Uncloneable Quantum Encryption via Oracles

Anne Broadbent
University of Ottawa
abroadbe@uottawa.ca

Sébastien Lord
University of Ottawa
slord050@uottawa.ca

Abstract

Quantum information is well-known to achieve cryptographic feats that are unattainable using classical information alone. Here, we add to this repertoire by introducing a new cryptographic functionality called *uncloneable encryption*. This functionality allows the encryption of a classical message such that two collaborating but isolated adversaries are prevented from simultaneously recovering the message, even when the encryption key is revealed. Clearly, such functionality is unattainable using classical information alone.

We formally define uncloneable encryption, and show how to achieve it using Wiesner's conjugate coding, combined with a quantum-secure pseudorandom function (qPRF). Modelling the qPRF as an oracle, we show security by adapting techniques from the quantum one-way-to-hiding lemma, as well as using bounds from quantum monogamy-of-entanglement games.

1 Introduction

One of the key distinctions between classical and quantum information is given by the *no-cloning principle*: unlike bits, arbitrary qubits cannot be perfectly copied [Par70, WZ82, Die82]. This principle is the basis of many of the feats of quantum cryptography, including quantum money [Wie83] and quantum key distribution (QKD) [BB84] (for a survey on quantum cryptography, see [BS16]).

In QKD, two parties establish a shared secret key, using public quantum communication combined with an authentic classical channel. The quantum communication allows to *detect* eavesdropping: when the parties detect only a small amount of eavesdropping, they can produce a shared string that is essentially guaranteed to be private. Gottesman [Got03] studied *quantum tamper-detection* in the case of *encryption schemes*: in this work, a classical message is encrypted into a quantum ciphertext such that, at decryption time, the receiver will *detect* if an adversary could have information about the plaintext when the key is revealed. We note that classical information alone cannot produce such encryption schemes, since it is always possible to perfectly *copy* ciphertexts.

Notably, Gottesman left open the question of an encryption scheme that would *prevent* the *splitting* of a ciphertext. In other words, would it be possible to encrypt

a classical message into a quantum ciphertext, such that no attack at the ciphertext level would be significantly successful in producing *two* quantum registers, each of which, when combined with the decryption key, could be used to reconstruct the plaintext?

In this work, we define, construct and prove security for a scheme that answers Gottesman's question in the positive. We call this *uncloneable encryption*. The core technical aspects of this work were first presented in one of the author's M.Sc. thesis [Lor19].

1.1 Summary of Contributions

We consider encryption schemes that encode classical plaintexts into quantum ciphertexts, which we formalize in Definition 4. For simplicity, in this work, we consider only the one-time, symmetric-key case. Next, we define uncloneable encryption (Definition 8). Informally, this can be thought of as a game, played between the honest sender (Alice) and two malicious recipients (Bob and Charlie). First, Alice picks a message $m \in \{0,1\}^n$ and a key $k \in \{0,1\}^{\kappa(\lambda)}$ (κ is a polynomial in some security parameter, λ). She encrypts her message into a quantum ciphertext register R. Initially, Bob and Charlie are physically together, and they receive R. They apply a quantum map to produce two registers: Bob keeps register B and Charlie keeps register C. Bob and Charlie are then isolated. In the next phase, Alice reveals k to both parties. Using k and their quantum register, Bob and Charlie produce m_B and m_C respectively. Bob and Charlie *win* if and only if $m_B = m_C = m$. The scheme is *t-uncloneable secure* if their winning probability is upper bounded by $2^{-n+t} + \eta(\lambda)$ for a negligible η.

Assuming that Alice picks her message uniformly at random, our results are summarized in Fig. 1, where we plot upper bounds for the winning probability of Bob and Charlie against various types of encodings, according to the length of m. First of all, if the encoding is classical, then Bob and Charlie can each keep a copy of the ciphertext. Combined with the key k, each party decrypts to obtain m. This gives the horizontal line at Pr[Adversaries win] = 1. Next, a lower bound on the winning probability for *any* encryption scheme is $\frac{1}{2^n}$ (corresponding to the parties coordinating a random guess). This is the *ideal* curve. Our goal is therefore to produce an encryption scheme that matches the ideal curve as close as possible.

It may seem that asking that Alice sample her message uniformly at random would be particularly restrictive, but this is not the case — we show in Theorem 9 that security in the case of uniformly sampled messages implies security in the case of non-uniformly sampled messages, if the message size does not grow with the security parameter. Specifically, if Bob and Charlie can win with probability at most $2^{-n+t}+\eta(\lambda)$ when the message is sampled uniformly at random, for some t and some negligible function η, then they can win with probability at most $2^{-h+t}+\eta'(\lambda)$ if the message m is sampled from a distribution with a min-entropy of h where η' is a negligible function which is larger than η.

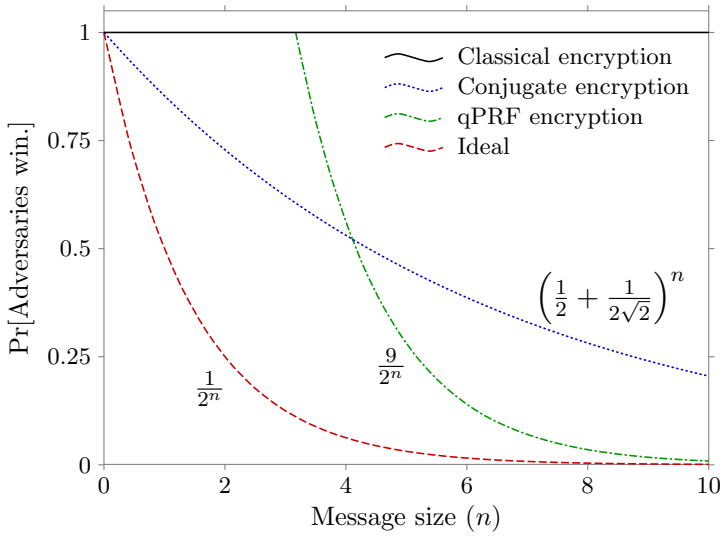

Figure 1: Upper-bounds on winning probabilities for various types of encodings (up to negligible functions of λ) for messages sampled uniformly at random.

