Quantum encryption with certified deletion

Anne Broadbent and Rabib Islam*

Abstract

Given a ciphertext, is it possible to prove the *deletion* of the underlying plaintext? Since classical ciphertexts can be copied, clearly such a feat is impossible using classical information alone. In stark contrast to this, we show that quantum encodings enable *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; the scheme is also robust against noise in these devices. Furthermore, we provide an analysis that is suitable in the finite-key regime.

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 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.

Quantum information, on the other hand, is known for its no-cloning principle [Die82, Par70, WZ82], which states that quantum states cannot, in general, be copied. 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 are achievable with unconditional security by means of quantum information. We give a formal definition

*University of Ottawa, Department of Mathematics and Statistics; {abroadbe,risla028}@uottawa.ca.

of certified deletion encryption and certified deletion security. Moreover, we construct an encryption scheme which, as we demonstrate, satisfies these notions (in addition, our proofs are applicable in the finite-key regime). 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.

1.1.1 Definitions

In order to define our notion of encryption, we build on the *quantum encryption of classical messages* (QECM) framework [BL20][1] (for simplicity, our work is restricted to the single-use, private-key setting). To the QECM, we add a *delete* circuit which is used by Bob if he wishes to delete his ciphertext and generate a corresponding verification state, and a *verify* circuit which uses the key 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 and Definition 3.5). Our definition is inspired by elements of the definition in [Unr14]. The starting point for this definition is the well-known indistinguishability experiment, this time 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 msg_0 to the challenger. Depending on a random bit b, the challenger either encrypts 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 classical "deletion certificate", y. Next, the key is sent to the adversary $\mathcal{A}_2$ who produces an output bit $b' \in \{0,1\}$.[2] A scheme is deemed *secure* if the choice of b does not change the probability of the following event: "$b' = 1$ *and* the deletion certificate y is accepted". We note that it would be incorrect to formulate a definition that conditions on y being accepted (see discussion in [Unr14]). We note that certified deletion security does not necessarily imply ciphertext indistinguishability; hence these two properties are defined and proven separately.

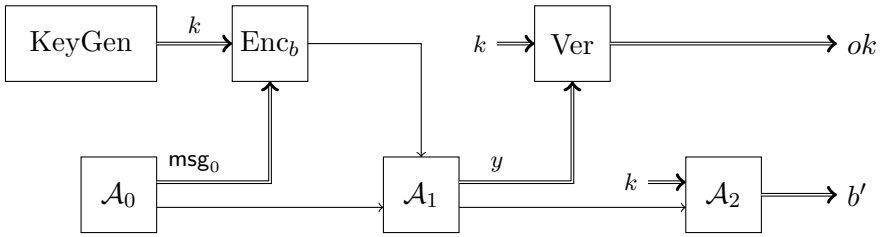

Figure 1: Schematic representation of the security notion for certified deletion security. The game is parametrized by $b \in \{0,1\}$ and Enc_0 outputs an encryption of 0^n while Enc_1 encrypts its input, msg_0. Security holds if for each adversary $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2)$, the probability of ($b' = 1$ *and* $ok = 1$) is essentially the same, regardless of the value of b.

[1] Apart from sharing this basic definition, our work differs significantly from [BL20]. For instance, the adversarial models are fundamentally different, since we consider here a single adversary, while [BL20] is secure against *two* separate adversaries.

[2] The key is leaked *after* y is produced; this is required because otherwise, with access to the ciphertext and the key, the adversary could (via purification) retrieve the plaintext without affecting the ciphertext, and therefore could decrypt while simultaneously producing a convincing proof of deletion.

1.1.2 Scheme

In Section 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 2.1). 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 classical *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 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. Intuitively speaking, the use of the hash function is required in order to prevent that *partial* information retained by Bob could be useful in distinguishing the plaintext, while 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.

1.1.3 Proof

In Section 5, we present the security analysis of our scheme and give concrete security parameters (Theorem 5.11 and its proof). First, the fact that the scheme is an encryption scheme is relatively straightforward; it follows via a generalization of the quantum one-time pad (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 3.5) to our concrete scheme (Scheme 4.1). This yields a "prepare-and-measure" security game (see Game 5.3). 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 5.4), the adversary, Bob, creates an initial entangled state, from which Alice derives (via measurements in a random basis θ of her choosing) the value of $r \in \{0,1\}^m$. We show that, without loss of generality, 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 θ, 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]. We consider the scenario of Eve preparing a tripartite state ρ_{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; meanwhile, Bob measures his qubits in the Hadamard basis to obtain Z'. We then have the relation:

$$H^{\epsilon}_{\min}(X \mid E) + H^{\epsilon}_{\max}(Z \mid Z') \geq n, \tag{1}$$

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 ϵ (for details, see Section 2.4).

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 and the Leftover Hashing Lemma of [Ren05] 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*[3]: in this case, the revocation process is fully quantum. Our main security definition (Definition 3.5) is closely related to the security definitions from this work. On the technical side, our work differs significantly since [Unr14] uses techniques related to CSS codes and quantum random oracles, whereas we use privacy amplification and uncertainty relations. Our work also considers the concept of "revocation" outside the context of timed-release encryption, and it is also a conceptual and technical improvement since it shows that a proof of deletion can be classical. 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 work 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. We note, however, that there are similarities between our scheme and the proposed scheme in [CW19], namely the use of conjugate coding, with the message encoded in one basis and the conjugate basis, to prove deletion.

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 ρ_{ABE}, measurement of a register B in a determined basis,

[3] Revocable timed-release encryption can be equivalently thought of as a revocable time-lock puzzle[RSW96], which does not satisfy standard cryptographic security (since the plaintexts are recoverable, by design, in polynomial time). In contrast, here we achieve a semantic-security-type security definition.

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 that 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 Applications and Open Questions

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. See also [GGV20]. 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. Future work could develop a type of homomorphic encryption with certified deletion so that the ciphertexts could be useful to some extent while a level of security, in terms of deletion, is maintained. Also useful would be a type of "public verifiability" which would enable parties other than the originator to verify deletion certificates. Contact tracing [CTV20] is another relevant scenario where individual data could be safeguarded against data retention by using certified deletion.

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 key is leaked in the future); such a functionality is unachievable with classical information alone, but it 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 percent 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 key is included in the ciphertext, but with the ciphertext encoded in a classical timed-release encryption.

Composable and Everlasting Security. We leave as an open question the composability of our scheme (as well as security beyond the one-time case). We note that through a combination of composability with our quantum encoding, it may be possible to transform a long-term computational assumption into a temporary one. That is, a computational assumption would need to be broken

during a protocol, or else the security would be information-theoretically secure as soon as the protocol ends. This is called *everlasting security* [Unr13].

For example, consider the situation encountered in a zero-knowledge proof system for a Σ-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 composable 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; this is highly desirable given steady progress in both algorithms and quantum computers. Another potential application would be proving erasure (in the context where there is no encryption) [CW19].

1.4 Outline

The remainder of this paper is structured as follows. Section 2 is an introduction to concepts and notation used in the rest of this work. Section 3 lays out the novel security definitions which appear in this paper. Section 4 is an exposition of our main scheme, while Section 5 provides a security analysis.

Acknowledgements

We would like to thank Carl Miller for related discussions. We are grateful to the anonymous reviewers for pointing out a mistake in a previous version of the security definition. This work was supported by the U.S. Air Force Office of Scientific Research under award number FA9550-17-1-0083, Canada's NSERC, an Ontario ERA, and the University of Ottawa's Research Chairs program.

2 Preliminaries

In this section, we outline certain concepts and notational conventions which are used throughout the article. We assume that the reader has a basic familiarity with quantum computation and quantum information. We refer to [NC00] for further background.

