $a \neq b$. We write $\mathrm{Diag}(u) \in \mathcal{L}(\mathcal{H})$ for a vector $u \in \mathcal{H}$ to denote

$$\mathrm{Diag}(u)(a,b) = \begin{cases} u(a) & \text{if } a = b \\ 0 & \text{if } a \neq b. \end{cases} \tag{2.3.5}$$

For two density operators $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, we use the notation $\rho \leq \sigma$ to say that $\sigma - \rho$ is positive semidefinite.

For an operator $M \in \mathcal{L}(\mathcal{H})$, the *trace* is defined as the sum of its diagonal entries:

$$\mathrm{Tr}[M] = \sum_{a \in \Sigma} M(a,a). \tag{2.3.6}$$

The trace allows us to define an inner product on the space $\mathcal{L}(\mathcal{H}, \mathcal{H}')$ by the following formula:

$$\langle M, N \rangle = \mathrm{Tr}\big[M^\dagger N\big] \tag{2.3.7}$$

for all $M, N \in \mathcal{L}(\mathcal{H}, \mathcal{H}')$.

As an example of a unitary operator, let $\mathsf{H} \in \mathcal{U}(\mathcal{Q})$ denote the Hadamard operator, which is defined by

$$|0\rangle \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |1\rangle \mapsto \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{2.3.8}$$

Now, for complex Euclidean spaces $\mathcal{H}$ and $\mathcal{H}'$, we can discuss linear maps of the form

$$\Phi \colon \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H}'). \tag{2.3.9}$$

The set of such maps is denoted $\mathcal{T}(\mathcal{H}, \mathcal{H}')$ and is a complex vector space.

We now list specific classes of the maps defined above.

1. A map $\Phi \in \mathcal{T}(\mathcal{H}, \mathcal{H}')$ is *Hermiticity-preserving* if, for every $H \in \mathrm{Herm}(\mathcal{H})$, it holds that

$$\Phi(H) \in \mathrm{Herm}(\mathcal{H}'). \tag{2.3.10}$$

2. A map $\Phi \in \mathcal{T}(\mathcal{H}, \mathcal{H}')$ is *positive* if it holds that

$$\Phi(P) \in \mathcal{P}(\mathcal{H}'). \tag{2.3.11}$$

3. A map $\Phi \in \mathcal{T}(\mathcal{H}, \mathcal{H}')$ is *completely positive* if, for every complex Euclidean space $\mathcal{H}''$, it holds that
$$\Phi \otimes \mathbb{1}_{\mathcal{L}(\mathcal{H}'')} \tag{2.3.12}$$
is a positive map.

4. A map $\Phi \in \mathcal{T}(\mathcal{H}, \mathcal{H}')$ is *trace-preserving* if, for all $M \in \mathcal{L}(\mathcal{H})$, it holds that
$$\mathrm{Tr}[\Phi(M)] = \mathrm{Tr}[M]. \tag{2.3.13}$$

Let us now consider some norms on the space of linear operators. For $M \in \mathcal{L}(\mathcal{H}, \mathcal{H}')$ and any real number $p \geq 1$, the *Schatten p-norm* of $M$ is defined as
$$\|M\|_p = \left(\mathrm{Tr}\left[(M^\dagger M)^{p/2}\right]\right)^{1/p}. \tag{2.3.14}$$
The Schatten $\infty$-norm is defined as
$$\|M\|_\infty = \lim_{p\to\infty} \|M\|_p = \max\{\|Mu\| \colon u \in \mathcal{H}, \|u\| \leq 1\}. \tag{2.3.15}$$
Of particular note is the Schatten 1-norm, also known as the *trace norm*. This is equal to
$$\|M\|_1 = \mathrm{Tr}\left[\sqrt{M^\dagger M}\right]. \tag{2.3.16}$$
For two density operators $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, the value $\|\rho - \sigma\|_1$ is often referred to as the *trace distance* between $\rho$ and $\sigma$.

### 2.3.2 Quantum States, Quantum Channels, and Measurements

In this thesis, we will represent strings in the classical regime via the formalism of registers.

**Definition 2.3.1** (Register)**.** A *register* $X$ is either one of the following two objects:

1. An alphabet $\Sigma$.
2. An $n$-tuple $X = (Y_1, \ldots, Y_n)$, where $n \in \mathbb{N}$ and $Y_1, \ldots, Y_n$ are registers.

For the case of a simple register which is equal to its own alphabet, the alphabet represents the classical states which the register may store.

Suppose we were unsure about the actual value of a bit $x$. We would know that $x$ can only take a value of either 0 or 1, but we might only know, for example, that $x$ would take on value 0 with probability $x|^0$ and value 1 with probability $x|^1$. Then we could represent our knowledge of the value of $x$ by a probability vector $v = (x|^0, x|^1)$.

Now, suppose we have a simple register $X$ with alphabet $\Sigma$. Then we represent a probabilistic state of $X$ to be a probability distribution over $\Sigma$. If we are working with reference to an implicit probability distribution, then we will use $X$ to represent a random variable from that distribution, rendering statements like $\Pr[X = x]$ for $x \in \Sigma$ meaningful. Such a distribution can be rendered simply as a probability vector.

However, quantum states are not represented by probability vectors, but by density operators.

**Definition 2.3.2** (Quantum state)**.** A *quantum state* or *quantum system* is a density operator of the form $\rho \in \mathcal{D}(\mathcal{H})$ for some choice of a complex Euclidean space $\mathcal{H}$.

Note that, at times, we make use of *subnormalized* states, which are positive semidefinite operators with trace greater than 0 and less than or equal to 1.

Often, a quantum state $\rho \in \mathcal{D}(\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \cdots \otimes \mathcal{H}_{A_n})$ which is a density operator of a tensor product of complex Euclidean spaces will be written as $\rho_{A_1 A_2 \cdots A_n}$. Taking the partial trace of such a quantum state may eliminate one of the subscripts, such as in the following example:

$$\rho_{A_2 \cdots A_n} = \mathrm{Tr}_{A_1}[\rho_{A_1 A_2 \cdots A_n}]. \tag{2.3.17}$$

Moreover, the individual subscripts $A_1, \ldots, A_n$ may on their own be referred to as "quantum systems" as a matter of convenience.

**Definition 2.3.3** (Qubit)**.** A *qubit* is a quantum state $\rho \in \mathcal{D}(\mathbb{C}^\Sigma)$ for $\Sigma = \{0, 1\}$. We use the notation $\mathcal{Q} \coloneqq \mathbb{C}^\Sigma$ to denote the state space of a single qubit, and we use $\mathcal{Q}(n) \coloneqq \mathcal{Q}^{\otimes n}$ to denote the state space of $n$ qubits.

**Definition 2.3.4** (Pure state)**.** A quantum state $\rho \in \mathcal{D}(\mathcal{H})$ is said to be a *pure state* if there exists a unit vector $|\psi\rangle \in \mathcal{H}$ such that

$$\rho = |\psi\rangle\langle\psi| . \tag{2.3.18}$$

Equivalently, $\rho$ is a pure state if its rank is equal to 1.

It is common practice to refer to a pure state as $|\psi\rangle$ instead of as $|\psi\rangle\langle\psi|$. An example of a pure state which we use is the Einstein-Podolsky-Rosen (EPR) state [EPR35], which is defined as

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle). \tag{2.3.19}$$

**Definition 2.3.5** (Completely mixed state)**.** For a complex Euclidean space $\mathcal{H}$, the *completely mixed state* is

$$\frac{\mathbb{1}_{\mathcal{H}}}{\dim(\mathcal{H})}. \tag{2.3.20}$$

Note that the formalism we have discussed so far is sufficient to represent probabilistic classical states. Suppose we have a register $X$ with classical state set $\Sigma$. Consider the associated complex Euclidean space $\mathcal{H} = \mathbb{C}^{\Sigma}$. Then the classical state for $a \in \Sigma$ can be represented as $E_{a,a} \in \mathcal{D}(\mathcal{H})$. Accordingly, probabilistic states correspond to diagonal density operators; for a given probability vector $\{p(a) \colon a \in \Sigma, \sum_{a\in\Sigma} p(a) = 1\}$, the state is represented as

$$\sum_{a\in\Sigma} p(a) E_{a,a} = \mathrm{Diag}(p). \tag{2.3.21}$$

Moreover, we use $x \xleftarrow{\$} X$ to denote sampling an element $x \in X$ uniformly at random from a set $X$. This uniform randomness is represented in terms of registers in the completely mixed state.

From now on, wherever a register which represents a classical state is denoted by an uppercase letter (e.g. $X$), we will use the script version of that letter to denote its alphabet (which in the current example would be $\mathcal{X}$).

Let us introduce a few more notational conventions that will prove useful later on. Let $|x_i\rangle\langle x_i| \in \mathcal{D}(\mathbb{C}^{\mathcal{X}})$ be classical states for integers $i$ such that $1 \leq i \leq n$. Then we use the notation

$$|x_1, x_2, \ldots, x_n\rangle\langle x_1, x_2, \ldots, x_n| \coloneqq |x_1\rangle\langle x_1| \otimes |x_2\rangle\langle x_2| \otimes \cdots \otimes |x_n\rangle\langle x_n| . \tag{2.3.22}$$

Recall that $\mathsf{H}$ is the Hadamard operator. For any strings $x, \theta \in \{0,1\}^n$, we define

$$\left|x^{\theta}\right\rangle = \mathsf{H}^{\theta} |x\rangle = \mathsf{H}^{\theta_1} |x_1\rangle \otimes \mathsf{H}^{\theta_2} |x_2\rangle \otimes \cdots \otimes \mathsf{H}^{\theta_n} |x_n\rangle . \tag{2.3.23}$$

States of the form $\left|x^{\theta}\right\rangle$ are here called *Wiesner states* in recognition of their first use in [Wie83].

The representation of classical states in the quantum formalism allows us to address the matter of correlation between quantum and classical states using *classical-quantum states* (cq-states). For a classical register $X$ and a quantum system $A$, one may write the cq-state

$$\rho_{XA} = \sum_{x\in\mathcal{X}} \Pr_X(x) \, |x\rangle\langle x|_X \otimes \rho_{A|X=x}, \tag{2.3.24}$$

where $\rho_{A|X=x}$ is the state of $A$ conditioned on the event that $X = x$.

Quantum channels are linear maps which are used to represent changes to quantum systems, whether these changes are related to computation, noise, or otherwise.

**Definition 2.3.6** (Quantum channel)**.** A *quantum channel* is a linear map

$$\Phi \colon \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H}') \tag{2.3.25}$$

for some choice of complex Euclidean spaces $\mathcal{H}$ and $\mathcal{H}'$, satisfying two properties:

1. $\Phi$ is completely positive; and

2. $\Phi$ is trace-preserving.

For classical registers $X$ and $Y$ and a function $f\colon \mathcal{X} \to \mathcal{Y}$, we denote by $\mathcal{E}_f\colon \mathcal{D}(\mathbb{C}^{\mathcal{X}}) \to \mathcal{D}(\mathbb{C}^{\mathcal{X}} \otimes \mathbb{C}^{\mathcal{Y}})$ the channel

$$\mathcal{E}_f[\cdot] \coloneqq \sum_{x\in\mathcal{X}} |f(x)\rangle_Y |x\rangle\langle x|_X \cdot |x\rangle\langle x|_X \langle f(x)|_Y . \tag{2.3.26}$$

Measurements are functions which enable the extraction of classical information from quantum states.

**Definition 2.3.7** (Measurement)**.** A *measurement* is a function of the form

$$\mu\colon \Sigma \to \mathcal{P}(\mathcal{H}) \tag{2.3.27}$$

for some choice of an alphabet $\Sigma$ and a complex Euclidean space $\mathcal{H}$, satisfying

$$\sum_{x\in\Sigma} \mu(x) = \mathbb{1}_{\mathcal{H}}. \tag{2.3.28}$$

The alphabet $\Sigma$ is the set of *measurement outcomes* of the measurement and each operator $\mu(a)$ is the *measurement operator* associated with the outcome $a \in \Sigma$.

The term *positive-operator valued measure* (POVM) may also be used to refer to a measurement. This may be used to distinguish it from a generalized measurement, which is a type of function which we do not discuss.

If one wants to measure a state $\rho_A \in \mathcal{D}(\mathcal{H}_A)$, then the measurement $\mu$ must map to $\mathcal{P}(\mathcal{H}_A)$. In performing the measurement, two things happen:

1. An element of $a \in \Sigma$ is selected as the outcome of the measurement according to the probability distribution given by $p(a) = \langle \mu(a), \rho\rangle$; and

2. The system $A$ ceases to exist; the measurement outcome may now reside in a register stated explicitly or left implicit.

In this thesis, we often specify measurements not as functions as above, but as a collection of measurement operators indexed by a set of measurement outcomes, such as the following:

$$\{P_a\colon a \in \Sigma\} \subset \mathcal{P}(\mathcal{H}); \tag{2.3.29}$$

This can be easily rewritten as a measurement $\mu\colon \Sigma \to \mathcal{P}(\mathcal{H})$ with $\mu(a) = P_a$ for each $a \in \Sigma$.

We can also describe measurements as quantum-to-classical channels.

**Definition 2.3.8** (Quantum-to-classical channel)**.** Let $\Phi \in \mathcal{T}(\mathcal{H}, \mathcal{H}')$ be a channel. It is said that $\Phi$ is a *quantum-to-classical channel* if, for every $\rho \in \mathcal{D}(\mathcal{H})$, $\Phi(\rho)$ is a diagonal density operator.

Such a description for measurements can be useful when we want to make obvious the systems involved in a measurement. For instance, the notation $\mathcal{M}_A \to X$ would indicate a channel mapping quantum states in $\mathcal{D}(\mathcal{H}_A)$ to classical states in classical register $X$.