Our first attempt at realizing uncloneable encryption (Section 4.1) shows that the well-known Wiesner conjugate coding [Wie83] already achieves a security bound that is better than any classical scheme. For any strings $x, \theta \in \{0,1\}^n$, define the Wiesner state $\left|x^\theta\right\rangle = H^{\theta_1}\left|x_1\right\rangle \otimes \ldots \otimes H^{\theta_n}\left|x_n\right\rangle$. The encryption uses a random key $r, \theta \in \{0,1\}^n$ and maps a classical message m into the quantum state $\rho = \left|(m \oplus r)^\theta\right\rangle\!\left\langle(m \oplus r)^\theta\right|$; given r, θ, decryption consists in measuring in the basis determined by θ to obtain x and then computing $x \oplus r$. We sketch a proof that this satisfies a notion of security for encryption schemes. The question of uncloneability then boils down to: "How well can an adversary *split* ρ into *two* registers, each of which, combined with (θ, r) can reconstruct m?" This question is answered in prior work on *monogamy-of-entanglement games* [TFKW13]: an optimal strategy wins with probability $\left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right)^n$. This is again illustrated in Fig. 1.

In order to improve this bound, we use a quantum-secure pseudorandom function (qPRF) $f_\lambda : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^n$ (see Definition 3). The encryption (see Section 4.2) consists of a quantum state $\rho = \left|r^\theta\right\rangle\!\left\langle r^\theta\right|$ for random $r, \theta \in \{0,1\}^\lambda$, together with a classical string $c = m \oplus f_\lambda(s, r)$ for a random s. The key k consists in θ and s. Once again, it can be shown that this is an encryption scheme in a more usual sense and we sketch this argument in Section 4.2. Intuitively, the use of f_λ affords us a gain in uncloneable security, because an adversary who wants to output m would need to know the pre-image of m under $f_\lambda(s, \cdot)$. Reaching a formal proof along these lines, however, is tricky. First, we model the qPRF using a quantum oracle [BBC+01, BDF+11]; this limits the adversaries' interaction

with the qPRF to be black-box quantum queries. Next, the quantum oracle model is notoriously tricky to use and many of the techniques in the classical literature are not directly applicable. Fortunately, we can adapt techniques from Unruh's quantum one-way-to-hiding lemma [Unr15] to the two-player setting, which enables us to recover a precise statement along the lines of the intuition above. We thus complete the proof of our main Theorem 22, obtaining the bound $9 \cdot \frac{1}{2^n} + \mathrm{negl}(\lambda)$. This is the fourth and final curve in Fig. 1.

In addition to the above, we formally define a different type of uncloneable security: inspired by more standard security definitions of *indistinguishability*, we define *uncloneable-indistinguishability* (Definition 11). This security definition bounds the advantage that the adversaries have at *simultaneously* distinguishing between an encryption of 0^n and an encryption of a plaintext of length n, as prepared by the adversaries. In a series of results (Theorems 12 and 23 and Corollary 24), we show that our main protocol achieves this security notion against adversaries that use *unentangled strategies* and if the message size does not grow with λ. As discussed in Section 1.2, there are interesting uses cases where we can assume that the adversaries do not share entanglement.

We note that our protocols (both Definition 13 and Definition 16) have the desirable property of being *prepare-and-measure* schemes. This means that the quantum technology for the honest users is limited to the preparation of single-qubit pure states, as well as to single-qubit measurements; these quantum technologies are mature and commercially available. (Note, however, that quantum storage remains a major challenge at the implementation level).

1.2 Applications

While our focus is on the conceptual contribution of defining and proving a new primitive, we believe that uncloneable encryption could have many applications. We give two such examples.

Quantum Money. As it captures the idea of "uncloneable classical information" in a very generic manner, uncloneable encryption can be used as a tool to build other primitives which leverage the uncloneability of quantum states. As an example, any uncloneable secure encryption scheme naturally yields a private-key quantum money scheme [Wie83, AC12].

To obtain quantum money from an uncloneable encryption scheme, we identify the notion of "simultaneously passing the bank's verification" with the notion of "simultaneously obtaining the correct plaintext". To generate a banknote, the bank samples a message m, a key k, a serial number s and produces as output $(s, Enc(k, m))$, where $Enc(k, m)$ is the uncloneable encryption of m with the key k. When the bank is asked to verify a banknote, it verifies the serial number in its database to retrieve k, decrypts the ciphertext and verifies if the message obtained is indeed m.

The uncloneable security guarantee implies that the probability of a malicious party producing two banknotes which pass this test is negligible. If this were not the case, we could use the attack which counterfeits the banknote to essentially copy the ciphertext in the underlying uncloneable encryption scheme. The adversaries tasked with obtaining the message once the key is revealed then simply decrypt as if they were the honest receivers.

Preventing Storage Attacks by Classical Adversaries. Indistinguishable-uncloneable encryption prevents a single eavesdropping adversary with no quantum memory from collecting ciphertexts exchanged by two honest parties in the hope of later learning the key. We sketch an argument for this fact.