2.1 Notation

We make use of the following notation: for a function $f\colon X \to \mathbb{R}$, we denote

$$\mathop{\mathbb{E}}_{x} f(x) = \frac{1}{|X|} \sum_{x \in X} f(x). \tag{2}$$

We represent the Hamming weight of strings as the output of a Hamming weight function $\omega\colon \{0,1\}^* \to \mathbb{N}$. If $x_1, \ldots, x_n$ are strings, then we define $(x_1, \ldots, x_n)$ to be the concatenation of these strings. Let $[n]$ denote the set $\{1, 2, \ldots, n\}$. 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 string x restricted to the bits indexed by $\mathcal{I}$. We call a

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

We let $\mathcal{Q} \coloneqq \mathbb{C}^2$ denote the state space of a single qubit, and we use the notation $\mathcal{Q}(n) \coloneqq \mathcal{Q}^{\otimes n}$ for any $n \in \mathbb{N}$. Let $\mathcal{H}$ be a Hilbert space. The group of unitary operators on $\mathcal{H}$ is denoted by $\mathcal{U}(\mathcal{H})$, and the set of density operators on $\mathcal{H}$ is denoted by $\mathcal{D}(\mathcal{H})$. Through density operators, a Hilbert space may correspond to a *quantum system*, which we represent by capital letters. The set of diagonal density operators on $\mathcal{H}$ is denoted by $\mathfrak{D}(\mathcal{H})$—the elements of this set represent classical states. Discrete random variables are thus modeled as finite-dimensional quantum systems, called *registers*. A register X takes values in $\mathcal{X}$. A density operator $|x\rangle\langle x|$ will be denoted as $|x\rangle\langle x|$. We employ the operator norm, which we define for a linear operator $A\colon \mathcal{H} \to \mathcal{H}'$ between finite-dimensional Hilbert spaces $\mathcal{H}$ and $\mathcal{H}'$ as

$$\|A\| = \sup\{\|Av\| \mid v \in \mathcal{H}, \|v\| = 1\}. \tag{3}$$

Moreover, 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 semi-definite.

In order to illustrate correlations between a classical register X and a quantum state A, we use the formalism of a *classical-quantum* state:

$$\rho_{XA} = \sum_{x \in \mathcal{X}} P_X(x) \, |x\rangle\langle x|_X \otimes \rho_{A|X=x}, \tag{4}$$

where $P_X(x) \coloneqq \Pr[X = x]_\rho = \operatorname{Tr}[|x\rangle\langle x|_X \, \rho_{XA}]$ and $\rho_{A|X=x}$ is the state of A conditioned on the event that $X = x$.

Let $|x_i\rangle\langle x_i| \in \mathfrak{D}(\mathcal{H})$ be classical states for integers i such that $1 \leq i \leq n$. Then we use the notation

$$|x_1, x_2, \ldots, x_n\rangle\langle x_1, x_2, \ldots, x_n| \coloneqq |x_1\rangle\langle x_1| \otimes |x_2\rangle\langle x_2| \otimes \cdots \otimes |x_n\rangle\langle x_n| \,. \tag{5}$$

Let $\mathsf{H} \in \mathcal{U}(\mathcal{Q})$ denote the Hadamard operator, which is defined by

$$|0\rangle \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |1\rangle \mapsto \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{6}$$

For any strings $x, \theta \in \{0,1\}^n$, we define

$$\left|x^\theta\right\rangle = \mathsf{H}^\theta |x\rangle = \mathsf{H}^{\theta_1} |x_1\rangle \otimes \mathsf{H}^{\theta_2} |x_2\rangle \otimes \cdots \otimes \mathsf{H}^{\theta_n} |x_n\rangle \,. \tag{7}$$

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

We make use of the Einstein-Podolsky-Rosen (EPR) state [EPR35], defined as

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle). \tag{8}$$

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 fully mixed state which is, given a d-dimensional Hilbert space $\mathcal{H}$, defined as $\frac{1}{d} 1_d$, where 1_d denotes the identity matrix with d rows.

For two quantum states $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, we define the *trace distance*

$$\|\rho - \sigma\|_{\mathrm{Tr}} \coloneqq \frac{1}{2}\|\rho - \sigma\|. \tag{9}$$

Note also an alternative formula for the trace distance:

$$\|\rho - \sigma\|_{\mathrm{Tr}} = \max_P \operatorname{Tr}[P(\rho - \sigma)], \tag{10}$$

where $P \leq 1_d$ is a positive operator. Hence, in terms of a physical interpretation, the trace distance is the upper bound for the difference in probabilities with respect to the states ρ and σ that a measurement outcome P may occur on the state.

We define purified distance, which is a metric on quantum states.

Definition 2.1 (Purified Distance)**.** Let A be a quantum system. For two (subnormalized) states ρ_A, σ_A, we define the *generalized fidelity*,

$$F(\rho_A, \sigma_A) \coloneqq \left(\mathrm{Tr}\left[\sqrt{\sqrt{\rho_A}\sigma_A\sqrt{\rho_A}} \right] + \sqrt{1 - \mathrm{Tr}[\rho_A]}\sqrt{1 - \mathrm{Tr}[\sigma_A]} \right)^2, \tag{11}$$

and the *purified distance*,

$$P(\rho_A, \sigma_A) \coloneqq \sqrt{1 - F(\rho_A, \sigma_A)}. \tag{12}$$

2.2 Hash Functions and Error Correction

We make use of universal$_2$ hash functions, first introduced by Carter and Wegman [CW79].

Definition 2.2 (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. Therefore, 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: $\{0,1\}^n \to \{0,1\}^s$ and corr: $\{0,1\}^n \times \{0,1\}^s \to \{0,1\}^n$, 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.

2.3 Quantum Channels and Measurements

Let A and B be two quantum systems, and let X be a classical register. A *quantum channel* $\Phi \colon A \to B$ is a completely positive trace-preserving (CPTP) map. A *generalized measurement* on A is a set of linear operators $\{M_A^x\}_{x \in \mathcal{X}}$, where $x \in \mathcal{X}$ are potential classical outcomes, such that

$$\sum_{x \in \mathcal{X}} (M_A^x)^\dagger (M_A^x) = 1_A. \tag{13}$$

A *positive-operator valued measure* (POVM) on A is a set of Hermitian positive semidefinite operators $\{M_A^x\}_{x \in \mathcal{X}}$, where $x \in \mathcal{X}$ are potential classical outcomes, such that

$$\sum_{x \in \mathcal{X}} (M_A^x) = 1_A. \tag{14}$$

We also represent measurements with CPTP maps such as $\mathcal{M}_{A\to X}$, which map quantum states in system A to classical states in register X using POVMs.

For two registers X and Y, if we have a function, $f\colon \mathcal{X} \to \mathcal{Y}$ then we denote by $\mathcal{E}_f\colon X \to XY$ the CPTP map

$$\mathcal{E}_f[\cdot] \coloneqq \sum_{x\in X} |f(x)\rangle_Y |x\rangle\langle x|_X \cdot |x\rangle\langle x|_X \langle f(x)|_Y . \tag{15}$$

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

$$c(\{M_A^x\}_x, \{N_B^y\}_y) \coloneqq \max_{x,y} \left\| \sqrt{M_A^x}\sqrt{N_A^y} \right\|_\infty^2 . \tag{16}$$

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

$$c_i \coloneqq c\left(\{M_{A_i}^{0,x}\}_x, \{M_{A_i}^{1,y}\}_y\right). \tag{17}$$

We assume our measurements are ideal, so $c_i = 1/2$.

2.4 Entropic 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 a generalization of conditional Rényi entropies [Rén61] to the quantum setting. Min-entropy, for instance, quantifies the degree of uniformity of the distribution of a random variable.

Definition 2.3 (Min-entropy)**.** Let A and B be two quantum systems. For any bipartite state ρ_{AB}, we define

$$H_{\min}(A \mid B)_\rho \coloneqq \sup\{\xi \in \mathbb{R} \mid \exists \text{ state } \sigma_B \text{ such that } \rho_{AB} \le 2^{-\xi} 1_A \otimes \sigma_B\}. \tag{18}$$

Max-entropy quantifies the size of the support of a random variable, and is here defined by its dual relation to min-entropy.

Definition 2.4 (Max-entropy)**.** Let A and B be two quantum systems. For any bipartite state ρ_{AB}, we define

$$H_{\max}(A \mid B)_\rho \coloneqq -H_{\min}(A \mid C)_\rho, \tag{19}$$

where ρ_{ABC} is any pure state with $\mathrm{Tr}_C[\rho_{ABC}] = \rho_{AB}$, for some quantum system C.