Given what we have discussed so far, we can now examine the problem of state discrimination. Let $\mathcal{H}$ be a complex Euclidean space, and suppose $\rho_0, \rho_1 \in \mathcal{D}(\mathcal{H})$ are both quantum states from the same state space. Consider two parties Alice and Bob who both know what the states $\rho_0$ and $\rho_1$ are. With probability $\lambda$, Alice sends $\rho_0$ to Bob, and with probability $1-\lambda$, Alice sends $\rho_1$ to Bob. Now, Bob's task is to determine whether he received $\rho_0$ or $\rho_1$ via measurement. The Holevo-Helstrom theorem relates this problem to the trace distance.

**Theorem 2.3.9** (Holevo-Helstrom theorem)**.** *Let $\mathcal{H}$ be a complex Euclidean space, let $\rho_0, \rho_1 \in \mathcal{D}(\mathcal{H})$ be density operators, and let $\lambda \in [0,1]$. For every choice of a measurement $\mu\colon \{0,1\} \to \mathcal{P}(\mathcal{H})$, it holds that*

$$\lambda\langle \mu(0), \rho_0\rangle + (1-\lambda)\langle \mu(1), \rho_1\rangle \leq \frac{1}{2} + \frac{1}{2}\|\lambda\rho_0 - (1-\lambda)\rho_1\|_1. \tag{2.3.30}$$

It follows by Theorem 2.3.9 that the best possible choice of measurement for Bob will result in the correct guess with probability

$$\frac{1}{2} + \frac{1}{2}\|\lambda\rho_0 - (1-\lambda)\rho_1\|_1. \tag{2.3.31}$$

In this work, measurement of a qubit in our scheme will always occur in one of two bases: the computational basis ($\{|0\rangle, |1\rangle\}$) or the Hadamard basis ($\{|+\rangle, |-\rangle\}$). Thus, for a quantum system $A$, we notate these measurements as $\{M_A^{\theta,x}\}_{x\in\{0,1\}}$, where $x \in \{0,1\}$ ranges over the possible outcomes, and where $\theta \in \{0,1\}$ determines the basis of measurement ($\theta = 0$ indicates computational basis and $\theta = 1$ indicates Hadamard basis).

Let $\{M_A^x\}_x$ and $\{N_A^y\}_y$ be two POVMs acting on a quantum system $A$. We define the overlap

$$c(\{M_A^x\}_x, \{N_A^y\}_y) \coloneqq \max_{x,y} \|\sqrt{M_A^x}\sqrt{N_A^y}\|_\infty^2. \tag{2.3.32}$$

Wherever dealing with an $m$-qubit quantum system $A$, we define, for all $i = 1, \ldots, m$,

$$c_i \coloneqq c\left(\{M_{A_i}^{0,x}\}_x, \{M_{A_i}^{1,y}\}_y\right). \tag{2.3.33}$$

We assume our measurements are ideal. Therefore, the overlap between measurements in the rectilinear and diagonal bases would be

$$c_i = \left\| \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} \right\|_\infty^2 = \left\| \begin{pmatrix} 1/2 & 1/2 \\ 0 & 0 \end{pmatrix} \right\|_\infty^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}. \tag{2.3.34}$$

## 2.4 Hash Functions and Error Correction

We make use of universal$_2$ hash functions, first introduced by Carter and Wegman [CW79]. This class of hash function families is made to ensure a low number of collisions when sampling from a family of hash functions at random.

**Definition 2.4.1** (Universal$_2$ Hashing)**.** Let $\mathfrak{H} = \{H\colon \mathcal{X} \to \mathcal{Z}\}$ be a family of functions. We say that $\mathfrak{H}$ is *universal*$_2$ if $\Pr[H(x) = H(x')] \leq \frac{1}{|\mathcal{Z}|}$ for any two distinct elements $x, x' \in \mathcal{X}$, when $H$ is chosen uniformly at random from $\mathfrak{H}$.

Such families exist if $|\mathcal{Z}|$ is a power of two (see [CW79]). Moreover, there exist universal$_2$ families of hash functions which take strings of length $n$ as input and which contain $2^{O(n)}$ hash functions; therefore it takes $O(n)$ bits to specify a hash function from such a family [WC81]. Thus, when we discuss communication of hash functions, we assume that both the sender and the recipient are aware of the family from which a hash function has been chosen, and that the transmitted data consists of $O(n)$ bits used to specify the hash function from the known family.

In the context of error correction, we note that linear error correcting codes can generate syndromes, and that corrections to a message can be made when given the syndrome of the correct message. This is called syndrome decoding, and it is an efficient means of decoding linear codes.

Suppose we have a linear code with parity check matrix $M$. Let $x$ be a trasmitted codeword, and let $y$ be the associated error vector. Then $z = x \oplus y$ is received. Now, we know that for all codewords $x$, $Mx = 0$. Therefore, due to the error, a syndrome is generated:

$$Mz = M(x \oplus e) = Mx \oplus Me = 0 + Me = Me. \tag{2.4.1}$$

The recipient can, assuming a bound on the number of errors, look up the value of $e$. Then,

$$x = z \oplus e. \tag{2.4.2}$$

We implicitly refer to syndrome decoding of an $[n, n-s]$-linear code which handles codewords of length $n$ and generates syndromes of length $s < n$ when we use functions synd$\colon \{0,1\}^n \to \{0,1\}^s$ and corr$\colon \{0,1\}^n \times \{0,1\}^s \to \{0,1\}^n$, where synd is a syndrome-generating function and corr is a string-correcting function. We also make reference to the distance of an error correcting code, which is the minimum distance between distinct codewords.

## 2.5 Smooth Entropies and Uncertainty Relations

The purpose of entropy is to quantify the amount of uncertainty an observer has concerning the outcome of a random variable. Since the uncertainty of random variables can be understood in different ways, there exist different kinds of entropy. Key to our

work are min- and max-entropy, first introduced by Renner and König [Ren05, KRS09], as an application of Rényi entropies [Rén61] to the quantum setting. Foundational to these, however, were the Boltzmann-Gibbs-Shannon entropy (hereafter known as the Shannon entropy) and the quantum generalization thereof, the von Neumann entropy.

Note that all the entropies that are discussed will be written as "conditional". The corresponding unconditional entropies are a special case where the side information is not correlated to the system of interest.

We begin, therefore, with Shannon entropy. Let $X$ be a random variable with a probability mass function $p(x)$. Then

$$H(X) = \sum_x p(x) \log \frac{1}{p(x)}. \tag{2.5.1}$$

The higher this value is, the higher the uncertainty concerning the outcome of the random variable $X$.

Let us now look to the conditional case. Let $X$ and $Y$ be random variables, and let $p(x, y)$ be a joint probability mass function with marginals $p(x)$ and $p(y)$. Then the conditional Shannon entropy is

$$H(X \mid Y) = \sum_{x,y} p(x, y) \log \frac{p(y)}{p(x, y)} \tag{2.5.2}$$

$$= H(XY) - H(Y). \tag{2.5.3}$$

From here, we can make the move to the conditional von Neumann entropy, or the quantum conditional entropy.

**Definition 2.5.1** (Conditional von Neumann Entropy)**.** For any bipartite state $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, we define the *conditional von Neumann entropy* of $A$ given $B$ for the state $\rho_{AB}$ as

$$H(A \mid B)_\rho \coloneqq H(AB)_\rho - H(B)_\rho, \tag{2.5.4}$$

where

$$H(A)_\rho \coloneqq -\operatorname{Tr}[\rho_A \log \rho_A]. \tag{2.5.5}$$

Note that the von Neumann entropy corresponds to the Shannon entropy of a state's eigenvalues.

Let us now consider min- and max-entropy.

**Definition 2.5.2** (Min- and max-entropy)**.** Let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\sigma_B \in \mathcal{D}(\mathcal{H}_B)$. The *min-entropy* of $\rho_{AB}$ relative to $\sigma_B$ is

$$H_{\min}(\rho_{AB} \mid \sigma_B) \coloneqq -\log \lambda \tag{2.5.6}$$

where $\lambda$ is the minimum real number such that $\lambda \cdot \mathbb{1}_{\mathcal{H}_A} \otimes \sigma_B - \rho_{AB}$ is non-negative. The *max-entropy* of $\rho_{AB}$ relative to $\sigma_B$ is

$$H_{\max}(\rho_{AB} \mid \sigma_B) \coloneqq \log \operatorname{Tr}\left[(\mathbb{1}_{\mathcal{H}_A} \otimes \sigma_B)\rho_{AB}^0\right], \tag{2.5.7}$$

where $\rho_{AB}^0$ is the projector onto the support of $\rho_{AB}$. The *min-entropy* and the *max-entropy of $\rho_{AB}$ given $\mathcal{H}_B$* are

$$H_{\min}(A \mid B)_\rho \coloneqq \sup_{\sigma_B \in \mathcal{D}(\mathcal{H}_B)} H_{\min}(\rho_{AB} \mid \sigma_B), \tag{2.5.8}$$

and

$$H_{\max}(A \mid B)_\rho \coloneqq \sup_{\sigma_B \in \mathcal{D}(\mathcal{H}_B)} H_{\max}(\rho_{AB} \mid \sigma_B). \tag{2.5.9}$$

In short, the min-entropy of a random variable measures the degree to which its distribution is uniform, and the max-entropy of a random variable measures the size of its support. It follows that min-entropy is never larger than max-entropy. One may find an elaboration on the operational meanings of these quantities in [KRS09].

The current definitions of min- and max-entropy entail that, were the state in question to change a little bit, the entropy might change drastically. Smooth entropies give the state in question some room to move about, so to speak. In the classical case, for instance, it allows one to study the distributions close to a given distribution.

**Definition 2.5.3** (Smooth min- and max-entropy)**.** Let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B), \sigma_B \in \mathcal{D}(\mathcal{H}_B)$, and $\epsilon \geq 0$. The *$\epsilon$-smooth min-entropy* and the *$\epsilon$-smooth max-entropy of $\rho_{AB}$ relative to $\sigma_B$* are

$$H_{\min}^\epsilon(\rho_{AB} \mid \sigma_B) \coloneqq \sup_{\overline{\rho}_{AB}} H_{\min}(\overline{\rho}_{AB} \mid \sigma_B), \tag{2.5.10}$$

and

$$H_{\max}^\epsilon(\rho_{AB} \mid \sigma_B) \coloneqq \inf_{\overline{\rho}_{AB}} H_{\max}(\overline{\rho}_{AB} \mid \sigma_B), \tag{2.5.11}$$

where the supremum and infimum range over the set of all operators $\overline{\rho}_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ such that $\|\overline{\rho}_{AB} - \rho_{AB}\|_1 \leq \operatorname{Tr}[\rho_{AB}] \cdot \epsilon$. The *$\epsilon$-smooth min-entropy* and the *$\epsilon$-smooth max-entropy of $\rho_{AB}$ given $\mathcal{H}_B$* are

$$H_{\min}^\epsilon(\rho_{AB} \mid B) \coloneqq \sup_{\sigma_B \in \mathcal{D}(\mathcal{H}_B)} H_{\min}^\epsilon(\rho_{AB} \mid \sigma_B), \tag{2.5.12}$$

and

$$H_{\max}^\epsilon(\rho_{AB} \mid B) \coloneqq \sup_{\sigma_B \in \mathcal{D}(\mathcal{H}_B)} H_{\max}^\epsilon(\rho_{AB} \mid \sigma_B). \tag{2.5.13}$$

It is of note that smooth entropies satisfy the following inequality, commonly referred to as the data-processing inequality [TCR10]. This states that the uncertainty of a system never decreases due to any sort of processing done to the side information.

**Proposition 2.5.4.** *Let $\epsilon \geq 0$, $\rho_{AB}$ be a quantum state, and $\mathcal{E}\colon \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_C)$ be a channel. Define $\sigma_{AC} \coloneqq (1_{\mathcal{D}(\mathcal{H}_A)} \otimes \mathcal{E})(\rho_{AB})$. Then,*

$$H_{\min}^{\epsilon}(A \mid B)_{\rho} \leq H_{\min}^{\epsilon}(A \mid C)_{\sigma} \quad \text{and} \quad H_{\max}^{\epsilon}(A \mid B)_{\rho} \leq H_{\max}^{\epsilon}(A \mid C)_{\sigma}. \tag{2.5.14}$$

We use the following uncertainty relation, introduced by Tomamichel and Renner [TR11], and expanded upon in [Tom12]. It was originally understood in terms of its application to QKD, and was used to prove the secrecy of the key in a finite-key analysis of QKD [TLGR12]. One can explain this in an intuitive sense: suppose the parts of a tripartite state are distributed among three parties: Alice, Bob, and Charlie. Suppose also that Alice has the choice of measuring in one of two bases. Then, depending on how distinct these bases are, there is a limit to how much certainty Bob can have about Alice's measurement outcome in one of the bases if Charlie is certain about Alice's measurement outcome in the other basis.

**Proposition 2.5.5.** *Let $\epsilon \geq 0$, let $\rho_{ACE} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_C \otimes \mathcal{H}_E)$ be a tripartite quantum state and let $\{M_A^x\}_{x\in\mathcal{X}}$ and $\{N_A^z\}_{z\in\mathcal{Z}}$ be two POVMs acting on $A$. Then*

$$H_{\min}^{\epsilon}(X \mid C)_{\sigma} + H_{\max}^{\epsilon}(Z \mid E)_{\hat{\sigma}} \geq q, \tag{2.5.15}$$

*where $q = \log \frac{1}{c}$ and $c = \max_{x,z} \| \sqrt{M_A^x}\sqrt{N_A^z} \|_{\infty}^2$. Moreover, $\sigma_{XCE} = \mathcal{M}_{A\to X}(\rho_{ACE})$ and $\hat{\sigma}_{ZCE} = \mathcal{M}_{A\to Z}(\rho_{ACE})$ with maps*

$$\mathcal{M}_{A\to X}(\cdot) = \mathrm{Tr}_A \left( \sum_{x\in\mathcal{X}} \langle x|_X \left(M_A^x\right) \cdot \left(M_A^x\right)^{\dagger} |x\rangle_X \right) \tag{2.5.16}$$

*and*

$$\mathcal{M}_{A\to Z}(\cdot) = \mathrm{Tr}_A \left( \sum_{z\in\mathcal{Z}} \langle z|_Z \left(N_A^z\right) \cdot \left(N_A^z\right)^{\dagger} |z\rangle_Z \right). \tag{2.5.17}$$

We also use the Leftover Hashing Lemma, introduced by Renner [Ren05]. It is typically understood in relation to the privacy amplification step of QKD. We state it in the form given in [TL17]. This result relates the min-entropy of a quantum state to the trace distance between a post-hashing state and a uniformly random state.