Suppose such an adversary obtains a ciphertext encoded with an uncloneable-indistinguishable encryption scheme. We claim that they cannot correctly determine if the ciphertext corresponds to the encryption of 0^n or of some known message m with non-negligible advantage, even if the decryption key becomes known after their measurement of the ciphertext. If such an adversary existed, it could be used to break the uncloneable-indistinguishable security of the encryption scheme. Indeed, the almost classical eavesdropper could create two copies of their classical memory and distribute it to the two adversaries who attempt to obtain the message once the key is revealed.[1]

Note that the adversaries in this attack do not share any entanglement and so we can apply Corollary 24 which states that our encryption scheme is uncloneable-indistinguishable secure under this condition.

Our work is currently in the private-key setting, but can be extended in a straightforward way to the public-key setting. In this scenario, we can still guarantee the secrecy of the message even if the eavesdropper is later able to determine the decryption key from the publicly known encryption key. In other words, an eavesdropping adversary with no quantum memory would need to attack the ciphertext at the moment of transmission. This is known as *everlasting* security or *long-term* security.

1.3 More on Related Work

Starting with the foundational work of Wiesner [Wie83], a rich body of literature has considered the encoding of classical information into quantum states in order to take advantage of quantum properties for cryptography.

Quantum Key Recycling. The concept of quantum key recycling is a precursor to the QKD protocol, developed by Bennett, Brassard, and Breidbart [BBB14] (the manuscript was prepared in 1982 but only published recently). According to this protocol, it is possible to encrypt a classical message into a quantum state, such

[1] We thank an anonymous reviewer for this suggestion.

that information-theoretic security is assured, but in addition, a tamper detection mechanism would allow the one-time pad key to be re-used in the case that no eavesdropping is detected. Quantum key recycling has been the object of recent related work [DPS05, FS17].

Tamper-Evident Encryption. We referred above to tamper-detection in the case of encryption, which we will also call *tamper-evident encryption*. However, we emphasize that the author originally called this contribution *uncloneable encryption* [Got03]. We justify this choice of re-labelling in quoting the conclusion of the work:

> One difficulty with such generalizations is that it is unclear to what extent the name "uncloneable encryption" is really deserved. I have not shown that a message protected by uncloneable encryption cannot be copied — only that Eve cannot copy it without being detected. Is it possible for Eve to create two states, (...), which can each be used (in conjunction with the secret key) to extract a good deal of information about the message? Or can one instead prove bounds, for instance, on the sum of the information content of the various purported copies? [Got03]

Since our work addresses this question, we have appropriately re-labeled prior work according to a seemingly more accurate name.

To the best of our knowledge, the precise relationship between quantum key-recycling, tamper-evident encryption, and uncloneable encryption is unknown (see Section 1.4).

Quantum Copy-Protection. Further related work includes the study of *quantum copy-protection*, as initiated by Aaronson [Aar09]. Informally, this is a means to encode a function (from a given family of functions) into a quantum program state, such that an honest party can evaluate the function given the program state, but it would be impossible to somehow *split* the quantum program state so as to enable *two* parties to simultaneously evaluate the function. Aaronson gave protocols for quantum copy-protection in an oracle model, but left wide open the question of quantum copy-protection in the plain model. In a way, uncloneable encryption is a first step towards quantum copy-protection, since it prevents copying of *data*, which can be seen as a unit of information that is even simpler than a function.

1.4 Outlook and Future Work

In this work, we show that, thanks to quantum information, one of the basic tacit assumptions of encryption, namely that an adversary can copy ciphertexts, is challenged. We believe that this has the potential to significantly change the landscape of cryptography, for instance in terms of techniques for *key management* [Bar16].

Furthermore, our techniques could become building blocks for a theory of uncloneable cryptography.

Our work leads to many follow-up questions, broadly classified according to the following themes:

Improvements. There are many possible improvements to the current work. For instance: Could our scheme be made resilient to errors? Can we remove the reliance on the oracle, and/or on the qPRF? Could an encryption scheme simultaneously be uncloneable *and* provide *tamper detection*? Would achieving uncloneable-indistinguishable security be possible, without any restrictions on the adversary's strategy?

Links with related work. What are the links, if any, between uncloneable encryption, tamper-evident encryption [Got03], and quantum encryption with key recycling [BBB14, DPS05, FS17]? We note that both uncloneable encryption and quantum encryption with key recycling [FS17] make use of theorems developed in the context of one-sided device-independent QKD [TFKW13]. Can we make more formal links between these primitives?

More uncloneability. Finally, our work paves the way for the study of more complex unclonable primitives. Could this lead to uncloneable programs [Aar09]? What about in complexity theory, could we define and realize uncloneable *proofs* [Aar09]?

1.5 Outline

The remainder of the paper is structured as follows. In Section 2, we introduce some basic notation and useful results from the literature. In Section 3, we formally define uncloneable encryption schemes and their security. Our two protocols are described and proved secure in Section 4.

2 Preliminaries

In this section, we present basic notation, together with techniques from prior work that are used in the remainder of the paper.

2.1 Notation and Basics of Quantum Information

We denote the set of all functions of the form $f : \{0,1\}^n \to \{0,1\}^m$ by $\mathrm{Bool}(n,m)$. We denote the set of strictly positive natural numbers by $\mathbb{N}^+$. All Hilbert spaces are finite dimensional. We overload the expectation symbol $\mathbb{E}$ in the following way: If X is a finite set, $\mathcal{X}$ a random variable on X, and $f : X \to \mathbb{R}$ some function, we

define

$$\mathop{\mathbb{E}}_{x \leftarrow \mathcal{X}} f(x) = \sum_{x \in X} \Pr\left[x = \mathcal{X}\right] f(x). \tag{1}$$

If we omit the random variable, we assume a uniform distribution. In other words, $\mathbb{E}_x f(x) = \frac{1}{|X|} \sum_{x \in X} f(x)$.

A comprehensive introduction to quantum information and quantum computing may be found in [NC00, Wat18]. We fix some notation in the following paragraphs.