In order to deal with finite-size effects, it is necessary to generalize min- and max-entropy to their smooth variants.

Definition 2.5 (Smooth Entropies)**.** Let A and B be two quantum systems. For any bipartite state ρ_{AB}, and $\epsilon \in \left[0, \sqrt{\mathrm{Tr}[\rho_{AB}]}\right)$, we define

$$H_{\min}^{\epsilon}(A \mid B)_{\rho} \coloneqq \sup_{\substack{\tilde{\rho}_{AB} \\ P(\tilde{\rho}_{AB}, \rho_{AB}) \leq \epsilon}} H_{\min}(A \mid B)_{\tilde{\rho}}, \tag{20}$$

$$H_{\max}^{\epsilon}(A \mid B)_{\rho} \coloneqq \inf_{\substack{\tilde{\rho}_{AB} \\ P(\tilde{\rho}_{AB}, \rho_{AB}) \leq \epsilon}} H_{\max}(A \mid B)_{\tilde{\rho}}. \tag{21}$$

It is of note that smooth entropies satisfy the following inequality, commonly referred to as the data-processing inequality [TCR10].

Proposition 2.6. *Let $\epsilon \geq 0$, ρ_{AB} be a quantum state, and $\mathcal{E}\colon \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_C)$ be a CPTP map. Define $\sigma_{AC} \coloneqq (1_{\mathcal{D}(\mathcal{H}_A)} \otimes \mathcal{E})(\rho_{AB})$. Then,*

$$H_{\min}^{\epsilon}(A \mid B)_{\rho} \leq H_{\min}^{\epsilon}(A \mid C)_{\sigma} \quad \textit{and} \quad H_{\max}^{\epsilon}(A \mid B)_{\rho} \leq H_{\max}^{\epsilon}(A \mid C)_{\sigma}. \tag{22}$$

We use one half of the generalized uncertainty relation theorem found in [Tom12], the precursor of which was introduced by Tomamichel and Renner [TR11]. The original uncertainty relation was 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].

Proposition 2.7. *Let $\epsilon \geq 0$, let ρ_{ACE} 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, and let $\{P_A^k\}_{k \in \mathcal{K}}$ be a projective measurement acting on A. Then the post-measurement states*

$$\rho_{XKC} = \sum_{x,k} \langle x|x\rangle \otimes \langle k|k\rangle \otimes \mathrm{Tr}_{AE}\left[\sqrt{M_A^x} P_A^k \rho_{ACE} P_A^k \sqrt{M_A^x}\right] \tag{23}$$

and

$$\rho_{YKE} = \sum_{y,k} \langle y|y\rangle \otimes \langle k|k\rangle \otimes \mathrm{Tr}_{AC}\left[\sqrt{N_A^y} P_A^k \rho_{ACE} P_A^k \sqrt{N_A^y}\right] \tag{24}$$

satisfy

$$H_{\min}^{\epsilon}(X \mid KC)_{\rho} + H_{\max}^{\epsilon}(Y \mid KE)_{\rho} \geq \log \frac{1}{c_{\mathcal{K}}} \tag{25}$$

where $c_{\mathcal{K}} = \max_{k,x,y} \left\| \sqrt{M_A^x} P^k \sqrt{N_A^y} \right\|_{\infty}$.

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].

Proposition 2.8. *Let $\epsilon \geq 0$ and σ_{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,*

$$\|\zeta_{AYS^H} - \chi_Y \otimes \zeta_{AS^H}\|_{\mathrm{Tr}} \leq \frac{1}{2} 2^{-\frac{1}{2}(H_{\min}^{\epsilon}(X|A)_{\sigma} - n)} + 2\epsilon. \tag{26}$$

2.5 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 2.9. *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 $\delta \in (0,1)$,*

$$\Pr\left[\sum_{i\in\mathcal{I}} Z_i \leq k\delta \wedge \sum_{i\in\bar{\mathcal{I}}} Z_i \geq s(\delta+\nu)\right] \leq \exp\left(\frac{-2\nu^2 sk^2}{m(k+1)}\right). \tag{27}$$

It will also be useful to condition a quantum state on future events. 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 2.10. *Let ρ_{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 $P(\rho_{AX}, \tilde{\rho}_{AX}) \leq \sqrt{\epsilon}$.*

2.6 Quantum Encryption and Security

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

Considering that the scheme introduced in this paper is an encryption scheme with a quantum ciphertext, we rely on the "quantum encryption of classical messages" framework developed by Broadbent and Lord [BL20]. This framework describes an encryption scheme as a set of parameterized CPTP maps which satisfy certain conditions.

Definition 2.11 (Quantum Encryption of Classical Messages)**.** Let n be an integer. An *n-quantum encryption of classical messages* (n-QECM) is a tuple of uniform efficient quantum circuits $\mathcal{S} = (\mathsf{key}, \mathsf{enc}, \mathsf{dec})$ implementing CPTP maps 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

$$\mathrm{Tr}\Big[|k\rangle\langle k|\, \Phi^{\mathsf{key}}(1)\Big] > 0 \Rightarrow \mathrm{Tr}\Big[|m\rangle\langle m|\, \Phi_k^{\mathsf{dec}} \circ \Phi_k^{\mathsf{enc}}\, |m\rangle\langle m|\Big] = 1, \tag{28}$$

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

$$\rho \mapsto \Phi_k^{\mathsf{enc}}(|\mathbf{0}\rangle\langle\mathbf{0}|) \tag{29}$$

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

$$\rho \mapsto \sum_{m\in\{0,1\}^n} \mathrm{Tr}[|m\rangle\langle m|\, \rho] \cdot \Phi_k^{\mathsf{enc}}(|m\rangle\langle m|). \tag{30}$$

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 ciphertext indistinguishability (called indistinguishable security in [BL20]). It is best understood in terms of a scheme's resilience to an adversary performing what we refer to as a distinguishing attack.

Definition 2.12 (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 CPTP maps 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 $s\colon \mathbb{N}^+ \to \mathbb{N}^+$.

Definition 2.13 (Ciphertext Indistinguishability)**.** Let $\mathcal{S} = (\mathsf{key}, \mathsf{enc}, \mathsf{dec})$ be an n-QECM. Then we say that $\mathcal{S}$ has *ciphertext indistinguishability* if for all distinguishing attacks $\mathcal{A}$ there exists a negligible function η such that

$$\mathop{\mathbb{E}}_{b} \mathop{\mathbb{E}}_{k \leftarrow \mathcal{K}} \operatorname{Tr}\left[|b\rangle\langle b|\, A_{1,\lambda} \circ (\Phi^{\mathsf{enc}}_{k,b} \otimes \mathbb{1}_S) \circ A_{0,\lambda}(1)\right] \leq \frac{1}{2} + \eta(\lambda) \tag{31}$$

where λ 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

$$\Pr[\mathcal{K}_\lambda = k] = \operatorname{Tr}\Big[|k\rangle\langle k|\, \Phi^{\mathsf{key}}_\lambda(1)\Big]. \tag{32}$$

3 Security Definitions

In this section, 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.

Definition 3.1 (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 CPTP map of the form

$$\Phi^{\widehat{\mathsf{dec}}}_\lambda\colon \mathcal{D}(\mathcal{H}_{K,\lambda} \otimes \mathcal{H}_{T,\lambda}) \to \mathcal{D}(\mathcal{H}_M \otimes \mathcal{Q}). \tag{33}$$

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

$$\operatorname{Tr}\Big[|k\rangle\langle k|\, \Phi^{\mathsf{key}}(1)\Big] > 0 \Rightarrow \operatorname{Tr}\Big[|m\rangle\langle m| \otimes |1\rangle\langle 1|\, \Phi^{\widehat{\mathsf{dec}}}_k \circ \Phi^{\mathsf{enc}}_k\, |m\rangle\langle m|\Big] = 1, \tag{34}$$

where λ is implicit, Φ^{enc}_k is the CPTP map defined by $\rho \mapsto \Phi^{\mathsf{enc}}(|k\rangle\langle k| \otimes \rho)$, and we define Φ^{dec}_k 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 paper, we henceforth note that all further references to the QECM framework are in fact references to the AQECM framework.