**Proposition 2.5.6.** *Let $\epsilon \geq 0$ and $\sigma_{AX}$ be a classical-quantum state, with $X$ a classical register which takes values on $\mathcal{X} = \{0,1\}^s$. Let $\mathfrak{H}$ be a universal$_2$ family of hash functions from $\mathcal{X}$ to $\mathcal{Y} = \{0,1\}^n$. Let $\chi_Y = \frac{1}{2^n} 1_{\mathcal{D}(\mathcal{Y})}$ be the fully mixed state, $\rho_{S^H} = \frac{1}{|\mathfrak{H}|} \sum_{H\in\mathfrak{H}} |H\rangle\langle H|_{S^H}$ and $\zeta_{AYS^H} = \mathrm{Tr}_X[\mathcal{E}_f(\sigma_{AX} \otimes \rho_{S^H})]$ for the function $f\colon (x,H) \mapsto H(x)$ be the post-hashing state. Then,*

$$\| \zeta_{AYS^H} - \chi_Y \otimes \zeta_{AS^H} \|_{\mathrm{Tr}} \leq \frac{1}{2} 2^{-\frac{1}{2}(H_{\min}^{\epsilon}(X|A)_{\sigma} - n)} + 2\epsilon. \tag{2.5.18}$$

## 2.6 Statistical Lemmas

The following lemmas are required to bound a specific max-entropy quantity. They are both proven in [TL17] as part of a security proof of finite-key QKD, and this line of thinking originated in [TLGR12].

The following lemma is a consequence of Serfling's bound [Ser74].

**Lemma 2.6.1.** *Let $Z_1, \dots Z_m$ be random variables taking values in $\{0,1\}$. Let $m = s + k$. Let $\mathcal{I}$ be an independent and uniformly chosen subset of $[m]$ with $s$ elements. Then, for $\nu \in [0,1]$ and $\delta \in (0,1)$,*

$$\Pr\left[\sum_{i\in\mathcal{I}} Z_i \leq k\delta \wedge \sum_{i\in\bar{\mathcal{I}}} Z_i \geq s(\delta+\nu)\right] \leq \exp\left(\frac{-2\nu^2 sk^2}{m(k+1)}\right). \tag{2.6.1}$$

It will also be useful to condition a quantum state on future events. This is called "smoothing". In order to proceed, we define purified distance, which is a metric on quantum states, and which is related to the minimal trace distance of purifications.

**Definition 2.6.2** (Purified Distance)**.** Let $A$ be a quantum system. For two (subnormalized) states $\rho_A, \sigma_A$, we define the *generalized fidelity*,

$$F(\rho_A,\sigma_A) \coloneqq \left(\mathrm{Tr}\left[\sqrt{\sqrt{\rho_A}\sigma_A\sqrt{\rho_A}}\right] + \sqrt{1-\mathrm{Tr}[\rho_A]}\sqrt{1-\mathrm{Tr}[\sigma_A]}\right)^2, \tag{2.6.2}$$

and the *purified distance*,

$$P(\rho_A,\sigma_A) \coloneqq \sqrt{1-F(\rho_A,\sigma_A)}. \tag{2.6.3}$$

The following lemma from [TL17] states that, given a classical-quantum state, there may exist a nearby state on which a certain event does not occur.

**Lemma 2.6.3.** *Let $\rho_{AX}$ be a classical-quantum state with $X$ a classical register, and $\Omega\colon \mathcal{X} \to \{0,1\}$ be an event with $\Pr[\Omega]_\rho = \epsilon < \mathrm{Tr}[\rho_{AX}]$. Then there exists a classical-quantum state $\tilde{\rho}_{AX}$ with $\Pr[\Omega]_{\tilde{\rho}} = 0$ and $P(\rho_{AX},\tilde{\rho}_{AX}) \leq \sqrt{\epsilon}$.*

## 2.7 Quantum Encryption and Security

Whenever an adversary $\mathcal{A}$ is mentioned, it is assumed to be quantum and to have unbounded computational power.

Considering that the scheme introduced in this thesis is an encryption scheme with a quantum ciphertext, we rely on the "quantum encryption of classical messages" framework from prior work [BL19]. This framework describes an encryption scheme as a set of parameterized channels which satisfy certain conditions.

**Definition 2.7.1** (Quantum Encryption of Classical Messages)**.** Let $n$ be an integer. An *$n$-quantum encryption of classical messages* ($n$-QECM) is a tuple of polynomial-time quantum circuits $\mathcal{S} = (\mathsf{key}, \mathsf{enc}, \mathsf{dec})$ implementing channels of the form

- $\Phi_\lambda^{\mathsf{key}} \colon \mathcal{D}(\mathbb{C}) \to \mathcal{D}(\mathcal{H}_{K,\lambda})$,
- $\Phi_\lambda^{\mathsf{enc}} \colon \mathcal{D}(\mathcal{H}_{K,\lambda} \otimes \mathcal{H}_M) \to \mathcal{D}(\mathcal{H}_{T,\lambda})$, and
- $\Phi_\lambda^{\mathsf{dec}} \colon \mathcal{D}(\mathcal{H}_{K,\lambda} \otimes \mathcal{H}_{T,\lambda}) \to \mathcal{D}(\mathcal{H}_M)$,

where $\mathcal{H}_M = \mathcal{Q}(n)$ is the plaintext space, $\mathcal{H}_{T,\lambda} = \mathcal{Q}(\ell(\lambda))$ is the ciphertext space, and $\mathcal{H}_{K,\lambda} = \mathcal{Q}(\kappa(\lambda))$ is the key space for functions $\ell, \kappa \colon \mathbb{N}^+ \to \mathbb{N}^+$.

For all $\lambda \in \mathbb{N}^+$, $k \in \{0,1\}^{\kappa(\lambda)}$, and $m \in \{0,1\}^n$, the maps must satisfy

$$\mathrm{Tr}\left[|k\rangle\langle k| \, \Phi^{\mathsf{key}}(1)\right] > 0 \Rightarrow \mathrm{Tr}\left[|m\rangle\langle m| \, \Phi_k^{\mathsf{dec}} \circ \Phi_k^{\mathsf{enc}} \, |m\rangle\langle m|\right] = 1, \tag{2.7.1}$$

where $\lambda$ is implicit, $\Phi_k^{\mathsf{enc}}$ is the channel defined by $\rho \mapsto \Phi^{\mathsf{enc}}(|k\rangle\langle k| \otimes \rho)$, and we define $\Phi_k^{\mathsf{dec}}$ analogously. We also define the channel $\Phi_{k,0}^{\mathsf{enc}} \colon \mathcal{D}(\mathcal{H}_M) \to \mathcal{D}(\mathcal{H}_{T,\lambda})$ by

$$\rho \mapsto \Phi_k^{\mathsf{enc}}(|\mathbf{0}\rangle\langle\mathbf{0}|) \tag{2.7.2}$$

where $\mathbf{0} \in \{0,1\}^n$ is the all-zero bit string, and the channel $\Phi_{k,1}^{\mathsf{enc}} \colon \mathcal{D}(\mathcal{H}_M) \to \mathcal{D}(\mathcal{H}_{T,\lambda})$ by

$$\rho \mapsto \sum_{m \in \{0,1\}^n} \mathrm{Tr}[|m\rangle\langle m| \, \rho] \cdot \Phi_k^{\mathsf{enc}}(|m\rangle\langle m|). \tag{2.7.3}$$

In Definition 2.7.1, we have three channels: a key generation channel, an encryption channel, and a decryption channel. The security parameter $\lambda$ allows us to determine how large we want our key and ciphertext to be; in our scheme to come, a larger key and ciphertext will result in a better security bound. The meaning of Eq. (2.7.1) is that, if the key is $k$, then encryption of that message with $k$ followed by decryption with $k$ should return the original message.

As part of the security of our scheme, we wish to ensure that should an adversary obtain a copy of the ciphertext and were to know that the original message is one of two hypotheses, she would not be able to distinguish between the hypotheses. We refer to this notion of security as indistinguishable security. It is best understood in terms of a scheme's resilience to an adversary performing what we refer to as a distinguishing attack.

**Definition 2.7.2** (Distinguishing Attack)**.** Let $\mathcal{S} = (\mathsf{key}, \mathsf{enc}, \mathsf{dec})$ be an $n$-QECM. A *distinguishing attack* is a quantum adversary $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ implementing channels of the form

- $A_{0,\lambda} \colon \mathcal{D}(\mathbb{C}) \to \mathcal{D}(\mathcal{H}_M \otimes \mathcal{H}_{S,\lambda})$ and

- $A_{1,\lambda}\colon \mathcal{D}(\mathcal{H}_{T,\lambda} \otimes \mathcal{H}_{S,\lambda}) \to \mathcal{D}(\mathcal{Q})$

where $\mathcal{H}_{S,\lambda} = \mathcal{Q}(s(\lambda))$ for a function $s\colon \mathbb{N}^+ \to \mathbb{N}^+$.

In Definition 2.7.2, we see the first adversarial circuit outputting a message to be sent to the challenger and a memory state. The second adversarial uses the ciphertext received from the challenger along with the memory state in order to make a guess as to whether the challenger encrypted the 0 state or the adversary's message.

**Definition 2.7.3** (Indistinguishable Security)**.** Let $\mathcal{S} = (\mathsf{key}, \mathsf{enc}, \mathsf{dec})$ be an $n$-QECM. Then we say that $\mathcal{S}$ is *indistinguishable secure* if for all distinguishing attacks $\mathcal{A}$ there exists a negligible function $\eta$ such that

$$\mathop{\mathbb{E}}_{b} \mathop{\mathbb{E}}_{k \leftarrow \mathcal{K}} \operatorname{Tr}\left[|b\rangle\langle b|\, A_{1,\lambda} \circ (\Phi^{\mathsf{enc}}_{k,b} \otimes \mathbb{1}_S) \circ A_{0,\lambda}(1)\right] \leq \frac{1}{2} + \eta(\lambda) \tag{2.7.4}$$

where $\lambda$ is implicit on the left-hand side, $b \in \{0,1\}$, and $\mathcal{K}_\lambda$ is the random variable distributed on $\{0,1\}^{\kappa(\lambda)}$ such that

$$\Pr[\mathcal{K}_\lambda = k] = \operatorname{Tr}\Big[|k\rangle\langle k|\, \Phi^{\mathsf{key}}_\lambda(1)\Big]. \tag{2.7.5}$$

In Definition 2.7.3, we see the first important security criterion formalized: it is that the adversary is unable to correctly guess whether the challenger encrypted 0 or the given message with probability greater than negligibly over $\frac{1}{2}$.

# Chapter 3

# Security Definitions

In this chapter, we introduce a new description of the certified deletion security notion. First, however, we must augment our QECM framework to allow it to detect errors on decryption.

## 3.1 QECM Modifications

**Definition 3.1.1** (Augmented Quantum Encryption of Classical Messages)**.** Let $n$ be an integer. Let $\mathcal{S} = (\mathsf{key}, \mathsf{enc}, \mathsf{dec})$ be an $n$-QECM. An *$n$-augmented quantum encryption of classical messages* (n-AQECM) is a tuple of uniform efficient quantum circuits $\hat{\mathcal{S}} = (\mathsf{key}, \mathsf{enc}, \widehat{\mathsf{dec}})$, where $\widehat{\mathsf{dec}}$ implements a channel of the form

$$\Phi_\lambda^{\widehat{\mathsf{dec}}} \colon \mathcal{D}(\mathcal{H}_{K,\lambda} \otimes \mathcal{H}_{T,\lambda}) \to \mathcal{D}(\mathcal{H}_M \otimes \mathcal{Q}). \tag{3.1.1}$$

For all $\lambda \in \mathbb{N}^+, k \in \{0,1\}^{\kappa(\lambda)}$, and $m \in \{0,1\}^n$, the maps corresponding to the circuits must satisfy

$$\mathrm{Tr}\big[|k\rangle\langle k| \, \Phi^{\mathsf{key}}(1)\big] > 0 \Rightarrow \mathrm{Tr}\Big[|m\rangle\langle m| \otimes |1\rangle\langle 1| \, \Phi_k^{\widehat{\mathsf{dec}}} \circ \Phi_k^{\mathsf{enc}} \, |m\rangle\langle m|\Big] = 1, \tag{3.1.2}$$

where $\lambda$ is implicit, $\Phi_k^{\mathsf{enc}}$ is the channel defined by $\rho \mapsto \Phi^{\mathsf{enc}}(|k\rangle\langle k| \otimes \rho)$, and we define $\Phi_k^{\mathsf{dec}}$ analogously.

The extra qubit (which will be referred to as a flag), though by itself without any apparent use, may serve as a way to indicate that the decryption process did not proceed as expected in any given run. In the case of decryption without error, the circuit should output $|1\rangle\langle 1|$, and in the case of decryption error, the circuit should output $|0\rangle\langle 0|$. This allows us to define a criterion by which an AQECM might be robust against a certain amount of noise.

Since the original QECM framework will no longer be used for the rest of this thesis, we henceforth note that all further references to the QECM framework are in fact references to the AQECM framework.