Let $\mathcal{Q} = \mathbb{C}^2$ be the state space of a single qubit. In particular, $\mathcal{Q}$ is a two-dimensional complex Hilbert space spanned by the orthonormal set $\{|0\rangle, |1\rangle\}$. For any $n \in \mathbb{N}^+$, we write $\mathcal{Q}(n) = \mathcal{Q}^{\otimes n}$ and note that

$$\{|s\rangle = |s_1\rangle \otimes |s_2\rangle \otimes \ldots \otimes |s_n\rangle\}_{s \in \{0,1\}^n} \tag{2}$$

forms an orthonormal basis of $\mathcal{Q}(n)$.

Let $\mathcal{H}$ be a Hilbert space. The set of all unitary and density operators on $\mathcal{H}$ are denoted by $\mathcal{U}(\mathcal{H})$ and $\mathcal{D}(\mathcal{H})$, respectively. We recall that the operator norm of any linear operator $A : \mathcal{H} \to \mathcal{H}'$ between finite dimensional Hilbert spaces is given by

$$\|A\| = \max_{\substack{v \in \mathcal{H} \\ \|v\| = 1}} \|Av\| \tag{3}$$

and satisfies the property that $\|Av\| \leq \|A\| \cdot \|v\|$. If A is either a projector or a unitary operator, then $\|A\| = 1$.

We use the term "quantum state" to refer to both unit vectors $|\psi\rangle \in \mathcal{H}$ and to density operators $\rho \in \mathcal{D}(\mathcal{H})$ on some Hilbert space.

If $H \in \mathcal{U}(\mathcal{Q})$ is the Hadamard operator defined by

$$|0\rangle \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ and } |1\rangle \mapsto \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{4}$$

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

$$\left|x^\theta\right\rangle = H^{\theta_1} |x_1\rangle \otimes H^{\theta_2} |x_2\rangle \otimes \ldots \otimes H^{\theta_n} |x_n\rangle \tag{5}$$

and note that $\left\{\left|s^\theta\right\rangle\right\}_{s \in \{0,1\}^n}$ forms an orthonormal basis of $\mathcal{Q}(n)$. Following their prominent use in [Wie83], we call states of the form $\left|x^\theta\right\rangle$ Wiesner states and, for any fixed $\theta \in \{0,1\}^n$, we call $\left\{\left|s^\theta\right\rangle\right\}_{s \in \{0,1\}^n}$ a Wiesner basis.

For any $n \in \mathbb{N}^+$, we define the Einstein-Podolski-Rosen [EPR35] (EPR) state by

$$|\mathrm{EPR}_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |x\rangle \tag{6}$$

and note that it is an element of $\mathcal{Q}(2n)$.

A positive operator-valued measurement (POVM) on a Hilbert space $\mathcal{H}$ is a finite collection of positive semidefinite operators $\{E_i\}_{i\in I}$ on $\mathcal{H}$ which sum to the identity. A projective measurement is a POVM composed of projectors.

We also recall that physically permissible transformation of a quantum system precisely coincide with the set of completely positive trace preserving (CPTP) maps. In particular, CPTP map will map density operators to density operators.

A polynomial-time uniform family of circuits $\mathtt{C} = \{\mathtt{C}_\lambda\}_{\lambda\in\mathbb{N}^+}$ is a collection of quantum circuits indexed by $\mathbb{N}^+$ such that there exists a polynomial-time deterministic Turing machine $\mathtt{T}$ which, on input 1^λ, produces a description of $\mathtt{C}_\lambda$. We refer to such families as efficient circuits. Each circuit $\mathtt{C}_\lambda$ defines and implements a certain CPTP map $C_\lambda : \mathcal{D}(\mathcal{H}_{\mathrm{In},\lambda}) \to \mathcal{D}(\mathcal{H}_{\mathrm{Out},\lambda})$, where the Hilbert spaces $\mathcal{H}_{\mathrm{In},\lambda}$ and $\mathcal{H}_{\mathrm{Out},\lambda}$ are implicitly defined by the circuit. Note that we consider general, which is to say possibly non-unitary, circuits. These were introduced in [AKN98]. It is worth noting that a universal gate set for general quantum circuits exists which is composed of only unitary gates, implementing maps of the form $\rho \mapsto U\rho U^\dagger$ for some unitary operator U, and two non-unitary maps which are

- the single qubit partial trace map $\mathrm{Tr} : \mathcal{D}(\mathcal{Q}) \to \mathcal{D}(\mathbb{C})$ and
- the state preparation map $\mathrm{Aux} : \mathcal{D}(\mathbb{C}) \to \mathcal{D}(\mathcal{Q})$ defined by $1 \mapsto |0\rangle\langle 0|$.

Further information on this circuit model can be found in [Wat09].

2.2 Monogamy of Entanglement Games

Monogamy-of-entanglement games were introduced and studied in [TFKW13]. In short, a monogamy-of-entanglement game is played by Alice against cooperating Bob and Charlie. Alice describes to Bob and Charlie a collection of different POVMs which she could use to measure a quantum state on a Hilbert space $\mathcal{H}_A$. These POVMs are indexed by a finite set Θ and each reports a measurement result taken from a finite set X. Bob and Charlie then produce a tripartite quantum state $\rho \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$, giving the A register to Alice, the B register to Bob and the C register to Charlie. Alice then picks a $\theta \in \Theta$, measures her subsystem with the corresponding POVM and obtains some result $x \in X$. She then announces θ to Bob and Charlie who are now isolated. Bob and Charlie win if and only if they can both simultaneously guess the result x.

Upper bounds on the winning probability of Bob and Charlie in such games was the primary subject of study in [TFKW13]. One of their main results, corresponding to a game where Alice measures in a random Wiesner basis, is as follows.