Definition 3.2 (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 ϵ-*robust* if, for all adversaries $\mathcal{A}$ implementing CPTP maps of the form

$$A\colon \mathcal{D}(\mathcal{H}_{T,\lambda}) \to \mathcal{D}(\mathcal{H}_{T,\lambda}), \tag{35}$$

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

$$\mathop{\mathbb{E}}_{k\leftarrow\mathcal{K}} \mathrm{Tr}\Big[\big|m'\big\rangle\big\langle m'\big| \otimes |1\rangle\langle 1|\, \Phi_k^{\mathsf{dec}} \circ A \circ \Phi_k^{\mathsf{enc}} |m\rangle\langle m|\Big] \leq \epsilon. \tag{36}$$

In other words, a QECM is ϵ-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 ϵ. This is functionally equivalent to a one-time quantum authentication scheme, where messages are classical (see *e.g.* [BCG+02, GYZ17, DNS12]).

Our description takes the form of an augmentation of the QECM framework described in Definition 3.1. 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 3.3 (Certified Deletion Encryption)**.** Let $\mathcal{S} = (\mathsf{key}, \mathsf{enc}, \mathsf{dec})$ be an n-QECM such that Let del and ver be efficient quantum circuits implemented by CPTP maps 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

$$\mathrm{Tr}\Big[|k\rangle\langle k|\, \Phi^{\mathsf{key}}(1)\Big] > 0 \implies \mathrm{Tr}\Big[|1\rangle\langle 1|\, \Phi^{\mathsf{ver}} \circ \Big(|k\rangle\langle k| \otimes \Big(\Phi^{\mathsf{del}} \circ \Phi_k^{\mathsf{enc}} |m\rangle\langle m|\Big)\Big)\Big] = 1 \tag{37}$$

where λ 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 3.4 (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 CPTP maps 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 1.1.1 for an informal explanation of the definition, and we recall that notation $\Phi_{k,b}^{\mathsf{enc}}$ is defined in Eq. (29).

$M_A^{\theta,x}$	Measurement operator acting on system A with setting θ 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^Θ, and outcome stored in register X
λ	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
θ	Basis in which the encrypting party prepares her quantum state
δ	Threshold error rate for the verification test
Θ	Set of possible bases from which θ 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_{pa}	Hash function used in the privacy amplification scheme
H_{ec}	Hash function used in the error correction scheme
S^Θ	Seed for the choice of θ
$S^{H_{\text{pa}}}$	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 1: Overview of nomenclature used in Section 4 and Section 5

Definition 3.5 (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 CPTP map $\Phi_k^{\mathsf{ver}}\colon \mathcal{D}(\mathcal{H}_{K,\lambda}\ otimes \mathcal{H}_{D,\lambda}) \to \mathcal{D}(\mathcal{Q} \otimes \mathcal{H}_{K,\lambda})$ by

$$\rho \mapsto \Phi^{\mathsf{ver}}(|k\rangle\langle k| \otimes \rho) \otimes |k\rangle\langle k|\,. \tag{38}$$

Let $b \in \{0,1\}$, let $\mathcal{A}$ be a certified deletion attack, and let

$$p_b = \big[\,\mathbb{E}_{k\leftarrow\mathcal{K}} \operatorname{Tr}\big[(|1,1\rangle\langle 1,1|)(\mathbb{1} \otimes A_2) \circ (\Phi_k^{\mathsf{ver}} \otimes \mathbb{1}_{ST'}) \circ A_1 \circ (\Phi_{k,b}^{\mathsf{enc}} \otimes \mathbb{1}_S) \circ A_0(1)\big], \tag{39}$$

where λ is implicit, and where $\mathcal{K}_\lambda$ is the random variable distributed on $\{0,1\}^{\kappa(\lambda)}$ such that

$$\Pr[\mathcal{K}_\lambda = k] = \operatorname{Tr}\Big[|k\rangle\langle k|\,\Phi_\lambda^{\mathsf{key}}(1)\Big]. \tag{40}$$

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

$$|p_0 - p_1| \leq \eta(\lambda). \tag{41}$$

4 Constructing an Encryption Scheme with Certified Deletion

Scheme 4.1 aims to exhibit a noise-tolerant prepare-and-measure n-CDE with ciphertext indistinguishability and certified deletion security.

Scheme 4.1 (Prepare-and-Measure Certified Deletion)**.** Let $n, \lambda, \tau, \mu, m = s + k$ be integers. Let $\Theta = \{\theta \in \{0,1\}^m \mid \omega(\theta) = k\}$. Let both $\mathfrak{H}_{\text{ec}} := \{h\colon \{0,1\}^s \to \{0,1\}^\tau\}$ and $\mathfrak{H}_{\text{pa}} := \{h\colon \{0,1\}^s \to \{0,1\}^n\}$ be universal$_2$ families of hash functions. Let synd$\colon \{0,1\}^n \to \{0,1\}^\mu$ be an error syndrome

function, let corr: $\{0,1\}^n \times \{0,1\}^\mu \to \{0,1\}^n$ 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 Equation (37). It is therefore an n-CDE.

Circuit 1: The key generation circuit key.

Input : None.

Output : A key state $\rho \in \mathcal{D}(\mathcal{Q}(k+m+n+\mu+\tau) \otimes \mathfrak{H}_{\text{pa}} \otimes \mathfrak{H}_{\text{ec}}))$.

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

2 Sample $r|_{\bar{\mathcal{I}}} \xleftarrow{\$} \{0,1\}^k$ where $\bar{\mathcal{I}} = \{i \in [m] \mid \theta_i = 1\}$.

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 $\rho = |r|_{\bar{\mathcal{I}}}, \theta, u, d, e, H_{\text{pa}}, H_{\text{ec}}\rangle\langle r|_{\bar{\mathcal{I}}}, \theta, u, d, e, H_{\text{pa}}, H_{\text{ec}}|$.

Circuit 2: The encryption circuit enc.

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

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

1 Sample $r|_{\mathcal{I}} \xleftarrow{\$} \{0,1\}^s$ where $\mathcal{I} = \{i \in [m] \mid \theta_i = 0\}$.

2 Compute $x = H_{\text{pa}}(r|_{\mathcal{I}})$ where $\mathcal{I} = \{i \in [m] \mid \theta_i = 0\}$.

3 Compute $p = H_{\text{ec}}(r|_{\mathcal{I}}) \oplus d$.

4 Compute $q = \text{synd}(r|_{\mathcal{I}}) \oplus e$.

5 Output $\rho = \left|r^\theta\right\rangle\!\left\langle r^\theta\right| \otimes |\mathsf{msg} \oplus x \oplus u, p, q\rangle\langle\mathsf{msg} \oplus x \oplus u, p, q|$.

5 Security Analysis

In this section, we present the security analysis for Scheme 4.1: 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 Ciphertext Indistinguishability

In considering whether Scheme 4.1 has ciphertext indistinguishability (Definition 2.13), 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. *Scheme 4.1 has ciphertext indistinguishability.*

Circuit 3: The decryption circuit dec.

Input : A key state
$|r|_{\bar{\mathcal{I}}}, \theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}\rangle\langle r|_{\bar{\mathcal{I}}}, \theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}| \in \mathcal{D}(\mathcal{Q}(k+m+n+\mu+\tau) \otimes \mathfrak{H}_{\mathrm{pa}} \otimes \mathfrak{H}_{\mathrm{ec}})$
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 ρ' 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 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 ρ in the Hadamard basis. Call the output y.
2 Output $\sigma = |y\rangle\langle y|$.

Circuit 5: The verification circuit ver.

Input : A key state
$|r|_{\bar{\mathcal{I}}}, \theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}\rangle\langle r|_{\bar{\mathcal{I}}}, \theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}| \in \mathcal{D}(\mathcal{Q}(k+m+n+\mu+\tau) \otimes \mathfrak{H}_{\mathrm{pa}} \otimes \mathfrak{H}_{\mathrm{ec}})$
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.