**Definition 3.1.2** (Robust Quantum Encryption of Classical Messages)**.** Let $\mathcal{S} = (\mathsf{key}, \mathsf{enc}, \mathsf{dec})$ be an $n$-QECM. We say that $\mathcal{S}$ is $\epsilon$-*robust* if, for all adversaries $\mathcal{A}$ implementing channels of the form

$$A\colon \mathcal{D}(\mathcal{H}_{T,\lambda}) \to \mathcal{D}(\mathcal{H}_{T,\lambda}), \tag{3.1.3}$$

and for two distinct messages $m, m' \in \mathcal{H}_M$, we have that

$$\mathop{\mathbb{E}}_{k\leftarrow\mathcal{K}} \operatorname{Tr}\left[|m'\rangle\langle m'| \otimes |1\rangle\langle 1| \, \Phi_k^{\mathsf{dec}} \circ A \circ \Phi_k^{\mathsf{enc}} \, |m\rangle\langle m|\right] \leq \epsilon. \tag{3.1.4}$$

In other words, a QECM is $\epsilon$-robust if, under interference by an adversary, the event that decryption yields a different message than was encrypted and that the decryption circuit approves of the outcome is less than or equal to $\epsilon$. This is functionally equivalent to a quantum authentication scheme [BCG+02].

Our description takes the form of an augmentation of the QECM framework described in Definition 3.1.1.

## 3.2 Certified Deletion Encryption and Security

Given a QECM with key $k$ and encrypting message $m$, the certified deletion property should guarantee that the recipient, Bob, cannot do the following two things simultaneously:

- Make Alice, the sender, accept his certificate of deletion; and
- Given $k$, recover information about $m$.

**Definition 3.2.1** (Certified Deletion Encryption)**.** Let $\mathcal{S} = (\mathsf{key}, \mathsf{enc}, \mathsf{dec})$ be an $n$-QECM such that

- $\mathcal{H}_{K,\lambda} = \mathcal{H}_{K',\lambda} \otimes \mathcal{H}_{K'',\lambda}$, where $\mathcal{H}_{K',\lambda} = \mathcal{Q}(\kappa'(\lambda))$ is the decryption key space and $\mathcal{H}_{K'',\lambda} = \mathcal{Q}(\kappa''(\lambda))$ is the auxiliary key space for functions $\kappa', \kappa''\colon \mathbb{N}^+ \to \mathbb{N}^+$; and
- for all $\lambda \in \mathbb{N}^+$, $k = (k', k'') \in \{0,1\}^{\kappa'(\lambda)+\kappa''(\lambda)}$, and $m \in \{0,1\}^n$, it must hold that

$$\operatorname{Tr}\left[|k\rangle\langle k| \, \Phi^{\mathsf{key}}(1)\right] > 0 \Rightarrow \operatorname{Tr}\left[|m\rangle\langle m| \otimes |1\rangle\langle 1| \, \Phi^{\mathsf{dec}}_{(k',0^{\kappa''})} \circ \Phi_k^{\mathsf{enc}} \, |m\rangle\langle m|\right] = 1, \tag{3.2.1}$$

  where $\lambda$ is implicit.

Let $\mathsf{del}$ and $\mathsf{ver}$ be efficient quantum circuits implemented by channels of the form

- $\Phi_\lambda^{\mathsf{del}}\colon \mathcal{D}(\mathcal{H}_{T,\lambda}) \to \mathcal{D}(\mathcal{H}_{D,\lambda})$
- $\Phi_\lambda^{\mathsf{ver}}\colon \mathcal{D}(\mathcal{H}_{K,\lambda} \otimes \mathcal{H}_{D,\lambda}) \to \mathcal{D}(\mathcal{Q})$

where $\mathcal{H}_{D,\lambda} = \mathcal{Q}(d(\lambda))$ for a function $d\colon \mathbb{N}^+ \to \mathbb{N}^+$.

For all $\lambda \in \mathbb{N}^+$, $k \in \{0,1\}^{\kappa(\lambda)}$, and $m \in \{0,1\}^n$, the maps must satisfy

$$\mathrm{Tr}\left[|k\rangle\langle k|\,\Phi^{\mathsf{key}}(1)\right] > 0 \implies \mathrm{Tr}\left[|1\rangle\langle 1|\,\Phi^{\mathsf{ver}} \circ \left(|k\rangle\langle k| \otimes \left(\Phi^{\mathsf{del}} \circ \Phi_k^{\mathsf{enc}}\,|m\rangle\langle m|\right)\right)\right] = 1 \tag{3.2.2}$$

where $\lambda$ is implicit.

We call the tuple $\mathcal{S}' = (\mathsf{key}, \mathsf{enc}, \mathsf{dec}, \mathsf{del}, \mathsf{ver})$ an *$n$-certified deletion encryption* ($n$-CDE).

**Definition 3.2.2** (Certified Deletion Attack)**.** Let $\mathcal{S} = (\mathsf{key}, \mathsf{enc}, \mathsf{dec}, \mathsf{del}, \mathsf{ver})$ be an $n$-CDE. A *certified deletion attack* is a quantum adversary $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2)$ implementing channels of the form

- $A_{0,\lambda}\colon \mathcal{D}(\mathbb{C}) \to \mathcal{D}(\mathcal{H}_M \otimes \mathcal{H}_{S,\lambda})$,
- $A_{1,\lambda}\colon \mathcal{D}(\mathcal{H}_{T,\lambda} \otimes \mathcal{H}_{S,\lambda}) \to \mathcal{D}(\mathcal{H}_{D,\lambda} \otimes \mathcal{H}_{S,\lambda} \otimes \mathcal{H}_{T',\lambda})$, and
- $A_{2,\lambda}\colon \mathcal{D}(\mathcal{H}_{K',\lambda} \otimes \mathcal{H}_{S,\lambda} \otimes \mathcal{H}_{T',\lambda}) \to \mathcal{D}(\mathcal{Q})$

where $\mathcal{H}_{S,\lambda} = \mathcal{Q}(s(\lambda))$ and $\mathcal{H}_{T',\lambda} = \mathcal{Q}(\ell'(\lambda))$ for functions $s, \ell'\colon \mathbb{N}^+ \to \mathbb{N}^+$.

We are now ready to define our notion of Certified Deletion Security. We refer the reader to Section 1.1 for an informal explanation of the definition, and we recall that notation $\Phi_{k,b}^{\mathsf{enc}}$ is defined in Eq. (2.7.2).

**Definition 3.2.3** (Certified Deletion Security)**.** Let $\mathcal{S} = (\mathsf{key}, \mathsf{enc}, \mathsf{dec}, \mathsf{del}, \mathsf{ver})$ be an $n$-CDE. For any fixed and implicit $\lambda \in \mathbb{N}^+$, we define the channel $\Phi_k^{\mathsf{ver}}\colon \mathcal{D}(\mathcal{H}_{K,\lambda} \otimes \mathcal{H}_{D,\lambda}) \to \mathcal{D}(\mathcal{Q} \otimes \mathcal{H}_{K',\lambda})$ by

$$\rho \mapsto \Phi^{\mathsf{ver}}(|k\rangle\langle k| \otimes \rho) \otimes |k'\rangle\langle k'|\,. \tag{3.2.3}$$

Then we say that $\mathcal{S}$ is *$\eta$-certified deletion secure* if for all certified deletion attacks $\mathcal{A}$, there exists a function $\eta$ such that

$$\mathop{\mathbb{E}}_{b} \mathop{\mathbb{E}}_{k \leftarrow \mathcal{K}} \mathrm{Tr}\left[(|1,b\rangle\langle 1,b|)(\mathbb{1} \otimes A_2) \circ (\Phi_k^{\mathsf{ver}} \otimes \mathbb{1}_{ST'}) \circ A_1 \circ (\Phi_{k,b}^{\mathsf{enc}} \otimes \mathbb{1}_S) \circ A_0(1)\right] \leq \frac{1}{2} + \eta(\lambda) \tag{3.2.4}$$

where $\lambda$ is implicit on the left-hand side, $b \in \{0,1\}$, and $\mathcal{K}_\lambda$ is the random variable distributed on $\{0,1\}^{\kappa(\lambda)}$ such that

$$\Pr[\mathcal{K}_\lambda = k] = \mathrm{Tr}\left[|k\rangle\langle k|\,\Phi_\lambda^{\mathsf{key}}(1)\right]. \tag{3.2.5}$$

We say that $\mathcal{S}$ is *certified deletion secure* if there exists such a function $\eta$ that is negligible.

# Chapter 4

# Constructing an Encryption Scheme with Certified Deletion

Scheme 4.0.1 aims to exhibit a noise-tolerant prepare-and-measure $n$-CDE with indistinguishable security and certified deletion.

**Scheme 4.0.1** (Prepare-and-Measure Certified Deletion)**.** Let $n, \lambda, \tau, \mu, m = s + k$ be integers. Let $\Theta = \{\theta \in \{0,1\}^m \mid \omega(\theta) = k\}$ be all $m$-length strings with Hamming weight $k$. Let both $\mathfrak{H}_{\text{ec}} \coloneqq \{h\colon \{0,1\}^s \to \{0,1\}^\tau\}$ and $\mathfrak{H}_{\text{pa}} \coloneqq \{h\colon \{0,1\}^s \to \{0,1\}^n\}$ be universal$_2$ families of hash functions. Let $\text{synd}\colon \{0,1\}^n \to \{0,1\}^\mu$ be an error syndrome function, let $\text{corr}\colon \{0,1\}^n \times \{0,1\}^\mu \to \{0,1\}^n$ be the corresponding function used to calculate the corrected string, and let $\delta \in [0,1]$ be a tolerated error rate for verification. We define a *noise-tolerant prepare-and-measure $n$-CDE* by Circuits 1-5. This scheme satisfies both Equation (3.2.1) and Equation (3.2.2). It is therefore an $n$-CDE.

We note that in Chapter 3, we allow for the general case of both an *auxiliary* and *decryption* key — both keys are accessible to the encryption and verification circuit, but the decryption circuit only has access to the decryption key. Furthermore, after the verification, only the decryption key is revealed. This makes our definition more general, and our scheme makes use of this framework, since the string $r$ is in the auxiliary key only (otherwise, letting $r$ be part of the decryption key would clearly make certified deletion impossible, since correctness would follow without the quantum portion of the ciphertext. However, we note that, strictly speaking, $\mathsf{ver}$ only requires the portion $q = r|_{\bar{\mathcal{I}}}$ of the auxiliary key, and that in fact the certified deletion property holds if we include $q$ in the decryption key. This means that the use of an auxiliary key is unnecessary in our scheme; we have nevertheless chosen to include it for ease of presentation.

| | |
|---|---|
| $M_A^{\theta,x}$ | Measurement operator acting on system $A$ with setting $\theta$ and outcome $x$ |
| $\mathcal{M}^{\mathcal{I}}_{A\to X\|S^\Theta}$ | Measurement map applied on the qubits of system $A$ indexed by $\mathcal{I}$ with setting $S^\Theta$ and outcome stored in register $X$ |
| $\lambda$ | Security parameter |
| $n$ | Length, in bits, of the message |
| $m = \kappa(\lambda)$ | Total number of qubits sent from encrypting party to decrypting party |
| $k$ | Length, in bits, of the string used for verification of deletion |
| $s = m - k$ | Length, in bits, of the string used for extracting randomness |
| $\tau = \tau(\lambda)$ | Length, in bits, of error correction hash |
| $\mu = \mu(\lambda)$ | Length, in bits, of error syndrome |
| $\theta$ | Basis in which the encrypting party prepares her quantum state |
| $\delta$ | Threshold error rate for the verification test |
| $\Theta$ | Set of possible bases from which $\theta$ is chosen |
| $\mathfrak{H}_{\text{pa}}$ | Universal$_2$ family of hash functions used in the privacy amplification scheme |
| $\mathfrak{H}_{\text{ec}}$ | Universal$_2$ family of hash functions used in the error correction scheme |
| $H_{\text{pa}}$ | Hash function used in the privacy amplification scheme |
| $H_{\text{ec}}$ | Hash function used in the error correction scheme |
| $S^\Theta$ | Seed for the choice of $\theta$ |
| $S^{H_{\text{pa}}}$ | Seed for the choice of the hash function used in the error correction scheme |
| $S^{H_{\text{ec}}}$ | Seed for the choice of the hash function used in the privacy amplification scheme |
| synd | Function that computes the error syndrome |
| corr | Function that computes the corrected string |

Table 4.1: Overview of nomenclature used in Chapter 4 and Chapter 5

**Circuit 1:** The key generation circuit $\mathsf{key}$.

**Input** : None.

**Output** : An auxiliary key state $\rho \in \mathcal{D}(\mathcal{Q}(m))$ and a decryption key state $\sigma \in \mathcal{D}(\mathcal{Q}(m+n+\mu+\tau) \otimes \mathfrak{H}_{\text{pa}} \otimes \mathfrak{H}_{\text{ec}}))$.

1 Sample $r \xleftarrow{\$} \{0,1\}^m$.

2 Sample $\theta \xleftarrow{\$} \Theta$.

3 Sample $u \xleftarrow{\$} \{0,1\}^n$.

4 Sample $d \xleftarrow{\$} \{0,1\}^\mu$.

5 Sample $e \xleftarrow{\$} \{0,1\}^\tau$.

6 Sample $H_{\text{pa}} \xleftarrow{\$} \mathfrak{H}_{\text{pa}}$.

7 Sample $H_{\text{ec}} \xleftarrow{\$} \mathfrak{H}_{\text{ec}}$.

8 Output $\rho = |r\rangle\langle r|$ and $\sigma = |\theta, u, d, e, H_{\text{pa}}, H_{\text{ec}}\rangle\langle\theta, u, d, e, H_{\text{pa}}, H_{\text{ec}}|$.

**Circuit 2:** The encryption circuit $\mathsf{enc}$.

**Input :** A plaintext state $|\mathsf{msg}\rangle\langle\mathsf{msg}| \in \mathcal{D}(\mathcal{Q}(n))$, an auxiliary key state $|r\rangle\langle r| \in \mathcal{D}(\mathcal{Q}(m))$, and a decryption key state $|\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}\rangle\langle\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}| \in \mathcal{D}(\mathcal{Q}(m+n+\mu+\tau) \otimes \mathfrak{H}_{\mathrm{pa}} \otimes \mathfrak{H}_{\mathrm{ec}})$.