Theorem 1.
Let $\lambda \in \mathbb{N}^+$. For any Hilbert spaces $\mathcal{H}_B$ and $\mathcal{H}_C$, any collections of POVMs

$$\left\{\left\{B_x^\theta\right\}_{x\in\{0,1\}^\lambda}\right\}_{\theta\in\{0,1\}^n} \text{ and } \left\{\left\{C_x^\theta\right\}_{x\in\{0,1\}^\lambda}\right\}_{\theta\in\{0,1\}^n} \tag{7}$$

on these Hilbert spaces, and any state $\rho \in \mathcal{D}(\mathcal{Q}(\lambda) \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$, we have that

$$\mathop{\mathbb{E}}_{\theta} \sum_{x \in \{0,1\}^\lambda} \mathrm{Tr}\left[\left(\left|x^\theta\right\rangle\!\left\langle x^\theta\right| \otimes B_x^\theta \otimes C_x^\theta\right)\rho\right] \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^\lambda. \tag{8}$$

Using standard techniques, we can recast this theorem in a context where Alice sends to Bob and Charlie a random Wiesner state and Bob and Charlie split this state among themselves via some CPTP map Φ.

Corollary 2.
Let $\lambda \in \mathbb{N}^+$. For any Hilbert spaces $\mathcal{H}_B$ and $\mathcal{H}_C$, any collections of POVMs

$$\left\{\left\{B_x^\theta\right\}_{x\in\{0,1\}^\lambda}\right\}_{\theta\in\{0,1\}^\lambda} \text{ and } \left\{\left\{C_x^\theta\right\}_{x\in\{0,1\}^\lambda}\right\}_{\theta\in\{0,1\}^\lambda} \tag{9}$$

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

$$\mathop{\mathbb{E}}_{\theta}\mathop{\mathbb{E}}_{x} \mathrm{Tr}\left[\left(B_x^\theta \otimes C_x^\theta\right)\Phi\left(\left|x^\theta\right\rangle\!\left\langle x^\theta\right|\right)\right] \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^\lambda. \tag{10}$$

The proof is relegated to Appendix A, but conceptually follows from a two-step argument. First, we only consider states of the form $(\mathbb{1} \otimes \Phi)\left|\mathrm{EPR}_\lambda\right\rangle\!\left\langle\mathrm{EPR}_\lambda\right|$ for some CPTP map Φ and where Alice keeps the intact subsytems from the EPR pairs. Then, we apply the correspondence between Alice measuring her half of an EPR pair in a random Wiesner basis and her sending a random Wiesner state. This correspondence is similar to the one used in the Shor-Preskill proof of security for the BB84 QKD protocol [SP00].

Corollary 2 can be seen as the source of "uncloneability" for our upcoming protocols. When Alice sends a state $\left|x^\theta\right\rangle\!\left\langle x^\theta\right|$, picked uniformly at random, to Bob and Charlie, she has a guarantee that it is unlikely for both of them to learn x even if she later divulges θ.

It is worth noting that Theorem 1 and Corollary 2 have no computational or hardness assumptions. This makes them an ideal tool with which to build uncloneable encryption schemes.

2.3 Oracles and Quantum-Secure Pseudorandom Functions

A quantum-secure pseudorandom function is a keyed function which appears random to an efficient quantum adversary who only sees its input/output behaviour and is ignorant of the particular key being used. We formally define this notion with the help of oracles. Quantum accessible oracles have been previously studied in the literature, for example in [BBC+01, BDF+11, Unr15].

Given a function $H \in \mathrm{Bool}(n, m)$, a quantum circuit $\mathtt{C}$ is said to have oracle access to H, denoted $\mathtt{C}^H$, if we add to its gate set a gate implementing the unitary

operator $O^H \in \mathcal{U}(\mathcal{Q}(n)_Q \otimes \mathcal{Q}(m)_R)$ defined on computational basis states by

$$|x\rangle_Q \otimes |y\rangle_R \mapsto |x\rangle_Q \otimes |y \oplus H(x)\rangle_R \ . \tag{11}$$

Colloquially, we are giving $\mathtt{C}$ a "black box" which computes the function H. Note that if $H, H' \in \mathrm{Bool}(n, m)$ are two functions, we can obtain the circuit $C^{H'}$ from C^H by replacing every instance of the O^H gate by the $O^{H'}$ gate.

We can now give a definition, inspired by the one in [Zha12], of a quantum-secure pseudorandom function.

Definition 3 (Quantum-Secure Pseudorandom Function)**.**
A *quantum-secure pseudorandom function* $\mathcal{F}$ is a collection of functions

$$\mathcal{F} = \left\{ f_\lambda : \{0,1\}^\lambda \times \{0,1\}^{\ell_{\mathrm{In}}(\lambda)} \to \{0,1\}^{\ell_{\mathrm{Out}}(\lambda)} \right\}_{\lambda \in \mathbb{N}^+} \tag{12}$$

where $\ell_{\mathrm{In}}, \ell_{\mathrm{Out}} : \mathbb{N}^+ \to \mathbb{N}^+$ and such that:

1. There is an efficient quantum circuit $\mathtt{F} = \{\mathtt{F}_\lambda\}_{\lambda \in \mathbb{N}^+}$ such that $\mathtt{F}_\lambda$ implements the CPTP map $F_\lambda(\rho) = U_\lambda \rho U_\lambda^\dagger$ where $U_\lambda \in \mathcal{U}(\mathcal{Q}(\lambda + \ell_{\mathrm{In}}(\lambda) + \ell_{\mathrm{Out}}(\lambda)))$ is defined by
$$U_\lambda\big(|k\rangle |a\rangle |b\rangle \big) = |k\rangle |a\rangle |b \oplus f_\lambda(k, a)\rangle \ . \tag{13}$$