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

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

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 ciphertext indistinguishability 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 Δ 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 4.1 ensure that errors in decryption are detected with high probability. In other words, we show that the scheme is ϵ_{rob}-robust, where $\epsilon_{\text{rob}} \coloneqq \frac{1}{2^\tau}$.

Recall that τ is the length of the error correction hash, and that μ 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 key $(r|_{\bar{\mathcal{I}}}, \theta, u, d, e, H_{\text{pa}}, H_{\text{ec}}) \in \Theta \times \{0,1\}^{n+\mu+\tau} \times \mathfrak{H}_{\text{pa}} \times \mathfrak{H}_{\text{ec}}$. Given θ, Bob learns $\mathcal{I}$. This allows him to perform the following measurement on ρ_B:

$$\mathcal{M}^{\mathcal{I}}_{B\to Y}(\cdot) = \sum_{y \in \{0,1\}^s} |y\rangle_Y \left(M^{0,y}_{B_{\mathcal{I}}}\right) \cdot \left(M^{0,y}_{B_{\mathcal{I}}}\right)^\dagger \langle y|_Y \tag{42}$$

The new register Y contains a hypothesis of the random string Alice used in generating c. Since ρ_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 ec: $\{0,1\}^s \times \{0,1\}^\mu \times \mathfrak{H}_{\text{ec}} \to \{0,1\}$ defined by

$$\text{ec}(x, y) = \begin{cases} 0 & \text{if } H_{\text{ec}}(x) \neq y \\ 1 & \text{else.} \end{cases} \tag{43}$$

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. *If $r|_{\mathcal{I}} \in \{0,1\}^m$ is the random string Alice samples in encryption, and $\hat{x} = \text{corr}(y, q \oplus e)$, then*

$$\Pr[H_{pa}(r|_{\mathcal{I}}) \neq H_{pa}(\hat{x}) \wedge F^{ec} = 1] \leq \frac{1}{2^\tau}. \tag{44}$$

Proof.

$$\begin{aligned}
\Pr[H_{\mathrm{pa}}(r|_{\mathcal{I}}) \neq H_{\mathrm{pa}}(\hat{x}) \wedge F^{\mathrm{ec}} = 1] &= \Pr[H_{\mathrm{pa}}(r|_{\mathcal{I}}) \neq H_{\mathrm{pa}}(\hat{x}) \wedge H_{\mathrm{ec}}(p \oplus d) = H_{\mathrm{ec}}(\hat{x})] && (45)\\
&= \Pr[H_{\mathrm{pa}}(r|_{\mathcal{I}}) \neq H_{\mathrm{pa}}(\hat{x}) \wedge H_{\mathrm{ec}}(r|_{\mathcal{I}}) = H_{\mathrm{ec}}(\hat{x})] && (46)\\
&\leq \Pr[r|_{\mathcal{I}} \neq \hat{x} \wedge H_{\mathrm{ec}}(r|_{\mathcal{I}}) = H_{\mathrm{ec}}(\hat{x})] && (47)\\
&= \Pr[r|_{\mathcal{I}} \neq \hat{x}] \Pr[H_{\mathrm{ec}}(r|_{\mathcal{I}}) = H_{\mathrm{ec}}(\hat{x})] && (48)\\
&\leq \Pr[H_{\mathrm{ec}}(r|_{\mathcal{I}}) = H_{\mathrm{ec}}(\hat{x}) \mid r|_{\mathcal{I}} \neq \hat{x}] && (49)\\
&\leq \frac{1}{\|\mathfrak{H}_{\mathrm{ec}}\|} && (50)\\
&= \frac{1}{2^{\tau}}. && \square
\end{aligned}$$

5.3 Certified Deletion Security

We now prove certified deletion security of Scheme 4.1. Our technique consists in formalizing a game (Game 5.3) that corresponds to the security definition (Definition 3.5) applied to Scheme 4.1. Next, we develop an entanglement-based sequence of interactions (Game 5.4) which accomplish the same task as in the previous Game. We analyze this game and afterwards we show formally that the aforementioned analysis, via its relation to Game 5.3, implies the certified deletion security of Scheme 4.1. To begin, we describe a game which exhibits a certified deletion attack on Scheme 4.1, 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 and send the message (Alice), and the adversary $\mathcal{A}$ represents the recipient (Bob). 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 msg_0; security holds if, for any adversary, the probabilities of the following two events are negligibly close:

- verification passes *and* Bob outputs 1, in the case that Alice encrypted 0^n;
- verification passes *and* Bob output 1, in the case that Alice encrypted msg_0.

Game 5.3 (Prepare-and-Measure Game)**.** Let $\mathcal{S} = (\mathsf{key}, \mathsf{enc}, \mathsf{dec}, \mathsf{del}, \mathsf{ver})$ be an n-CDE with λ implicit, and with circuits defined as in Scheme 4.1. Let $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2)$ be a certified deletion attack. The game is parametric in $b \xleftarrow{\$} \{0,1\}$ and is called Game 5.3(b)..

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

$$|\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}, r|_{\bar{\mathcal{I}}}\rangle\langle\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}, r|_{\bar{\mathcal{I}}}|_K \leftarrow \Phi^{\mathsf{key}}. \tag{51}$$

Denote

$$\mathsf{msg} \coloneqq \begin{cases} 0^n & \text{if } b = 0 \\ \mathsf{msg}_0 & \text{if } b = 1. \end{cases} \tag{52}$$

Compute

$$\begin{aligned}
&\left|r^{\theta}\right\rangle\!\left\langle r^{\theta}\right|_T \otimes |\mathsf{msg} \oplus x \oplus u, p, q\rangle\langle\mathsf{msg} \oplus x \oplus u, p, q|_T \\
&\qquad \leftarrow \Phi^{\mathsf{enc}}(|\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}, r|_{\bar{\mathcal{I}}}\rangle\langle\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}, r|_{\bar{\mathcal{I}}}|_K \otimes |\mathsf{msg}\rangle\langle\mathsf{msg}|_M).
\end{aligned} \tag{53}$$

2. Run

$$|y\rangle\langle y|_D \otimes \rho'_S \otimes \rho_{T'} \leftarrow A_1(\left|r^\theta\right\rangle\left\langle r^\theta\right|_T \otimes |\mathsf{msg} \oplus x \oplus u, p, q\rangle\langle \mathsf{msg} \oplus x \oplus u, p, q|_T \otimes \rho_S). \tag{54}$$

Compute

$$\Gamma(ok) \leftarrow \Phi^{\mathsf{ver}}(|\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}, r|_{\bar{\mathcal{I}}}\rangle\langle\theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}, r|_{\bar{\mathcal{I}}}|_K \otimes |y\rangle\langle y|_D). \tag{55}$$

3. If $ok = 1$, run

$$\left|b'\right\rangle\left\langle b'\right| \leftarrow A_2(|r|_{\bar{\mathcal{I}}}, \theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}\rangle\langle r|_{\bar{\mathcal{I}}}, \theta, u, d, e, H_{\mathrm{pa}}, H_{\mathrm{ec}}|_{K'} \otimes \rho'_S \otimes \rho_{T'}); \tag{56}$$

else, $b' := 0$.

Let p_b be the probability that the output of Game 5.3(b) is 1. Comparing Game 5.3 with Definition 3.5, we note that the former runs the adversary to the end only in the case that $ok = 1$, while the latter runs the adversary to the end in both cases. However, the obtained distribution for p_b is the same, since in Game 5.3, $p_b = 1$ whenever the adversary outputs 1 *and* $ok = 1$. Hence we wish to bound $|p_0 - p_1|$ in Game 5.3. Instead of directly analyzing Game 5.3, we analyze a game wherein the parties use entanglement; this allows us to express the game in a format that is conducive for the analysis that follows.

Game 5.4 (EPR Game)**.** Alice is the sender, and Bob is the recipient and adversary. The game is parametric in $b \xleftarrow{\$} \{0,1\}$ and is called Game 5.4(b).