**Output :** A ciphertext state $\rho \in \mathcal{D}(\mathcal{Q}(m+n+\tau+\mu))$.

1 Compute $x = H_{\mathrm{pa}}(r|_{\mathcal{I}})$ where $\mathcal{I} = \{i \in [m] \mid \theta_i = 0\}$.
2 Compute $p = H_{\mathrm{ec}}(r|_{\mathcal{I}}) \oplus d$.
3 Compute $q = \mathrm{synd}(r|_{\mathcal{I}}) \oplus e$.
4 Output $\rho = \left|r^{\theta}\right\rangle\!\left\langle r^{\theta}\right| \otimes |\mathsf{msg} \oplus x \oplus u, p, q\rangle\langle\mathsf{msg} \oplus x \oplus u, p, q|$.

**Circuit 3:** The decryption circuit $\mathsf{dec}$.

**Input :** A decryption key state $|\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}\rangle\langle\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}| \in \mathcal{D}(\mathcal{Q}(m+n+\mu+\tau) \otimes \mathfrak{H}_{\mathrm{pa}} \otimes \mathfrak{H}_{\mathrm{ec}})$ and a ciphertext $\rho \otimes |c, p, q\rangle\langle c, p, q| \in \mathcal{D}(\mathcal{Q}(m+n+\mu+\tau))$.

**Output :** A plaintext state $\sigma \in \mathcal{D}(\mathcal{Q}(n))$ and an error flag $\gamma \in \mathcal{D}(\mathcal{Q})$.

1 Compute $\rho' = \mathsf{H}^{\theta}\, \rho\, \mathsf{H}^{\theta}$.
2 Measure $\rho'$ in the computational basis. Call the result $r$.
3 Compute $r' = \mathrm{corr}(r|_{\mathcal{I}}, q \oplus e)$ where $\mathcal{I} = \{i \in [m] \mid \theta_i = 0\}$.
4 Compute $p' = H_{\mathrm{ec}}(r') \oplus d$.
5 If $p \neq p'$, then set $\gamma = |0\rangle\langle 0|$. Else, set $\gamma = |1\rangle\langle 1|$.
6 Compute $x' = H_{\mathrm{pa}}(r')$.
7 Output $\sigma \otimes \gamma = |c \oplus x' \oplus u\rangle\langle c \oplus x' \oplus u| \otimes \gamma$.

**Circuit 4:** The deletion circuit $\mathsf{del}$.

**Input :** A ciphertext $\rho \otimes |c, p, q\rangle\langle c, p, q| \in \mathcal{D}(\mathcal{Q}(m+n+\mu+\tau))$.

**Output :** A certificate string state $\sigma \in \mathcal{D}(\mathcal{Q}(m))$.

1 Measure $\rho$ in the Hadamard basis. Call the output $y$.
2 Output $\sigma = |y\rangle\langle y|$.

**Circuit 5:** The verification circuit $\mathsf{ver}$.

**Input :** An auxiliary key state $|r\rangle\langle r| \in \mathcal{D}(\mathcal{Q}(m))$, a decryption key state $|\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}\rangle\langle\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}| \in \mathcal{D}(\mathcal{Q}(m+n+\mu+\tau) \otimes \mathfrak{H}_{\mathrm{pa}} \otimes \mathfrak{H}_{\mathrm{ec}})$, and a certificate string state $|y\rangle\langle y| \in \mathcal{D}(\mathcal{Q}(m))$.

**Output :** A bit.

1 Compute $\hat{y}' = \hat{y}|_{\bar{\mathcal{I}}}$ where $\bar{\mathcal{I}} = \{i \in [m] \mid \theta_i = 1\}$.
2 Compute $q = r|_{\bar{\mathcal{I}}}$.
3 If $\omega(q \oplus \hat{y}') < k\delta$, output 1. Else, output 0.

# Chapter 5

# Security Analysis

In this chapter, we present the security analysis for Scheme 4.0.1: in Section 5.1, we show the security of the scheme in terms of an encryption scheme, then, in Section 5.2, we show that the scheme is correct and robust. Finally in Section 5.3, we show that the scheme is a certified deletion scheme.

## 5.1 Indistinguishable Security

In considering whether Scheme 4.0.1 is indistinguishable secure (Definition 2.7.3), one need only verify that an adversary, given a ciphertext, would not be able to discern whether a known message was encrypted.

**Theorem 5.1.1.** *Scheme 4.0.1 is indistinguishable secure.*

**Proof:** For any distinguishing attack $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$, any state $\rho = \rho_S \otimes |\mathsf{msg}\rangle\langle\mathsf{msg}| \in \mathcal{D}(\mathcal{H}_S \otimes \mathcal{Q}(n))$, and where $k = (r, \theta, u, d, e, H_{\text{pa}}, H_{\text{ec}}) \in \{0,1\}^{m+n+\mu+\tau} \times \mathfrak{H}_{\text{pa}} \times \mathfrak{H}_{\text{ec}}$ is a key, we have that

$$\begin{aligned}
\mathop{\mathbb{E}}_{k}\left(\mathbb{1}_S \otimes \Phi^{\mathsf{enc}}_{k,1}\right)(\rho) &= \frac{1}{2^{m+n+\mu+\tau}|\mathfrak{H}_{\text{pa}}||\mathfrak{H}_{\text{ec}}|}\sum_k \rho_S \otimes \left|r^\theta\right\rangle\!\left\langle r^\theta\right| \\
&\qquad\qquad \otimes |\mathsf{msg} \oplus x \oplus u, p, q\rangle\langle\mathsf{msg} \oplus x \oplus u, p, q| \\
&= \frac{1}{2^{m+n+\mu+\tau}|\mathfrak{H}_{\text{pa}}||\mathfrak{H}_{\text{ec}}|}\sum_k \rho_S \otimes \left|r^\theta\right\rangle\!\left\langle r^\theta\right| \otimes |x \oplus u, p, q\rangle\langle x \oplus u, p, q| \\
&= \mathop{\mathbb{E}}_{k}\left(\mathbb{1}_S \otimes \Phi^{\mathsf{enc}}_{k,0}\right)(\rho),
\end{aligned}$$

where the second equality is due to the uniform distribution of both $\mathsf{msg} \oplus x \oplus u$ and $u$. Therefore, an adversary can do no better than guess $b$ correctly half of the time in a distinguishing attack. This implies perfect indistinguishable security with $\eta = 0$. ∎

## 5.2 Correctness

Thanks to the syndrome and correction functions included in the scheme, the decryption circuit is robust against a certain amount of noise; that is, below such a level of noise, the decryption circuit outputs Alice's original message with high probability. This noise threshold is determined by the distance of the linear code used. In particular, where $\Delta$ is the distance of the code, decryption should proceed normally as long as fewer than $\lfloor \frac{\Delta-1}{2} \rfloor$ errors occur to the quantum encoding of $r|_{\mathcal{I}}$ during transmission through the quantum channel.

To account for greater levels of noise (such as may occur in the presence of an adversary), we show that the error correction measures implemented in Scheme 4.0.1 ensure that errors in decryption are detected with high probability. In other words, we show that the scheme is $\epsilon_{\text{rob}}$-robust, where $\epsilon_{\text{rob}} \coloneqq \frac{1}{2^\tau}$.

Recall that $\tau$ is the length of the error correction hash, and that $\mu$ is the length of the error correction syndrome. Consider that Bob has received a ciphertext state $\rho_B \otimes |c,p,q\rangle\langle c,p,q| \in \mathcal{D}(\mathcal{Q}(m+n+\mu+\tau))$ and a decryption key $(\theta, u, d, e, H_{\text{pa}}, H_{\text{ec}}) \in \Theta \times \{0,1\}^{n+\mu+\tau} \times \mathfrak{H}_{\text{pa}} \times \mathfrak{H}_{\text{ec}}$. Given $\theta$, Bob learns $\mathcal{I}$. This allows him to perform the following measurement on $\rho_B$:

$$\mathcal{M}^{\mathcal{I}}_{B\to Y}(\cdot) = \sum_{y\in\{0,1\}^s} |y\rangle_Y \left(M^{0,y}_{B_{\mathcal{I}}}\right) \cdot \left(M^{0,y}_{B_{\mathcal{I}}}\right)^\dagger \langle y|_Y \tag{5.2.1}$$

The new register $Y$ contains a hypothesis of the random string Alice used in generating $c$. Since $\rho_B$ was necessarily transmitted through a quantum channel, it may have been altered due to noise. Bob calculates a corrected estimate: $\hat{x} = \text{corr}(y, q \oplus e)$. Finally, he compares a hash of the estimate with $p \oplus d$, which is the hash of Alice's corresponding randomness. This procedure is represented by a function $\text{ec}\colon \{0,1\}^s \times \{0,1\}^\mu \times \mathfrak{H}_{\text{ec}} \to \{0,1\}$ defined by

$$\text{ec}(x,y) = \begin{cases} 0 & \text{if } H_{\text{ec}}(x) \neq y \\ 1 & \text{else.} \end{cases} \tag{5.2.2}$$

To record the value of this test, we use a flag $F^{\text{ec}} \coloneqq \text{ec}(\hat{x}, p \oplus d)$. It is very unlikely that both $F^{\text{ec}} = 1$ and the outcome of Bob's decryption procedure is not equal to Alice's originally intended message. This is shown in the following proposition, the proof of which follows that of an analogous theorem in [TL17].

**Theorem 5.2.1.** *If $r \in \{0,1\}^m$ is the random string Alice samples in key generation, and $\hat{x} = \text{corr}(y, q \oplus e)$, then*

$$\Pr[H_{pa}(r|_{\mathcal{I}}) \neq H_{pa}(\hat{x}) \wedge F^{ec} = 1] \leq \frac{1}{2^\tau}. \tag{5.2.3}$$

**Proof:**

$$\begin{aligned}
&\Pr[H_{\mathrm{pa}}(r|_{\mathcal{I}}) \neq H_{\mathrm{pa}}(\hat{x}) \wedge F^{\mathrm{ec}} = 1] \\
&\quad = \Pr[H_{\mathrm{pa}}(r|_{\mathcal{I}}) \neq H_{\mathrm{pa}}(\hat{x}) \wedge H_{\mathrm{ec}}(p \oplus d) = H_{\mathrm{ec}}(\hat{x})] && (5.2.4)\\
&\quad = \Pr[H_{\mathrm{pa}}(r|_{\mathcal{I}}) \neq H_{\mathrm{pa}}(\hat{x}) \wedge H_{\mathrm{ec}}(r|_{\mathcal{I}}) = H_{\mathrm{ec}}(\hat{x})] && (5.2.5)\\
&\quad \leq \Pr[r|_{\mathcal{I}} \neq \hat{x} \wedge H_{\mathrm{ec}}(r|_{\mathcal{I}}) = H_{\mathrm{ec}}(\hat{x})] && (5.2.6)\\
&\quad = \Pr[r|_{\mathcal{I}} \neq \hat{x}] \Pr[H_{\mathrm{ec}}(r|_{\mathcal{I}}) = H_{\mathrm{ec}}(\hat{x})] && (5.2.7)\\
&\quad \leq \Pr[H_{\mathrm{ec}}(r|_{\mathcal{I}}) = H_{\mathrm{ec}}(\hat{x}) \mid r|_{\mathcal{I}} \neq \hat{x}] && (5.2.8)\\
&\quad \leq \frac{1}{|\mathfrak{H}_{\mathrm{ec}}|} && (5.2.9)\\
&\quad = \frac{1}{2^{\tau}}. && (5.2.10)
\end{aligned}$$

The first inequality follows from the fact that $r|_{\mathcal{I}} = \hat{x}$ implies a collision under $H_{\mathrm{pa}}$. The second inequality follows from the fact that it may be true that $r|_{\mathcal{I}} = \hat{x}$. The final inequality follows by the definition of universal$_2$. ∎

## 5.3 Certified Deletion Security

We now prove certified deletion security of Scheme 4.0.1. Our technique consists in formalizing a game (Game 5.3.1 that corresponds to the security definition (Definition 3.2.3) applied to Scheme 4.0.1. Next, we develop an entanglement-based sequence of interactions (Game 5.3.2) which accomplish the same task as in the previous Game (the formal proof that an upper bound on the winning probability of Game 5.3.2 is an upper bound on the winning probability of Game 5.3.1 is postponed until Section 5.4).

To begin, we describe a game which exhibits a certified deletion attack on Scheme 4.0.1, and which thus allows us to examine whether the scheme has certified deletion security. In what follows, the challenger represents the party who would normally encrypt the message, and the adversary $\mathcal{A}$ represents the recipient. The adversary sends the challenger a candidate message $\mathsf{msg}_0 \in \{0,1\}^n$ and Alice chooses, with uniform randomness, whether to encrypt $0^n$ or $\mathsf{msg}_0$; the adversary's task is to guess which one has been encrypted.

**Game 5.3.1** (Prepare-and-Measure Game)**.** Let $\mathcal{S} = (\mathsf{key}, \mathsf{enc}, \mathsf{dec}, \mathsf{del}, \mathsf{ver})$ be an $n$-CDE with $\lambda$ implicit, and with circuits defined as in Scheme 4.0.1. Let $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2)$ be a certified deletion attack. The game is parametric in $b \xleftarrow{\$} \{0,1\}$.