2. For all efficient quantum circuits $\mathtt{D} = \{\mathtt{D}_\lambda^H\}_{\lambda \in \mathbb{N}^+}$ having oracle access to a function of the form $H \in \mathrm{Bool}(\ell_{\mathrm{In}}(\lambda), \ell_{\mathrm{Out}}(\lambda))$, each implementing a CPTP map of the form $D_\lambda^H : \mathcal{D}(\mathbb{C}) \to \mathcal{D}(\mathcal{Q})$, there is a negligible function η such that:
$$\left| \mathop{\mathbb{E}}_k \mathrm{Tr}\left[|0\rangle\langle 0| \, D_\lambda^{f_\lambda(k,\cdot)}(1) \right] - \mathop{\mathbb{E}}_H \mathrm{Tr}\left[|0\rangle\langle 0| \, D_\lambda^H(1) \right] \right| \leq \eta(\lambda) \, . \tag{14}$$

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

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

In his work on quantum-secure pseudorandom functions [Zha12], Zhandry showed that certain pseudorandom functions that are secure against classical adversaries are insecure against quantum adversaries. Fortunately, Zhandry also showed that some common constructions of pseudorandom functions remain secure against quantum adversaries.

3 Uncloneable Encryption

The encryption of classical plaintexts into classical ciphertexts has been extensively studied. The study of encrypting quantum plaintexts into quantum ciphertexts has also received some attention, for example in [ABF+16]. Uncloneable encryption is a security notion for classical plaintexts which is impossible to achieve in any meaningful way with classical ciphertexts. Thus, we need to formally define a notion of quantum encryptions for classical messages.

3.1 Quantum Encryptions of Classical Messages

A quantum encryption of classical messages scheme is a procedure which takes as input a plaintext and a key, in the form of classical bit strings, and produces a ciphertext in the form of a quantum state. We model these schemes as efficient quantum circuits and CPTP maps where classical bit strings are identified with computational basis states: $s \leftrightarrow |s\rangle\langle s|$. Our schemes are parametrized by a security parameter λ. In general, the message size $n = n(\lambda)$, the key size $\kappa = \kappa(\lambda)$, and the size of the ciphertext $\ell = \ell(\lambda)$ may depend on λ. This is formalized in Definition 4.

Definition 4 (Quantum Encryption of Classical Messages)**.**
A *quantum encryption of classical messages* (QECM) scheme is a triplet of efficient quantum circuits $\mathcal{S} = (\texttt{Key}, \texttt{Enc}, \texttt{Dec})$ implementing CPTP maps of the form

- $Key_\lambda : \mathcal{D}(\mathbb{C}) \to \mathcal{D}(\mathcal{H}_{K,\lambda})$,
- $Enc_\lambda : \mathcal{D}(\mathcal{H}_{K,\lambda} \otimes \mathcal{H}_{M,\lambda}) \to \mathcal{D}(\mathcal{H}_{T,\lambda})$, and
- $Dec_\lambda : \mathcal{D}(\mathcal{H}_{K,\lambda} \otimes \mathcal{H}_{T,\lambda}) \to \mathcal{D}(\mathcal{H}_{M,\lambda})$

where $\mathcal{H}_{M,\lambda} = \mathcal{Q}(n(\lambda))$ 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 $n, \ell, \kappa : \mathbb{N}^+ \to \mathbb{N}^+$.

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

$$\mathrm{Tr}[|k\rangle\langle k|\, Key(1)] > 0 \implies \mathrm{Tr}[|m\rangle\langle m|\, Dec_k \circ Enc_k\, |m\rangle\langle m|] = 1 \tag{15}$$

where λ is implicit, Enc_k is the CPTP map defined by $\rho \mapsto Enc(|k\rangle\langle k| \otimes \rho)$, and we define Dec_k analogously.

A short discussion on the key generation circuit, $\texttt{Key}$, is in order. First, note that $\texttt{Key}$ takes no input. Indeed, the domain of Key_λ is $\mathcal{D}(\mathbb{C})$ and $\mathbb{C}$ is the state space of zero qubits. In particular, there is a single valid quantum state on $\mathbb{C}$: $\mathcal{D}(\mathbb{C}) = \{1\}$. To generate a classical key to be used by the encryption and decryption circuits $\texttt{Enc}_\lambda$ and $\texttt{Dec}_\lambda$, a party runs the circuit $\texttt{Key}_\lambda$ and obtains the quantum state $Key_\lambda(1)$. This quantum state is then measured in the computational basis and the result of this measurement is used as the key. We then see that Eq. (15) is a correctness condition which imposes that, for all keys that may be generated, a valid ciphertext is always correctly decrypted.

3.2 Security Notions

Now that we have formal definition for QECM schemes, we can define security notions for these schemes. We define three such notions:

1. Indistinguishable security. Conceptually inspired by the original security notion of indistinguishable encryptions [GM84], which considers classical plaintexts and classical ciphertexts, and similar in details to an analogue definition in [ABF+16] which considers quantum plaintexts and quantum ciphertexts, this security notion considers classical plaintexts and quantum ciphertexts. It is formally stated in Definition 6.

2. Uncloneable security. This security notion is novel to this work and captures, in the broadest sense, what we mean by an "uncloneable encryption scheme". This security notion is defined in Definition 8 and is paramatrized by a real value $0 \leq t \leq n$, where n is the message size. The case where $t = 0$ is ideal and $t = n$ is trivial. In particular, no encryption scheme with classical ciphertexts may achieve t-uncloneable security for $t < n$.

3. Uncloneable-indistinguishable security. This security notion is also novel to this work. It can be seen as a combination of indistinguishable and uncloneable security. It is formally defined in Definition 11.