1. Bob selects a string $\mathsf{msg}_0 \in \{0,1\}^n$ and sends 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 $\theta \xleftarrow{\$} \Theta$, $r|_{\bar{\mathcal{I}}} \xleftarrow{\$} \{0,1\}^k$, $u \xleftarrow{\$} \{0,1\}^n$, $d \xleftarrow{\$} \{0,1\}^\mu$, $e \xleftarrow{\$} \{0,1\}^\tau$, $H_{\mathrm{pa}} \xleftarrow{\$} \mathfrak{H}_{\mathrm{pa}}$, and $H_{\mathrm{ec}} \xleftarrow{\$} \mathfrak{H}_{\mathrm{ec}}$. She applies a CPTP map 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 $x = H_{\mathrm{pa}}(r|_{\mathcal{I}}), p = H_{\mathrm{ec}}(r|_{\mathcal{I}}) \oplus d$, and $q = \mathrm{synd}(r|_{\mathcal{I}}) \oplus e$. Alice selects a message:

$$\mathsf{msg} := \begin{cases} 0^n & \text{if } b = 0 \\ \mathsf{msg}_0 & \text{if } b = 1. \end{cases} \tag{57}$$

If $\omega(y \oplus r|_{\bar{\mathcal{I}}}) < k\delta$, $ok := 1$ and Alice sends

$$(\mathsf{msg} \oplus x \oplus u, r|_{\bar{\mathcal{I}}}, \theta, u, d, e, p, q, H_{\mathrm{pa}}, H_{\mathrm{ec}}) \tag{58}$$

to Bob. Else, $ok := 0$ and $b := 0$.

3. If $ok = 1$, Bob computes

$$\left|b'\right\rangle\left\langle b'\right| \leftarrow \mathcal{E}(\rho_{B'} \otimes |\mathsf{msg} \oplus x \oplus u, \mathsf{msg}_0, r_{\bar{\mathcal{I}}}, \theta, u, d, e, p, q, H_{\mathrm{pa}}, H_{\mathrm{ec}}\rangle\langle \mathsf{msg} \oplus x \oplus u, \mathsf{msg}_0, r_{\bar{\mathcal{I}}}, \theta, u, d, e, p, q, H_{\mathrm{pa}}, H_{\mathrm{ec}}|) \tag{59}$$

for some CPTP map $\mathcal{E}$; else $b' := 0$.

Game 5.4 is intended to model a purified version of Game 5.3. Note that Bob's measuremement of B in the Hadamard basis is meant to mimic the del circuit of Scheme 4.1. 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 has more information when producing the deletion string than Bob in Game 5.4. This, however, is not true, as the adversary in Game 5.3 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 5.4.

Bob's measurements. Measurement of Bob's system B of m qubits in Step 1 is represented using two CPTP maps: 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 θ, 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.

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

$$\mathcal{M}^{\mathcal{I}}_{B\to Y}(\cdot) = \sum_{y\in\{0,1\}^s} |y\rangle_Y \left(M^{1,y}_{B_{\mathcal{I}}}\right)\cdot\left(M^{1,y}_{B_{\mathcal{I}}}\right)^\dagger \langle y|_Y \tag{60}$$

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

$$\mathcal{M}^{\bar{\mathcal{I}}}_{B\to W}(\cdot) = \sum_{w\in\{0,1\}^k} |w\rangle_W \left(M^{1,w}_{B_{\bar{\mathcal{I}}}}\right)\cdot\left(M^{1,w}_{B_{\bar{\mathcal{I}}}}\right)^\dagger \langle w|_W\,, \tag{61}$$

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

$$\rho_{S^\Theta} = \frac{1}{\binom{m}{k}} \sum_{\theta\in\Theta} |\theta\rangle\langle\theta|_{S^\Theta}\,. \tag{62}$$

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

$$\rho_{S^{H_{\mathrm{pa}}}} = \frac{1}{|\mathfrak{H}_{\mathrm{pa}}|} \sum_{h\in\mathfrak{H}_{\mathrm{pa}}} |h\rangle\langle h|_{S^{H_{\mathrm{pa}}}}\,. \tag{63}$$

Recall that $m = s + k$, where k is the weight of all strings in Θ. Measurement of Alice's system A of m qubits in Step 2 is represented using two CPTP maps: 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

$$\mathcal{M}_{AB\to VWXY|S^\Theta} = \mathcal{M}^{\mathcal{I}}_{A\to X|S^\Theta} \circ \mathcal{M}^{\bar{\mathcal{I}}}_{A\to V|S^\Theta} \circ \mathcal{M}^{\mathcal{I}}_{B\to Y} \circ \mathcal{M}^{\bar{\mathcal{I}}}_{B\to W}. \tag{64}$$

The overall post-measurement state is denoted σ_{VWXYS^Θ}. 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 comp: $\{0,1\}^k \times \{0,1\}^k \to \{0,1\}$ defined by

$$\mathrm{comp}(v,w) = \begin{cases} 0 & \text{if } \omega(v\oplus w) \geq k\delta \\ 1 & \text{else.} \end{cases} \tag{65}$$

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

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 2.7.

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 $\tau_{ABVWS^\Theta|F^{\mathrm{comp}}=1}$.

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 key, his knowledge about Alice's hypothetical Hadamard measurement outcome must be bounded below.

Proposition 5.5. *Let $\epsilon \geq 0$. Then*

$$H^\epsilon_{\min}(X \wedge F^{\mathrm{comp}} = 1|VWS^\Theta B')_\sigma + H^\epsilon_{\max}(Z \wedge F^{\mathrm{comp}} = 1|Y)_\sigma \geq s. \tag{66}$$

Proof. We apply Proposition 2.7 to the state $\tau_{ABVWS^\Theta|F^{\mathrm{comp}}=1}$. 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 $\mathcal{M}_{A\to Z|S^\Theta}$ as the POVMs and using $\{\langle\theta|\theta\rangle\}$ as the projective measurement, applying *Proposition* 2.7 yields

$$H^\epsilon_{\min}(X \wedge F^{\mathrm{comp}} = 1|VWS^\Theta B')_\sigma + H^\epsilon_{\max}(Z \wedge F^{\mathrm{comp}} = 1|S^\Theta B)_\tau \geq s. \tag{67}$$

We then apply the measurement map $\mathcal{M}_{B\to Y|S^\Theta}$ and discard S^Θ. Finally, by Proposition 2.6, we note that

$$H^\epsilon_{\max}(Z \wedge F^{\mathrm{comp}} = 1 \mid S^\Theta B)_\tau \leq H^\epsilon_{\max}(Z \wedge F^{\mathrm{comp}} = 1 \mid Y)_{\hat{\sigma}}, \tag{68}$$

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

$$\epsilon(\nu) \coloneqq \exp\left(\frac{-sk^2\nu^2}{m(k+1)}\right). \tag{69}$$

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

$$H_{\max}^{\epsilon(\nu)}(Z \wedge F^{\text{comp}} = 1 \mid Y)_{\hat{\sigma}} \leq s \cdot h(\delta + \nu) \tag{70}$$

where

$$h(x) \coloneqq -x \log x - (1-x)\log(1-x). \tag{71}$$

Proof. Define the event

$$\Omega \coloneqq \begin{cases} 1 & \text{if } \omega(Z \oplus Y) \geq s(\delta+\nu) \\ 0 & \text{else.} \end{cases} \tag{72}$$

Using Lemma 2.9, we get that

$$\begin{aligned} \Pr\left[F^{\text{comp}} = 1 \wedge \Omega\right]_{\hat{\sigma}} &= \Pr\left[\omega(V \oplus W) \leq k\delta \wedge \omega(Z \oplus Y) \geq s(\delta+\nu)\right]_\sigma && (73) \\ &\leq \epsilon(\nu)^2. && (74) \end{aligned}$$

Given the state $\hat{\sigma}_{ZYF^{\text{comp}}=1}$, we use Lemma 2.10 to remove the possibility of Ω and arrive at the smoothed state $\tilde{\sigma}_{ZYF^{\text{comp}}}$ with $\Pr[\Omega]_{\tilde{\sigma}} = 0$ and

$$P(\hat{\sigma}_{ZYF^{\text{comp}}=1}, \tilde{\sigma}_{ZYF^{\text{comp}}}) \leq \epsilon(\nu). \tag{75}$$