1. Run $|\mathsf{msg}_0\rangle\langle\mathsf{msg}_0|_M \otimes \rho_S \leftarrow A_0(1)$. Generate

$$|\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}, r\rangle\langle\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}, r|_K \leftarrow \Phi^{\mathsf{key}}. \tag{5.3.1}$$

Denote

$$\mathsf{msg} \coloneqq \begin{cases} 0^n & \text{if } b = 0 \\ \mathsf{msg}_0 & \text{if } b = 1. \end{cases} \tag{5.3.2}$$

Compute

$$\left|r^\theta\right\rangle\!\left\langle r^\theta\right|_T \otimes |\mathsf{msg} \oplus x \oplus u, p, q\rangle\langle \mathsf{msg} \oplus x \oplus u, p, q|_T \\ \leftarrow \Phi^{\mathsf{enc}}(|\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}, r\rangle\langle\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}, r|_K \otimes |\mathsf{msg}\rangle\langle\mathsf{msg}|_M). \tag{5.3.3}$$

2. Run

$$|y\rangle\langle y|_D \otimes \rho'_S \otimes \rho_{T'} \leftarrow A_1(\left|r^\theta\right\rangle\!\left\langle r^\theta\right|_T \otimes |\mathsf{msg} \oplus x \oplus u, p, q\rangle\langle \mathsf{msg} \oplus x \oplus u, p, q|_T \otimes \rho_S). \tag{5.3.4}$$

$$\text{If } |0\rangle\langle 0| \leftarrow \Phi^{\mathsf{ver}}(|\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}, r\rangle\langle\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}, r|_K \otimes |y\rangle\langle y|_D), \tag{5.3.5}$$

then $\mathcal{A}$ loses the game. Else, the game continues.

3. Run

$$|b'\rangle\langle b'| \leftarrow A_2(|\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}\rangle\langle\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}|_{K'} \otimes \rho'_S \otimes \rho_{T'}). \tag{5.3.6}$$

If $b' = b$, then $\mathcal{A}$ wins the game.

Per Definition 3.2.3, we say that Scheme 4.0.1 is certified deletion secure if the probability that $\mathcal{A}$ wins Game 5.3.1 is bounded above by $\frac{1}{2} + \eta(\lambda)$, where $\lambda$ is the security parameter and $\eta$ is a negligible function.

Instead of directly analyzing Game 5.3.1, we analyze a game wherein the parties use entanglement; essentially, this allows us show to express the game in a format that is conducive for the analysis that follows. Please note, as we will show in Section 5.4, the probability that Bob wins Game 5.3.1 is bounded above by the probability that Bob wins Game 5.3.2.

**Game 5.3.2** (EPR Game)**.** Alice is the sender, and Bob is the recipient and adversary. The game is parametric in $b \xleftarrow{\$} \{0, 1\}$.

1. Bob selects a string $\mathsf{msg}_0 \in \{0, 1\}^n$ and sends $\mathsf{msg}_0$ to Alice. Bob prepares a tripartite state $\rho_{ABB'} \in \mathcal{D}(\mathcal{Q}(3m))$ where each system contains $m$ qubits. Bob sends the $A$ system to Alice and keeps the systems $B$ and $B'$. Bob measures the $B$ system in the Hadamard basis and obtains a string $y \in \{0, 1\}^m$. Bob sends $y$ to Alice.

2. Alice samples $\theta \xleftarrow{\$} \Theta$, $u \xleftarrow{\$} \{0,1\}^n$, $d \xleftarrow{\$} \{0,1\}^\mu$, $e \xleftarrow{\$} \{0,1\}^\tau$, $H_{\text{pa}} \xleftarrow{\$} \mathfrak{H}_{\text{pa}}$, and $H_{\text{ec}} \xleftarrow{\$} \mathfrak{H}_{\text{ec}}$. She applies a channel to system $A$ which measures $A_i$ according to the computational basis if $\theta_i = 0$ and the Hadamard basis if $\theta_i = 1$. Call the result $r$. Let $\mathcal{I} = \{i \in [m] \mid \theta_i = 0\}$. Alice computes $x = H_{\text{pa}}(r|_{\mathcal{I}}), p = H_{\text{ec}}(r|_{\mathcal{I}}) \oplus d$, and $q = \text{synd}(r|_{\mathcal{I}}) \oplus e$. Alice selects a message:

$$\mathsf{msg} = \begin{cases} 0^n & \text{if } b = 0 \\ \mathsf{msg}_0 & \text{if } b = 1. \end{cases} \tag{5.3.7}$$

If $y = r|_{\bar{\mathcal{I}}}$, Alice sends $(\mathsf{msg} \oplus x \oplus u, \theta, u, d, e, p, q, H_{\text{pa}}, H_{\text{ec}})$ to Bob. If $\omega(y \oplus r|_{\bar{\mathcal{I}}}) \geq k\delta$, Bob loses the game. Otherwise, the game continues.

3. Denote

$$c = (\mathsf{msg} \oplus x \oplus u, \mathsf{msg}_0, \theta, u, d, e, p, q, H_{\text{pa}}, H_{\text{ec}}). \tag{5.3.8}$$

Bob computes

$$|b'\rangle\langle b'| = \mathcal{E}(\rho_{B'} \otimes |c\rangle\langle c|) \tag{5.3.9}$$

for some channel $\mathcal{E}$. If $b' = b$, Bob wins the game. Otherwise, he loses the game.

Game 5.3.2 is intended to model a purified version of Game 5.3.1. Note that Bob's measuremement of $B$ in the Hadamard basis is meant to mimic the $\mathsf{del}$ circuit of Scheme 4.0.1. Although it may seem strange that we impose a limitation of measurement basis on Bob here, it is in fact no limitation at all; indeed, since Bob prepares $\rho_{ABB'}$, he is in total control of the state that gets measured, and hence may assume an arbitrary degree of control over the measurement outcome. Therefore, the assumption that he measures in the Hadamard basis is made without loss of generality.

It may also appear that the adversary in Game 5.3.1 has more information when producing the deletion string than Bob in Game 5.3.2. This, however, is not true, as the adversary in Game 5.3.1 has only received information from Alice that appears to him to be uniformly random (as mentioned, the statement is formalized later, in Section 5.4). In order to further the analysis, we assign more precise notation for the maps described in Game 5.3.2.

**Bob's measurements.** Measurement of Bob's system $B$ of $m$ qubits in Step 1 is represented using two channels: one acting on the systems in $\mathcal{I}$, with outcome recorded in register $Y$; and one acting on the systems in $\bar{\mathcal{I}}$, with outcome recorded in $W$. Note, however, that Bob has no access to $\theta$, and therefore has no way of determining $\mathcal{I}$. The formal separation of registers $Y$ and $W$ is simply for future ease of specifying the qubits to which we refer.

Recall the definition of the measurements $M_B^{x,y}$ from Section 2.3.2.

The first measurement, where the outcome is stored in register $Y$, is defined by

$$\mathcal{M}^{\mathcal{I}}_{B\to Y}(\cdot) = \sum_{y\in\{0,1\}^s} |y\rangle_Y \left(M^{1,y}_{B_{\mathcal{I}}}\right)\cdot\left(M^{1,y}_{B_{\mathcal{I}}}\right)^\dagger \langle y|_Y \tag{5.3.10}$$

and the second, where the outcome is stored in register $W$, is defined by

$$\mathcal{M}^{\bar{\mathcal{I}}}_{B\to W}(\cdot) = \sum_{w\in\{0,1\}^k} |w\rangle_W \left(M^{1,w}_{B_{\bar{\mathcal{I}}}}\right)\cdot\left(M^{1,w}_{B_{\bar{\mathcal{I}}}}\right)^\dagger \langle w|_W\,, \tag{5.3.11}$$

where $M^{1,y}_{B_{\mathcal{I}}} \coloneqq \bigotimes_{i\in\mathcal{I}} M^{1,y_i}_{B_i}$, and the definition of $M^{1,w}_{B_{\bar{\mathcal{I}}}}$ is analogous.

**Alice's measurements.** We represent the randomness of Alice's sampling using seed registers. Thus, the randomness used for Alice's choice of basis is represented as

$$\rho_{S^\Theta} = \frac{1}{\binom{m}{k}} \sum_{\theta\in\Theta} |\theta\rangle\langle\theta|_{S^\Theta}\,. \tag{5.3.12}$$

Similarly, Alice's randomness for choice of a hash function for privacy amplification is represented as

$$\rho_{S^{H_{\mathrm{pa}}}} = \frac{1}{|\mathfrak{H}_{\mathrm{pa}}|} \sum_{h\in\mathfrak{H}_{\mathrm{pa}}} |h\rangle\langle h|_{S^{H_{\mathrm{pa}}}}\,. \tag{5.3.13}$$

Recall that $m = s + k$, where $k$ is the weight of all strings in $\Theta$. Measurement of Alice's system $A$ of $m$ qubits in Step 2 is represented using two channels: one acting on the systems in $\mathcal{I}$, with outcome recorded in register $X$ (by definition, these qubits are measured in the computational basis); and one acting on the systems in $\bar{\mathcal{I}}$, with outcome recorded in register $V$ (by definition, these qubits are measured in the Hadamard basis).

$$\mathcal{M}^{\mathcal{I}}_{A\to X|S^\Theta}(\cdot) = \sum_{\theta\in\Theta}\sum_{x\in\{0,1\}^s} |x\rangle_X \left(M^{0,x}_{A_{\mathcal{I}}}\otimes|\theta\rangle\langle\theta|_{S^\Theta}\right)\cdot\left(M^{0,x}_{A_{\mathcal{I}}}\otimes|\theta\rangle\langle\theta|_{S^\Theta}\right)^\dagger\langle x|_X\,;$$

and the second measurement, where the outcome is stored in register $V$, is defined by

$$\mathcal{M}^{\bar{\mathcal{I}}}_{A\to V|S^\Theta}(\cdot) = \sum_{\theta\in\Theta}\sum_{v\in\{0,1\}^k} |v\rangle_V \left(M^{1,v}_{A_{\bar{\mathcal{I}}}}\otimes|\theta\rangle\langle\theta|_{S^\Theta}\right)\cdot\left(M^{1,v}_{A_{\bar{\mathcal{I}}}}\otimes|\theta\rangle\langle\theta|_{S^\Theta}\right)^\dagger\langle v|_V\,,$$

where $M^{0,x}_{A_{\mathcal{I}}} \coloneqq \bigotimes_{i\in\mathcal{I}} M^{0,x_i}_{A_i}$ and the definition of $M^{1,v}_{A_{\bar{\mathcal{I}}}}$ is analogous.

We also introduce a hypothetical measurement for the sake of the security analysis. Consider the case where Alice measures all of her qubits in the Hadamard basis. In this case, instead of $\mathcal{M}^{\mathcal{I}}_{A\to X|S^\Theta}$, Alice would use the measurement

$$\mathcal{M}^{\mathcal{I}}_{A\to Z|S^\Theta}(\cdot) = \sum_{\theta\in\Theta}\sum_{z\in\{0,1\}^s} |z\rangle_Z \left(M^{1,z}_{A_{\mathcal{I}}}\otimes|\theta\rangle\langle\theta|_{S^\Theta}\right)\cdot\left(M^{1,z}_{A_{\mathcal{I}}}\otimes|\theta\rangle\langle\theta|_{S^\Theta}\right)^\dagger\langle z|_Z\,.$$

Each of Alice's and Bob's measurements commute with each other as they all act on distinct quantum systems. We can thus define the total measurement map

$$\mathcal{M}_{AB\to VWXY|S^\Theta} = \mathcal{M}^{\mathcal{I}}_{A\to X|S^\Theta} \circ \mathcal{M}^{\bar{\mathcal{I}}}_{A\to V|S^\Theta} \circ \mathcal{M}^{\mathcal{I}}_{B\to Y} \circ \mathcal{M}^{\bar{\mathcal{I}}}_{B\to W}. \tag{5.3.14}$$

The overall post-measurement state is denoted $\sigma_{VWXYS^\Theta}$ and is given by

$$\begin{aligned}
&\sigma_{VWXYS^\Theta} \\
&= \mathrm{Tr}_{AB}[\mathcal{M}_{AB\to VWXY|S^\Theta}(\rho_{ABS^\Theta})] \\
&= \sum_{\theta\in\Theta} \sum_{x,y\in\{0,1\}^s} \sum_{v,w\in\{0,1\}^k} \frac{1}{\binom{m}{k}} |\theta\rangle\langle\theta|_{S^\Theta} \otimes |v,w,x,y\rangle\langle v,w,x,y|_{VWXY} \otimes \\
&\quad \mathrm{Tr}_{AB}\left[\left((M^{\theta,x}_{A_{\mathcal{I}}})^\dagger M^{\theta,x}_{A_{\mathcal{I}}} \otimes (M^{\theta,v}_{A_{\bar{\mathcal{I}}}})^\dagger M^{\theta,v}_{A_{\bar{\mathcal{I}}}} \otimes (M^{\theta,y}_{B_{\mathcal{I}}})^\dagger M^{\theta,y}_{B_{\mathcal{I}}} \otimes (M^{\theta,w}_{B_{\bar{\mathcal{I}}}})^\dagger M^{\theta,w}_{B_{\bar{\mathcal{I}}}}\right) \rho_{AB}\right]
\end{aligned}$$

We analogously define the hypothetical post-measurement state $\hat{\sigma}_{VWZYS^\Theta}$.

**Alice's verification:** Alice completes the verification procedure by comparing the $V$ register to the $W$ register. If they differ in less than $k\delta$ bits, then the test is passed. The test is represented by a function $\mathrm{comp}\colon \{0,1\}^k \times \{0,1\}^k \to \{0,1\}$ defined by

$$\mathrm{comp}(v,w) = \begin{cases} 0 & \text{if } \omega(v\oplus w) \geq k\delta \\ 1 & \text{else.} \end{cases} \tag{5.3.15}$$

To record the value of this test, we use a flag $F^{\mathrm{comp}} := \mathrm{comp}(v,w)$.

The import of the outcome of this comparison test is that if Bob is good at guessing Alice's information in the Hadamard basis, it is unlikely that he is good at guessing Alice's information in the computational basis. This trade-off is represented in the uncertainty relation of Proposition 2.5.5.