Each of these security notions is defined in two steps. First, we define a type of attack (Definitions 5, 7 and 10). Then, we say that the QECM scheme achieves the given security notion if all admissible attacks have their winning probability appropriately bounded (Definitions 6, 8 and 11). The definitions for uncloneable security and uncloneable-indistinguishable security will formalize the games which we described in Section 1.1.

Note that many classical encryption schemes which are secure against quantum adversaries, such as the one-time pad, are indistinguishable secure but satisfy neither uncloneable security notions as their ciphertexts can alway be perfectly copied. We also discuss in Section 4.1 a scheme which offers non-trivial uncloneable security but is not in any way uncloneable-indistinguishable secure.

We first define our notion of indistinguishable security.

Definition 5 (Distinguishing Attack)**.**
Let $\mathcal{S}$ be a QECM scheme. A *distinguishing attack* against $\mathcal{S}$ is a pair of efficient quantum circuits $\mathcal{A} = (\mathtt{G}, \mathtt{A})$ implementing CPTP maps of the form

- $G_\lambda : \mathcal{D}(\mathbb{C}) \to \mathcal{D}(\mathcal{H}_{S,\lambda} \otimes \mathcal{H}_{M,\lambda})$ and
- $A_\lambda : \mathcal{D}(\mathcal{H}_{S,\lambda} \otimes \mathcal{H}_{T,\lambda}) \to \mathcal{D}(\mathcal{Q})$

where $\mathcal{H}_{S,\lambda} = \mathcal{Q}(s(\lambda))$ for a function $s : \mathbb{N}^+ \to \mathbb{N}^+$ and $\mathcal{H}_{M,\lambda}$ and $\mathcal{H}_{T,\lambda}$ are as defined in $\mathcal{S}$.

Definition 6 (Indistinguishable Security)**.**
Let $\mathcal{S}$ be an QECM scheme. For a fixed and implicit λ, we define the CPTP map $Enc_k^1 : \mathcal{D}(\mathcal{H}_{M,\lambda}) \to \mathcal{D}(\mathcal{H}_{T,\lambda})$ by

$$\rho \mapsto \sum_{m \in \{0,1\}^n} \mathrm{Tr}\left[|m\rangle\langle m|\,\rho\right] \cdot Enc_k(|m\rangle\langle m|) \tag{16}$$

and the CPTP map $Enc_k^0 : \mathcal{D}(\mathcal{H}_{M,\lambda}) \to \mathcal{D}(\mathcal{H}_{T,\lambda})$ by

$$\rho \mapsto Enc_k(|0^n\rangle\langle 0^n|) \tag{17}$$

where $0^n \in \{0,1\}^n$ is the all zero bit string.

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

$$\mathop{\mathbb{E}}_{b} \mathop{\mathbb{E}}_{k \leftarrow \mathcal{K}} \mathrm{Tr}\left[|b\rangle\langle b|\, A_\lambda \circ \left(\mathbb{1}_S \otimes Enc_k^b\right) \circ G(1)\right] \leq \frac{1}{2} + \eta(\lambda) \tag{18}$$

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

In Definition 6, the map Enc_k^0 should be seen as discarding whatever plaintext was given and producing the encryption of the all zero bit string. On the other hand, Enc_k^1 is the map which first measures the state given in the computational basis, to ensure that the plaintext is indeed a classical message, and then encrypts this message. We say that a QECM scheme has indistinguishable security if no efficient adversary can distinguish between both of these scenarios with more then a negligible advantage. This security notion allows us to show that the schemes we define do offer a level of security as encryption schemes.

Next, we formalize the intuitive definition for uncloneable security as given by the game described in Section 1.1. In Fig. 2, we sketch out the relation between the various CPTP maps and the underlying Hilber spaces considered in this definition.

Definition 7 (Cloning Attack)**.**
Let $\mathcal{S}$ be a QECM scheme. A *cloning attack* against $\mathcal{S}$ is a triplet of efficient quantum circuits $\mathcal{A} = (\mathtt{A}, \mathtt{B}, \mathtt{C})$ implementing CPTP maps of the form

- $A_\lambda : \mathcal{D}(\mathcal{H}_{T,\lambda}) \to \mathcal{D}(\mathcal{H}_{B,\lambda} \otimes \mathcal{H}_{C,\lambda})$,
- $B_\lambda : \mathcal{D}(\mathcal{H}_{K,\lambda} \otimes \mathcal{H}_{B,\lambda}) \to \mathcal{D}(\mathcal{H}_{M,\lambda})$, and
- $C_\lambda : \mathcal{D}(\mathcal{H}_{K,\lambda} \otimes \mathcal{H}_{C,\lambda}) \to \mathcal{D}(\mathcal{H}_{M,\lambda})$

where $\mathcal{H}_{B,\lambda} = \mathcal{Q}(\beta(\lambda))$ and $\mathcal{H}_{C,\lambda} = \mathcal{Q}(\gamma(\lambda))$ for some functions $\beta, \gamma : \mathbb{N}^+ \to \mathbb{N}^+$ and $\mathcal{H}_{K,\lambda}$, $\mathcal{H}_{M,\lambda}$, and $\mathcal{H}_{T,\lambda}$ are as defined by $\mathcal{S}$.

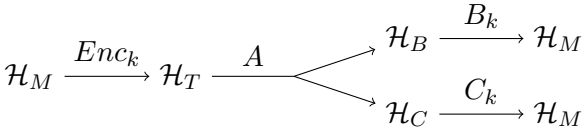

Figure 2: Schematic representation of the maps considered in a cloning attack as given in Definition 7.