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

$$H_{\max}^{\epsilon(\nu)}(Z \wedge F^{\text{comp}} = 1 \mid Y)_{\hat{\sigma}} \leq H_{\max}(Z \wedge F^{\text{comp}} = 1 \mid Y)_{\tilde{\sigma}} = H_{\max}(Z \mid Y)_{\tilde{\sigma}}. \tag{76}$$

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

$$\begin{aligned} H_{\max}(Z \mid Y)_{\tilde{\sigma}} &= \log\left(\sum_{y \in \{0,1\}^s} \Pr[Y = y]_{\tilde{\sigma}} 2^{H_{\max}(Z|Y)_{\tilde{\sigma}}}\right) && (77) \\ &\leq \max_{\substack{y \in \{0,1\}^s \\ \Pr[Y=y]_{\tilde{\sigma}} > 0}} H_{\max}(Z \mid Y = y)_{\tilde{\sigma}} && (78) \\ &\leq \max_{\substack{y \in \{0,1\}^s \\ \Pr[Y=y]_{\tilde{\sigma}} > 0}} \log\left|\{z \in \{0,1\}^s : \Pr[Z = z \mid Y = y]_{\tilde{\sigma}} > 0\}\right| && (79) \\ &= \max_{y \in \{0,1\}^s} \log\left|\{z \in \{0,1\}^s : \Pr[Z = z \wedge Y = y]_{\tilde{\sigma}} > 0\}\right|. && (80) \end{aligned}$$

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

$$\begin{aligned} \left|\{z \in \{0,1\}^s : \Pr[Z = z \wedge Y = y]_{\tilde{\sigma}} > 0\}\right| &\leq \left|\{z \in \{0,1\}^s : \omega(z \oplus y) < s(\delta+\nu)\}\right| && (81) \\ &= \sum_{\gamma=0}^{\lfloor s(\delta+\nu)\rfloor} \binom{s}{\gamma}. && (82) \end{aligned}$$

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 2.8, 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 5.7. *Let $\epsilon(\nu)$ be as defined in (69). Then for any $\nu \in (0, \frac{1}{2} - \delta]$ such that $\epsilon(\nu)^2 < \Pr[F^{\text{comp}} = 1]_\sigma$, we have*

$$\|\zeta_{\tilde{X}SF^{\text{comp}}E\wedge F^{\text{comp}}=1} - \chi_{\tilde{X}} \otimes \zeta_{SF^{\text{comp}}E\wedge F^{\text{comp}}=1}\|_{\text{Tr}} \leq \frac{1}{2} 2^{-\frac{1}{2}g(\nu)} + 2\epsilon(\nu), \tag{83}$$

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

Proof. By Proposition 5.6, we see that

$$H_{\max}^{\epsilon(\nu)}(Z \wedge F^{\text{comp}} = 1 \mid Y)_\sigma \leq s \cdot h(\delta + \nu). \tag{84}$$

Together, with Proposition 5.5, and taking $q = 1 - h(\delta + \nu)$, we get:

$$H_{\min}^{\epsilon}(X \wedge F^{\text{comp}} = 1 | VWS^\Theta B')_\sigma \geq sq. \tag{85}$$

Finally, applying Proposition 2.8, 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 $\Pr[F^{\text{comp}} = 1]_\zeta$. Hence, considering the inequality $\Pr[F^{\text{comp}} = 1]_\zeta \leq \epsilon(\nu)^2 \leq \epsilon(\nu)$ results in the proof of the following corollary.

Corollary 5.8. *For any $\nu \in (0, \frac{1}{2} - \delta]$, the following holds:*

$$\|\zeta_{\tilde{X}SF^{\text{comp}}E\wedge F^{\text{comp}}=1} - \chi_{\tilde{X}} \otimes \zeta_{SF^{\text{comp}}E\wedge F^{\text{comp}}=1}\|_{\text{Tr}} \leq \frac{1}{2}\sqrt{2^{-s(1-h(\delta+\nu))+n}} + 2\epsilon(\nu). \tag{86}$$

Finally, we would like to translate this into a statement about $|p_0 - p_1|$ in Game 5.4.

Corollary 5.9. *The difference of probabilities*

$$|\Pr[b' = 1 \wedge ok = 1 \mid \textit{Game } 5.4(0)] - \Pr[b' = 1 \wedge ok = 1 \mid \textit{Game } 5.4(1)]| \tag{87}$$

is negligible.

Proof. Let $\zeta^b_{\tilde{X}SF^{\text{comp}}E\wedge F^{\text{comp}}=1}$ be the state of $\zeta_{\tilde{X}SF^{\text{comp}}E\wedge F^{\text{comp}}=1}$ in the case that $b \in \{0, 1\}$ was selected at the beginning of Game 5.4. Note that the following trace distance is bounded above by a negligible function:

$$\begin{aligned}
&\|\zeta^0_{\tilde{X}SF^{\text{comp}}E\wedge F^{\text{comp}}=1} - \zeta^1{}_{\tilde{X}SF^{\text{comp}}E\wedge F^{\text{comp}}=1}\|_{\text{Tr}} && (88)\\
&\quad\leq \|\zeta^0_{\tilde{X}SF^{\text{comp}}E\wedge F^{\text{comp}}=1} - \chi_{\tilde{X}} \otimes \zeta_{SF^{\text{comp}}E\wedge F^{\text{comp}}=1}\|_{\text{Tr}} \\
&\quad\quad + \|\zeta^1_{\tilde{X}SF^{\text{comp}}E\wedge F^{\text{comp}}=1} - \chi_{\tilde{X}} \otimes \zeta_{SF^{\text{comp}}E\wedge F^{\text{comp}}=1}\|_{\text{Tr}} && (89)\\
&\quad\leq 2\left(\frac{1}{2}\sqrt{2^{-s(1-h(\delta+\nu))+n}} + 2\epsilon(\nu)\right). && (90)
\end{aligned}$$

Next, note the following equality:

$$\Pr\left[b' = 1 \wedge ok = 1 \mid \textit{Game } 5.4(b)\right] \tag{91}$$

$$= \sum_{\zeta} \mathrm{Tr}\left[\zeta_{\tilde{X}SF^{\mathrm{comp}}E\wedge F^{\mathrm{comp}}=1}\right] \Pr\left[b' = 1 \mid \textit{Game } 5.4(b)\right] \tag{92}$$

Hence,

$$\left|\Pr\left[b' = 1 \wedge ok = 1 \mid \textit{Game } 5.4(0)\right] - \Pr\left[b' = 1 \wedge ok = 1 \mid \textit{Game } 5.4(1)\right]\right| \tag{93}$$

$$\leq \sum_{\zeta} \mathrm{Tr}\left[\zeta_{\tilde{X}SF^{\mathrm{comp}}E\wedge F^{\mathrm{comp}}=1}\right] \|\zeta^0_{\tilde{X}SF^{\mathrm{comp}}E\wedge F^{\mathrm{comp}}=1} - \zeta^1_{\tilde{X}SF^{\mathrm{comp}}E\wedge F^{\mathrm{comp}}=1}\|_{\mathrm{Tr}} \tag{94}$$

$$\leq \sum_{\zeta} 2\,\mathrm{Tr}\left[\zeta_{\tilde{X}SF^{\mathrm{comp}}E\wedge F^{\mathrm{comp}}=1}\right] \left(\frac{1}{2}\sqrt{2^{-s(1-h(\delta+\nu))+n}} + 2\epsilon(\nu)\right) \tag{95}$$

$$= 2\left(\frac{1}{2}\sqrt{2^{-s(1-h(\delta+\nu))+n}} + 2\epsilon(\nu)\right). \tag{96}$$

The conclusion follows from convexity and the physical interpretation of the trace distance (see Section 2). In particular, the difference in probabilities of obtaining the measurement outcome $b' = 1$ given states ζ^0 and ζ^1 is bounded above by the aforementioned trace distance. □

5.4 Security Reduction

We now show that the security of Game 5.3 can be reduced to that of Game 5.4. In order to do so, we construct a sequence of games starting at Game 5.3 and ending at Game 5.4, and show that each transformation can only increase the advantage in distinguishing the case of $b = 0$ from the case of $b = 1$.