Note that we can define the post-comparison test state, since $A|_{\mathcal{I}}$ is disjoint from $A|_{\bar{\mathcal{I}}}$ and $B|_{\mathcal{I}}$ is disjoint from $B|_{\bar{\mathcal{I}}}$. The state is denoted $\tau_{ABVWS^\Theta|F^{\mathrm{comp}}=1}$ and is given by

$$\begin{aligned}
\tau_{ABVWS^\Theta|F^{\mathrm{comp}}=1} = \frac{1}{\Pr[F^{\mathrm{comp}}=1]} \sum_{\theta\in\Theta} \sum_{\substack{v,w\in\{0,1\}^k \\ \omega(v_i\oplus w_i)<k\delta}} \frac{1}{\binom{m}{k}} |\theta\rangle\langle\theta|_{S^\Theta} \otimes \\
|v,w\rangle\langle v,w|_{VW} \otimes (M^{1,v}_{A_{\bar{\mathcal{I}}}} \otimes M^{1,w}_{B_{\bar{\mathcal{I}}}}) \rho_{AB} (M^{1,v}_{A_{\bar{\mathcal{I}}}} \otimes M^{1,w}_{B_{\bar{\mathcal{I}}}})^\dagger.
\end{aligned} \tag{5.3.16}$$

The following proposition shows that in order to ensure that Bob's knowledge of $X$ is limited after a successful comparison test, and receiving the decryption key, his knowledge about Alice's hypothetical Hadamard measurement outcome must be bounded below.

**Proposition 5.3.3.** *Let $\epsilon \geq 0$. Then*

$$H^{\epsilon}_{\min}(X \wedge F^{\text{comp}} = 1|VWS^{\Theta}B')_{\sigma} + H^{\epsilon}_{\max}(Z \wedge F^{\text{comp}} = 1|Y)_{\hat{\sigma}} \geq s. \tag{5.3.17}$$

**Proof:** We apply Proposition 2.5.5 to the state $\tau_{ABVWS^{\Theta}|F^{\text{comp}}=1}$.To do this, we equate $C = VWS^{\Theta}B'$ and $E = S^{\Theta}B$. Using the measurement maps $\mathcal{M}_{A\to X|S^{\Theta}}$ and $\mathcal{M}_{A\to Z|S^{\Theta}}$ and applying Proposition 2.5.5 then yields

$$H^{\epsilon}_{\min}(X \wedge F^{\text{comp}} = 1|VWS^{\Theta}B')_{\sigma} + H^{\epsilon}_{\max}(Z \wedge F^{\text{comp}} = 1|S^{\Theta}B)_{\tau} \geq s. \tag{5.3.18}$$

We then apply the measurement map $\mathcal{M}_{B\to Y|S^{\Theta}}$ and discard $S^{\Theta}$. Finally, by Proposition 2.5.4, we note that

$$H^{\epsilon}_{\max}(Z \wedge F^{\text{comp}} = 1 \mid S^{\Theta}B)_{\tau} \leq H^{\epsilon}_{\max}(Z \wedge F^{\text{comp}} = 1 \mid Y)_{\hat{\sigma}}, \tag{5.3.19}$$

which concludes the proof. ∎

In the spirit of [TL17], we provide an upper bound for the max-entropy quantity, thus establishing a lower bound for the min-entropy quantity.

**Proposition 5.3.4.** *Letting $\nu \in (0,1)$, we define*

$$\epsilon(\nu) \coloneqq \exp\left(\frac{-sk^2\nu^2}{m(k+1)}\right). \tag{5.3.20}$$

*Then, for any $\nu \in (0, \frac{1}{2} - \delta]$ such that $\epsilon(\nu)^2 < \Pr[F^{\text{comp}} = 1]_{\sigma} = \Pr[F^{\text{comp}} = 1]_{\hat{\sigma}}$,*

$$H^{\epsilon(\nu)}_{\max}(Z \wedge F^{\text{comp}} = 1 \mid Y)_{\hat{\sigma}} \leq s \cdot h(\delta + \nu) \tag{5.3.21}$$

*where*

$$h(x) \coloneqq -x \log x - (1-x)\log(1-x). \tag{5.3.22}$$

**Proof:** Define the event

$$\Omega \coloneqq \begin{cases} 1 & \text{if } \omega(Z \oplus Y) \geq s(\delta + \nu) \\ 0 & \text{else.} \end{cases} \tag{5.3.23}$$

Using Lemma 2.6.1, we get that

$$\Pr\left[F^{\text{comp}} = 1 \wedge \Omega\right]_{\hat{\sigma}} = \Pr\left[\omega(V \oplus W) \leq k\delta \wedge \omega(Z \oplus Y) \geq s(\delta + \nu)\right]_{\hat{\sigma}} \tag{5.3.24}$$

$$\leq \epsilon(\nu)^2. \tag{5.3.25}$$

Given the state $\hat{\sigma}_{ZYF^{\text{comp}}=1}$, we use Lemma 2.6.3 to remove the possibility of $\Omega$ and arrive at the smoothed state $\tilde{\sigma}_{ZYF^{\text{comp}}}$ with $\Pr[\Omega]_{\tilde{\sigma}} = 0$ and

$$P(\hat{\sigma}_{ZYF^{\text{comp}}=1}, \tilde{\sigma}_{ZYF^{\text{comp}}}) \leq \epsilon(\nu). \tag{5.3.26}$$

Since $\Pr[F^{\text{comp}} = 1]_{\tilde{\sigma}} = 1$, we get that

$$H_{\max}^{\epsilon(\nu)}(Z \wedge F^{\text{comp}} = 1 \mid Y)_{\hat{\sigma}} \leq H_{\max}(Z \wedge F^{\text{comp}} = 1 \mid Y)_{\tilde{\sigma}} = H_{\max}(Z \mid Y)_{\tilde{\sigma}}. \quad (5.3.27)$$

Expanding this conditional max-entropy [Tom12, Sec. 4.3.2], we obtain

$$\begin{aligned} H_{\max}(Z \mid Y)_{\tilde{\sigma}} &= \log \left( \sum_{y \in \{0,1\}^s} \Pr[Y = y]_{\tilde{\sigma}} 2^{H_{\max}(Z|Y)_{\tilde{\sigma}}} \right) && (5.3.28) \\ &\leq \max_{\substack{y \in \{0,1\}^s \\ \Pr[Y=y]_{\tilde{\sigma}} > 0}} H_{\max}(Z \mid Y = y)_{\tilde{\sigma}} && (5.3.29) \\ &\leq \max_{\substack{y \in \{0,1\}^s \\ \Pr[Y=y]_{\tilde{\sigma}} > 0}} \log \left| \{ z \in \{0,1\}^s \colon \Pr[Z = z \mid Y = y]_{\tilde{\sigma}} > 0 \} \right| && (5.3.30) \\ &= \max_{y \in \{0,1\}^s} \log \left| \{ z \in \{0,1\}^s \colon \Pr[Z = z \wedge Y = y]_{\tilde{\sigma}} > 0 \} \right|. && (5.3.31) \end{aligned}$$

Since $\Pr[\Omega]_{\tilde{\sigma}} = 0$, we have

$$\begin{aligned} &\left| \{ z \in \{0,1\}^s \colon \Pr[Z = z \wedge Y = y]_{\tilde{\sigma}} > 0 \} \right| \\ &\qquad \leq \left| \{ z \in \{0,1\}^s \colon \omega(z \oplus y) < s(\delta + \nu) \} \right| && (5.3.32) \\ &\qquad = \sum_{\gamma=0}^{\lfloor s(\delta+\nu) \rfloor} \binom{s}{\gamma}. && (5.3.33) \end{aligned}$$

When $\delta + \nu \leq 1/2$ (see [vLvdG12, Sec. 1.4]), we have that $\sum_{\gamma=0}^{\lfloor s(\delta=\nu) \rfloor} \binom{s}{\gamma} \leq 2^{s \cdot h(\delta+\nu)}$. ∎

At this point, we use Proposition 2.5.6, the Leftover Hashing Lemma, to turn the min-entropy bound into a statement about how close to uniformly random the string $\tilde{X} = H_{\text{pa}}(X)$ is from Bob's perspective. We name this final state $\zeta_{\tilde{X}SF^{\text{comp}}E \wedge F^{\text{comp}}=1} = \text{Tr}_X[\mathcal{E}_f(\sigma_{XS^{\Theta}S^{H_{\text{ec}}}F^{\text{comp}}} \otimes \rho_{S^{H_{\text{pa}}}})]$ for the function $f \colon (X, H_{\text{pa}}) \mapsto H_{\text{pa}}(X)$. We compare this to the state $\chi_{\tilde{X}} \otimes \zeta_{SF^{\text{comp}}E \wedge F^{\text{comp}}=1}$ where $\chi_{\tilde{X}}$ is the fully mixed state on $\tilde{X}$.

**Proposition 5.3.5.** *Let $\epsilon(\nu)$ be as defined in (5.3.20). Then for any $\nu \in (0, \frac{1}{2} - \delta]$ such that $\epsilon(\nu)^2 < \Pr[F^{\text{comp}} = 1]_{\sigma}$, we have*

$$\| \zeta_{\tilde{X}SF^{\text{comp}}E \wedge F^{\text{comp}}=1} - \chi_{\tilde{X}} \otimes \zeta_{SF^{\text{comp}}E \wedge F^{\text{comp}}=1} \|_{\text{Tr}} \leq \frac{1}{2} 2^{-\frac{1}{2} g(\nu)} + 2\epsilon(\nu), \quad (5.3.34)$$

*where $g(\nu) \coloneqq s(1 - h(\delta + \nu)) - n$.*

**Proof:** By Proposition 5.3.4, we see that

$$H_{\max}^{\epsilon(\nu)}(Z \wedge F^{\text{comp}} = 1 \mid Y)_{\sigma} \leq s \cdot h(\delta + \nu). \quad (5.3.35)$$

Together, with Proposition 5.3.3, this means that

$$H_{\min}^{\epsilon}(X \wedge F^{\text{comp}} = 1|VWS^{\Theta}B')_{\sigma} \geq sq, \tag{5.3.36}$$

where $q = 1 - h(\delta + \nu)$. Finally, applying Proposition 2.5.6, we obtain the desired inequality. ∎

For the case where $\epsilon(\nu)^2 \geq \Pr[F^{\text{comp}} = 1]_{\sigma}$, we note that the trace distance $\|\zeta_{\tilde{X}SF^{\text{comp}}E\wedge F^{\text{comp}}=1} - \chi_{\tilde{X}} \otimes \zeta_{SF^{\text{comp}}E\wedge F^{\text{comp}}=1}\|_{\text{Tr}}$ is upper bounded by the trace of both states ($\Pr[F^{\text{comp}} = 1]_{\zeta}$). Therefore, the inequalities $\Pr[F^{\text{comp}} = 1]_{\zeta} \leq \epsilon(\nu)^2 \leq \epsilon(\nu)$ grants us the following corollary.

**Corollary 5.3.6.** *For any $\nu \in (0, \frac{1}{2} - \delta]$, the following holds:*

$$\begin{aligned}\|\zeta_{\tilde{X}SF^{\text{comp}}E\wedge F^{\text{comp}}=1} - \chi_{\tilde{X}} \otimes \zeta_{SF^{\text{comp}}E\wedge F^{\text{comp}}=1}\|_{\text{Tr}} \\ \leq \frac{1}{2}\sqrt{2^{-s(1-h(\delta+\nu))+n}} + 2\epsilon(\nu).\end{aligned} \tag{5.3.37}$$

Finally, we would like to translate this statement into a probability that Bob would win Game 5.3.2. Let $\zeta^{g}_{\tilde{X}SF^{\text{comp}}E\wedge F^{\text{comp}}=1}$ be the state of $\zeta_{\tilde{X}SF^{\text{comp}}E\wedge F^{\text{comp}}=1}$ in the case that $g \in \{0, 1\}$ was selected at the beginning of Game 5.3.2.

**Corollary 5.3.7.** *The probability that Bob wins Game 5.3.2 is bounded above by $\frac{1}{2} + 2\left(\frac{1}{2}\sqrt{2^{-s(1-h(\delta+\nu))+n}} + 2\epsilon(\nu)\right)$.*

**Proof:**

$$\|\zeta^{0}{}_{\tilde{X}SF^{\text{comp}}E\wedge F^{\text{comp}}=1} - \zeta^{1}_{\tilde{X}SF^{\text{comp}}E\wedge F^{\text{comp}}=1}\|_{\text{Tr}} \tag{5.3.38}$$

$$\begin{aligned}&\leq \|\zeta^{0}_{\tilde{X}SF^{\text{comp}}E\wedge F^{\text{comp}}=1} - \chi_{\tilde{X}} \otimes \zeta_{SF^{\text{comp}}E\wedge F^{\text{comp}}=1}\|_{\text{Tr}} \\ &+\|\zeta^{1}_{\tilde{X}SF^{\text{comp}}E\wedge F^{\text{comp}}=1} - \chi_{\tilde{X}} \otimes \zeta_{SF^{\text{comp}}E\wedge F^{\text{comp}}=1}\|_{\text{Tr}}\end{aligned} \tag{5.3.39}$$

$$= 2\left(\frac{1}{2}\sqrt{2^{-s(1-h(\delta+\nu))+n}} + 2\epsilon(\nu)\right). \tag{5.3.40}$$

The conclusion follows from Theorem 2.3.9. ∎

## 5.4 Security Reduction

We now show that the security of Game 5.3.1 can be reduced to that of Game 5.3.2. In order to do so, we construct a sequence of games starting at Game 5.3.1 and

ending at Game 5.3.2. Each game will be winnable by the adversary (or Bob) with a probability only less than or equal to that of the subsequent game.

The first new game, $G$, deprives $\mathcal{A}_1$ of the classical portion of the ciphertext. In the second new game, $G'$, instead of selecting $r$ uniformly at random, $m$ EPR pairs are prepared, with one half of each being sent to the adversary, and the other half of each being measured in basis $\theta$, yielding $r$. In the third new game, $G''$, the aforementioned measurement, and hence the determination of $r$, is delayed until after running $\mathcal{A}_1$.

**Proposition 5.4.1.** *The probability that $\mathcal{A}$ wins Game 5.3.1 is bounded above by the probability that Bob wins Game 5.3.2.*

**Proof:** The probability that $\mathcal{A}$ wins Game 5.3.1 is given by the following formula:

$$\Pr[b = b' \wedge |1\rangle\langle 1| \leftarrow \Phi^{\mathsf{ver}}(\rho_K \otimes |y\rangle\langle y|_D) \mid \textit{Game } 5.3.1]. \tag{5.4.1}$$

The probability that Bob wins Game 5.3.2 is given by the following formula:

$$\Pr[b = b' \wedge \omega(y \oplus r|_{\bar{T}}) < k\delta \mid \textit{Game } 5.3.2]. \tag{5.4.2}$$

Let $G$ be a game like Game 5.3.1 except that, in $G$, $\mathcal{A}_1$ does not have access to $|\mathsf{msg} \oplus x \oplus u, p, q\rangle\langle \mathsf{msg} \oplus x \oplus u, p, q|$. Then

$$\begin{aligned} &\Pr[b = b' \wedge |1\rangle\langle 1| \leftarrow \Phi^{\mathsf{ver}}(\rho_K \otimes |y\rangle\langle y|_D) \mid \textit{Game } 5.3.1] \\ &= \Pr[b = b' \wedge |1\rangle\langle 1| \leftarrow \Phi^{\mathsf{ver}}(\rho_K \otimes |y\rangle\langle y|_D) \mid G], \end{aligned} \tag{5.4.3}$$

because, from the perspective of $\mathcal{A}_1$ in Game 5.3.1, $|\mathsf{msg} \oplus x \oplus u, p, q\rangle\langle \mathsf{msg} \oplus x \oplus u, p, q|$ is uniformly random. Let $G'$ be a game like $G$ except that, in $G'$, instead of $A_1$ being given $\left|r^\theta\right\rangle\!\left\langle r^\theta\right|$, $m$ EPR pairs are prepared, yielding quantum systems $A$ and $B$, of which the adversary $A_1$ is given $B$. System $A$ is measured in basis $\theta$ yielding a string $r$, and $\mathcal{A}_1$ then computes

$$|y\rangle\langle y|_D \otimes \rho'_S \otimes \rho_{T'} \leftarrow A_1(\rho_B \otimes \rho_S). \tag{5.4.4}$$

We show that, due to the measurement of system $A$, adversary $\mathcal{A}_1$ receives $\left|r^\theta\right\rangle\!\left\langle r^\theta\right|$, where $r$ is uniformly random. The post-measurement state, conditioned on the measurement of system $A$ yielding outcome $r$, will be equivalent to

$$|\psi_r\rangle = \left(\mathsf{H}^\theta |r\rangle\langle r| \mathsf{H}^\theta \otimes 1_m\right) |\mathrm{EPR}^m\rangle \tag{5.4.5}$$

$$= \left(\mathsf{H}^\theta \otimes 1_m\right) \left(|r\rangle\langle r| \otimes 1_m\right) \left(1_m \otimes \mathsf{H}^\theta\right) |\mathrm{EPR}^m\rangle \tag{5.4.6}$$

$$= \sum_{\tilde{r} \in \{0,1\}^m} \frac{1}{2^{m/2}} \left(\mathsf{H}^\theta |r\rangle\langle r| |\tilde{r}\rangle\right) \left(\mathsf{H}^\theta |\tilde{r}\rangle\right) \tag{5.4.7}$$

$$= \frac{1}{2^{m/2}} \left(\mathsf{H}^\theta |r\rangle\right) \left(\mathsf{H}^\theta |r\rangle\right) \tag{5.4.8}$$

$$= \frac{1}{2^{m/2}} \left|r^\theta\right\rangle \otimes \left|r^\theta\right\rangle, \tag{5.4.9}$$

which occurs with probability $\| |\psi_r\rangle \|^2 = \frac{1}{2^m}$. Therefore,

$$\begin{aligned}&\Pr[b = b' \wedge |1\rangle\langle 1| \leftarrow \Phi^{\mathsf{ver}}(\rho_K \otimes |y\rangle\langle y|_D) \mid G] \\ &= \Pr[b = b' \wedge |1\rangle\langle 1| \leftarrow \Phi^{\mathsf{ver}}(\rho_K \otimes |y\rangle\langle y|_D) \mid G'].\end{aligned} \tag{5.4.10}$$

Let $G''$ be a game like $G'$ except that, in $G''$, instead of system $A$ being measured before running $\mathcal{A}_1$, system $A$ is measured after. Then

$$\begin{aligned}&\Pr[b = b' \wedge |1\rangle\langle 1| \leftarrow \Phi^{\mathsf{ver}}(\rho_K \otimes |y\rangle\langle y|_D) \mid G'] \\ &= \Pr[b = b' \wedge |1\rangle\langle 1| \leftarrow \Phi^{\mathsf{ver}}(\rho_K \otimes |y\rangle\langle y|_D) \mid G''],\end{aligned} \tag{5.4.11}$$

because the measurement and $A_1$ act on distinct systems, and therefore commute. $G''$ is like Game 5.3.2 except that, in the latter game, Bob is the party that prepares the state. Since allowing Bob to select the initial state can only increase Bob's chance of winning, it follows that

$$\begin{aligned}&\Pr[b = b' \wedge |1\rangle\langle 1| \leftarrow \Phi^{\mathsf{ver}}(\rho_K \otimes |y\rangle\langle y|_D) \mid G''] \\ &\leq \Pr[b = b' \wedge \omega(y \oplus r|_{\bar{\mathcal{I}}}) < k\delta \mid \textit{Game 5.3.2}].\end{aligned} \tag{5.4.12}$$

∎

**Theorem 5.4.2.** *Scheme 4.0.1 is certified deletion secure.*

**Proof:** By Corollary 5.3.7, Bob can win Game 5.3.2 with at most a probability of

$$\frac{1}{2} + 2\left(\frac{1}{2}\sqrt{2^{-s(1-h(\delta+\nu))+n}} + 2\epsilon(\nu)\right). \tag{5.4.13}$$

By Proposition 5.4.1, this also serves as an upper bound for the probability that $\mathcal{A}$ wins Game 5.3.1. Since Game 5.3.1 is a certified deletion attack for Scheme 4.0.1, we see that Scheme 4.0.1 is $\eta$-certified deletion secure for

$$\eta(\lambda) = 2\left(\frac{1}{2}\sqrt{2^{-(s(\lambda))(1-h(\delta+\nu))+n}} + 2\exp\left(\frac{-(s(\lambda))(k(\lambda))^2\nu^2}{(m(\lambda))((k(\lambda))+1)}\right)\right), \tag{5.4.14}$$

which is negligible for large enough functions $s, k$. ∎

# Chapter 6

# Conclusion

We have built on the QECM framework (Definition 2.7.1) to give rise to a new type of scheme (Definition 3.2.1) and security notion (Definition 3.2.3). We presented an encryption scheme (Scheme 4.0.1) which satisfies indistinguishable security (Theorem 5.1.1), is robust to a certain amount of noise (Theorem 5.2.1), and satisfies the new security notion (Theorem 5.4.2). This has scaled up the task originally posed by Fu and Miller [FM18] while only requiring commercially available technology.

There remain a number of issues which could leave openings for future work. We present a few potential avenues here.

**Can the key be shortened?** The current key is very lengthy, and this would pose a problem in scenarios where shorter key lengths are desired. Can the key length be shortened while retaining the level of security guaranteed by Scheme 4.0.1? If not, is there a feasible scheme with a reduced key length, yet which guarantees some useful level of security? Indeed, one could consider limiting adversaries in terms of computational power. Moreover, the current scheme guarantees perfect indistinguishable security, whereas one could potentially achieve the indistinguishable security of Definition 2.7.3 without going to the length seen in our work.

**Timed-release encryption with classical revocation.** Comparing our scheme to that of [Unr14], a notable difference is that Unruh's revocation step requires the transmission of quantum information, while our deletion step requires only the transmission of classical information. However, our proof does not guarantee that the scheme would carry its security guarantee if the key were given to Bob in a timed-release encryption (TRE). As Unruh notes, Bob's possession of the TRE complicates the matter of security due to the randomness extractor being fixed and included in the TRE. Therefore, the question remains: is it possible to develop a secure timed-release encryption scheme with classical revocation?

**Everlasting security.** Using our quantum encoding, it may be possible to transform a long-term computational assumption into a temporary one. That is, that a computational assumption would need to be broken *during* a protocol, or else the security is information-theoretically secure as soon as the protocols ends. This is called *everlasting security* [Unr13].

For example, consider the situation encountered in a zero-knowledge proof system for a $\Sigma$ protocol (for instance, for graph 3-colouring [GMW91]): the prover commits to an encoding of an NP-witness using a statistically binding and computationally concealing commitment scheme. The verifier then randomly chooses which commitments to open, and the prover provides the information required to open the commitment. If, in addition, we could encode the commitments with a scheme that provides certified deletion, then the verifier could also prove that the unopened commitments are effectively *deleted*. This has the potential of ensuring that the zero-knowledge property becomes *statistical* as long as the computational assumption is not broken *during* the execution of the proof system. This description assumes an extension of our certified deletion encoding to the computational setting, and also somehow assumes that the verifier would collaborate in its deletion actions (we leave for future work the formal statement and analysis). Nevertheless, since zero-knowledge proofs are building blocks for a host of cryptographic protocols, certified deletion has the potential to unleash everlasting security, which is highly desirable given steady progress in both algorithms and quantum computers.

**Public verification.** In the scheme we present in this thesis, verification of a certificate of deletion can only be done by a party who has access to the entire key, e.g. Alice. However, is it possible for a third party, without access to the entire key, to independently verify that the recipient has deleted the message? Consider the following addition to our scheme. Let $H$ be a randomly selected universal$_2$ hash function with domain $\{0,1\}^k$ and have Alice secretly distribute it among third parties along with $\theta$ and $H(r_{\bar{\mathcal{I}}})$. Then, upon receiving the certificate of deletion $y$, the third parties can verify it by checking whether $H(r_{\bar{\mathcal{I}}}) = H(y_{\bar{\mathcal{I}}})$. Other potential schemes with this property, along with accompanying analyses, might be worth further research.

# Bibliography


[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.

[BCG+02] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp. Authentication of quantum messages. In *43rd Annual Symposium on Foundations of Computer Science—FOCS 2002*, pages 449–485, 2002. DOI: 10.1109/SFCS.2002.1181969.

[BL19] A. Broadbent and S. Lord. Uncloneable quantum encryption via oracles, 2019. Available at https://arxiv.org/abs/1903.00130.

[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.

[CW79] J. L. Carter and M. N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2): 143–154, 1979. DOI: 10.1016/0022-0000(79)90044-8.

[CW19] X. Coiteux-Roy and S. Wolf. Proving erasure, 2019. Available at https://arxiv.org/abs/1902.06656.

[Die82] D. Dieks. Communication by EPR devices. *Physics Letters A*, 92(6): 271–272, 1982. DOI: 10.1016/0375-9601(82)90084-6.

[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.

[FM18] H. Fu and C. A. Miller. Local randomness: Examples and application. *Physical Review A*, 97(3): 032324, 2018. DOI: 10.1103/PhysRevA.97.032324.

[GMW91] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity for all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, 38(3): 690–728, 1991.
DOI: 10.1145/116825.116852.

[KRS09] R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory*, 55(9): 4337–4347, 2009.
DOI: 10.1109/TIT.2009.2025545.

[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.

[Par70] J. L. Park. The concept of transition in quantum mechanics. *Foundations of Physics*, 1(1): 23–33, 1970.
DOI: 10.1007/BF00708652.

[PLWC16] C. Pfister, N. Lütkenhaus, S. Wehner, and P. J. Coles. Sifting attacks in finite-size quantum key distribution. *New Journal of Physics*, 18(5): 053001, 2016.
DOI: 10.1088/1367-2630/18/5/053001.

[Rén61] A. Rényi. On measures of entropy and information. In *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability*, volume 1, pages 547–561, 1961.

[Ren05] R. Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 06(01): 1–127, 2005.
DOI: 10.1142/S0219749908003256.

[Ser74] R. J. Serfling. Probability inequalities for the sum in sampling without replacement. *The Annals of Statistics*, 2(1): 39–48, 1974.
DOI: 10.1214/aos/1176342611.

[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.

[TCR10] M. Tomamichel, R. Colbeck, and R. Renner. Duality between smooth min-and max-entropies. *IEEE Transactions on Information Theory*, 56(9): 4674–4681, 2010.
DOI: 10.1109/TIT.2010.2054130.

[The16] The European Parliament and the Council of the European Union. Regulation (EU) 2016/679. *Official Journal of the European Union*, L 119: 1–88, 2016.
Online: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[TL17] M. Tomamichel and A. Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1: 14, 2017.
DOI: 10.22331/q-2017-07-14-14.

[TLGR12] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3: 634, 2012.
DOI: 10.1038/ncomms1631.

[Tom12] M. Tomamichel. *A Framework for Non-Asymptotic Quantum Information Theory*. PhD thesis, ETH Zurich, 2012.
DOI: 10.3929/ethz-a-7356080.

[TR11] M. Tomamichel and R. Renner. Uncertainty relation for smooth entropies. *Physical Review Letters*, 106(11), 2011.
DOI: 10.1103/PhysRevLett.106.110506.

[Unr13] D. Unruh. Everlasting multi-party computation. In *Advances in Cryptology—CRYPTO 2013*, pages 380–397, 2013.
DOI: 10.1007/978-3-642-40084-1_22.

[Unr14] D. Unruh. Revocable quantum timed-release encryption. In *Advances in Cryptology—EUROCRYPT 2014*, pages 129–146, 2014.
DOI: 10.1007/978-3-642-55220-5_8.

[vLvdG12] J. H. van Lint and G. van der Geer. *Introduction to Coding Theory and Algebraic Geometry*. Birkhäuser Basel, 2012.
DOI: 10.1007/978-3-0348-9286-5.

[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/.

[WC81] M. N. Wegman and J. Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3): 265–279, 1981.
DOI: 10.1016/0022-0000(81)90033-7.

[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.