For a game G, let $\mathsf{Adv}(G) = |p_0 - p_1|$ be the *advantage*, as defined in Equation (41).

Proposition 5.10.

$$\mathsf{Adv}(\textit{Game } 5.3) \leq \mathsf{Adv}(\textit{Game } 5.4). \tag{97}$$

Proof. Let G be a game like Game 5.3 except that in G, we run

$$\mathcal{A}_1(\left|r^\theta\right\rangle\!\left\langle r^\theta\right|_T \otimes |\alpha_1, \alpha_2, \alpha_3\rangle\langle\alpha_1, \alpha_2, \alpha_3|_T \otimes \rho_S), \tag{98}$$

where $\alpha_1, \alpha_2, \alpha_3$ are uniformly random bit strings of the appropriate length. Verification is performed as usual, and if $ok = 1$, we run $\mathcal{A}_2$ on a state containing $r|_{\bar{\mathcal{I}}}, \theta, \mathsf{msg} \oplus x \oplus \alpha_1, H_{\mathrm{ec}}(r|_{\mathcal{I}}) \oplus \alpha_2, \mathrm{synd}(r|_{\mathcal{I}}) \oplus \alpha_3, H_{\mathrm{pa}}, H_{\mathrm{ec}}$ along with $\rho'_S \otimes \rho_{T'}$. By a change of variable, $\mathsf{Adv}(\textit{Game } 5.3) = \mathsf{Adv}(G)$.

Next, we obtain G' from G by defining a new adversary $\mathcal{A}'_1$ which is like $\mathcal{A}'_1$, but only receives part of register T. Thus we run

$$\mathcal{A}'_1(\left|r^\theta\right\rangle\!\left\langle r^\theta\right|_T \otimes \rho_S), \tag{99}$$

and to compensate, we directly give $\mathcal{A}'_2$ the information that was previously hidden by the α values: we run $\mathcal{A}'_2$ on a state containing $r|_{\bar{\mathcal{I}}}, \theta, \mathsf{msg} \oplus x, H_{\mathrm{ec}}(r|_{\mathcal{I}}), synd(r|_{\mathcal{I}}), H_{\mathrm{pa}}, H_{\mathrm{ec}}$ together with $\rho'_S \otimes \rho_{T'}$. Then $\mathsf{Adv}(G) \leq \mathsf{Adv}(G')$, since an adversary $\mathcal{A}'$ for G' can simulate any adversary $\mathcal{A}$ in G, and win with the same advantage. To do this, $\mathcal{A}'$ simply creates its own randomness for α_1, α_2 and α_3, and adjusts the input to $\mathcal{A}_2$ based on its own knowledge of $\mathsf{msg} \oplus x, H_{\mathrm{ec}}(r|_{\mathcal{I}})$ and $\mathrm{synd}(r|_{\mathcal{I}})$. Let G'' be a game like G' except that, in G'', instead of $\mathcal{A}'_1$ 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 $\mathcal{A}'_1$ is given B. System A is measured in basis θ yielding a string r, and $\mathcal{A}'_1$ then computes

$$|y\rangle\langle y|_D \otimes \rho'_S \otimes \rho_{T'} \leftarrow A'_1(\rho_B \otimes \rho_S). \tag{100}$$

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

$$|\psi_r\rangle = \left(\mathsf{H}^\theta |r\rangle\langle r| \mathsf{H}^\theta \otimes 1_m\right) |\mathrm{EPR}^m\rangle \tag{101}$$

$$= \left(\mathsf{H}^\theta \otimes 1_m\right) (|r\rangle\langle r| \otimes 1_m) \left(1_m \otimes \mathsf{H}^\theta\right) |\mathrm{EPR}^m\rangle \tag{102}$$

$$= \sum_{\tilde{r}\in\{0,1\}^m} \frac{1}{2^{m/2}} \left(\mathsf{H}^\theta |r\rangle\langle r| |\tilde{r}\rangle\right) \left(\mathsf{H}^\theta |\tilde{r}\rangle\right) \tag{103}$$

$$= \frac{1}{2^{m/2}} \left(\mathsf{H}^\theta |r\rangle\right) \left(\mathsf{H}^\theta |r\rangle\right) \tag{104}$$

$$= \frac{1}{2^{m/2}} \left|r^\theta\right\rangle \otimes \left|r^\theta\right\rangle, \tag{105}$$

which occurs with probability $\||\psi_r\rangle\|^2 = \frac{1}{2^m}$. Therefore, the advantage in G' is the same as the advantage in G''. 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 running $\mathcal{A}'_1$. Then the advantage is unchanged because the measurement and $\mathcal{A}_1$ act on distinct systems, and therefore commute. We note that G''' is like Game 5.4 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 the advantage, we get that $\mathsf{Adv}(G''') \leq \mathsf{Adv}(\textit{Game 5.4})$. This concludes the proof. □

Theorem 5.11. *Scheme 4.1 is certified deletion secure.*

Proof. Through a combination of Corollary 5.9 and Proposition 5.10, we arrive at the following inequality:

$$\left|\Pr\left[b' = 1 \wedge ok = 1 \mid \textit{Game 5.4}(0)\right] - \Pr\left[b' = 1 \wedge ok = 1 \mid \textit{Game 5.3}(1)\right]\right| \tag{106}$$

$$\leq 2\left(\frac{1}{2}\sqrt{2^{-s(1-h(\delta+\nu))+n}} + 2\epsilon(\nu)\right). \tag{107}$$

Since Game 5.3 is a certified deletion attack for Scheme 4.1, we see that Scheme 4.1 is η-certified deletion secure for

$$\eta(\lambda) = 2\left(\frac{1}{2}\sqrt{2^{-(s(\lambda))(1-h(\delta+\nu))+n}} + 2\exp\left(\frac{-(s(\lambda))(k(\lambda))^2\nu^2}{(m(\lambda))((k(\lambda))+1)}\right)\right), \tag{108}$$

which is negligible for large enough functions s, k. □

References

[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.

[BL20] A. Broadbent and S. Lord. Uncloneable quantum encryption via oracles. In *15th Conference on the Theory of Quantum Computation, Communication and Cryptography—TQC 2020*, pages 4:1–4:22, 2020.
DOI: 10.4230/LIPIcs.TQC.2020.4.

[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.

[CTV20] R. Canetti, A. Trachtenberg, and M. Varia. Anonymous collocation discovery: Harnessing privacy to tame the coronavirus, 2020. Available at https://arxiv.org/abs/2003.13670.

[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. In *IEEE International Symposium on Information Theory, ISIT 2019, Paris, France, July 7-12, 2019*, 2019.
DOI: 10.1109/ISIT.2019.8849661.

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

[DNS12] F. Dupuis, J. B. Nielsen, and L. Salvail. Actively secure two-party evaluation of any quantum operation. In *Advances in Cryptology—CRYPTO 2012*, pages 794–811, 2012.
DOI: 10.1007/978-3-642-32009-5_46.

[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.

[GGV20] S. Garg, S. Goldwasser, and P. N. Vasudevan. Formalizing data deletion in the context of the right to be forgotten. In *Advances in Cryptology—CRYPTO 2020*, pages 373–402, 2020.
DOI: 10.1007/978-3-030-45724-2_13.

[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.

[GYZ17] S. Garg, H. Yuen, and M. Zhandry. New security notions and feasibility results for authentication of quantum data. In *Advances in Cryptology—CRYPTO 2017*, volume 2, pages 342–371, 2017.
DOI: 10.1007/978-3-319-63715-0_12.

[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.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[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. Ltkenhaus, 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.

[RSW96] R. L. Rivest, A. Shamir, and D. A. Wagner. Time-lock puzzles and timed-release crypto. Technical Report Technical memo MIT/LCS/TR-684, MIT Laboratory for Computer Science, 1996. Revision 3/10/96.

[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.

[WC81] M. N. Wegman and J. L. 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.