Definition 8 (Uncloneable Security)**.**
A QECM scheme $\mathcal{S}$ is $t(\lambda)$-*uncloneable secure* if for all cloning attacks $\mathcal{A}$ against $\mathcal{S}$ there exists a negligible function η such that

$$\mathop{\mathbb{E}}_{m}\mathop{\mathbb{E}}_{k\leftarrow\mathcal{K}}\mathrm{Tr}\left[\left(|m\rangle\langle m|\otimes|m\rangle\langle m|\right)\left(B_k\otimes C_k\right)\circ A\circ Enc_k\left(|m\rangle\langle m|\right)\right]\leq 2^{-n+t(\lambda)}+\eta(\lambda) \tag{19}$$

where λ is implicit on the left-hand side, $\mathcal{K}_\lambda$ is a random variable distributed on $\{0,1\}^{\kappa(\lambda)}$ such that $\Pr\left[\mathcal{K}_\lambda=k\right]=\mathrm{Tr}\left[|k\rangle\langle k|\,Key_\lambda(1)\right]$ and B_k is the CPTP map defined by $\rho\mapsto B(|k\rangle\langle k|\otimes\rho)$ and similarly for C_k.

If $\mathcal{S}$ is 0-uncloneable secure, we say that it is simply *uncloneable secure*.

We note that any encryption which produces classical ciphertexts cannot be t-uncloneable secure for any $t<n$. Indeed, an attack $\mathcal{A}$ where $\mathtt{A}$ copies the classical ciphertext and where $\mathtt{B}=\mathtt{C}=\mathtt{Dec}$ succeeds with probability 1.

Our definition of uncloneable security is with respect to messages sampled uniformly at random. However, if the length of the message is fixed, t-uncloneable security implies a similar security notion for messages sampled according to other distributions. We formalize this in the next theorem.

Theorem 9.
Let $\mathcal{S}$ be a QECM scheme which is t-uncloneable secure and whose message size is constant, i.e.: $n(\lambda)=n$. Let $\mathcal{M}$ be a random variable distributed over $\{0,1\}^n$ with min-entropy h. Then, for any cloning attack $\mathcal{A}$ on $\mathcal{S}$ there is a negligible function η such that

$$\mathop{\mathbb{E}}_{m\leftarrow\mathcal{M}}\mathop{\mathbb{E}}_{k\leftarrow\mathcal{K}}\mathrm{Tr}\left[\left(|m\rangle\langle m|\otimes|m\rangle\langle m|\right)\left(B_k\otimes C_k\right)\circ A\circ Enc_k\,|m\rangle\langle m|\right]\leq 2^{-h+t(\lambda)}+\eta(\lambda) \tag{20}$$

where λ is implicit on the left-hand side.

Proof. For all $k\in\{0,1\}^{\kappa(\lambda)}$ and $m\in\{0,1\}^n$, define

$$p(k,m)=\mathrm{Tr}\left[\left(|m\rangle\langle m|\otimes|m\rangle\langle m|\right)\left(B_k\otimes C_k\right)\circ A\circ Enc_k\left(|m\rangle\langle m|\right)\right]. \tag{21}$$

Recalling the min-entropy of $\mathcal{M}$ and that $\mathcal{S}$ is t-uncloneable, we may write

$$\begin{aligned}&\mathop{\mathbb{E}}_{m\leftarrow\mathcal{M}}\mathop{\mathbb{E}}_{k\leftarrow\mathcal{K}}\operatorname{Tr}\left[(|m\rangle\langle m|\otimes|m\rangle\langle m|)\,(B_k\otimes C_k)\circ A\circ Enc_k\,(|m\rangle\langle m|)\right] \qquad (22)\\ &=\sum_{m\in\{0,1\}^n}\Pr\left[\mathcal{M}=m\right]\mathop{\mathbb{E}}_{k\leftarrow\mathcal{K}}p(k,m)\leq 2^{-h}\cdot 2^n\mathop{\mathbb{E}}_{m}\mathop{\mathbb{E}}_{k\leftarrow\mathcal{K}}p(k,m)\leq 2^{-h}\left(2^t+2^n\eta(\lambda)\right).\end{aligned}$$

Noting that $\lambda\mapsto 2^{-h+n}\eta(\lambda)$ is a negligible function concludes the proof. □

Finally, we formalize the notion of uncloneable-indistinguishable security (see Section 1.1 for a description in terms of a game, and Fig. 3 for the relation between the various CPTP maps and the underlying Hilbert spaces).

Definition 10 (Cloning-Distinguishing Attack)**.**
Let $\mathcal{S}$ be a QECM scheme. A *cloning-distinguishing attack* against $\mathcal{S}$ is a tuple $\mathcal{A}=(\mathtt{G},\mathtt{A},\mathtt{B},\mathtt{C})$ of efficient quantum circuits implementing CPTP maps of the form

- $G_\lambda:\mathcal{D}(\mathbb{C})\to\mathcal{D}(\mathcal{H}_{S,\lambda}\otimes\mathcal{H}_{M,\lambda})$,
- $A_\lambda:\mathcal{D}(\mathcal{H}_{S,\lambda}\otimes\mathcal{H}_{T,\lambda})\to\mathcal{D}(\mathcal{H}_{B,\lambda}\otimes\mathcal{H}_{C,\lambda})$,
- $B_\lambda:\mathcal{D}(\mathcal{H}_{K,\lambda}\otimes\mathcal{H}_{B,\lambda})\to\mathcal{D}(\mathcal{Q})$, and
- $C_\lambda:\mathcal{D}(\mathcal{H}_{K,\lambda}\otimes\mathcal{H}_{C,\lambda})\to\mathcal{D}(\mathcal{Q})$

where $\mathcal{H}_{S,\lambda}=\mathcal{Q}(s(\lambda))$, $\mathcal{H}_{B,\lambda}=\mathcal{Q}(\beta(\lambda))$, and $\mathcal{H}_{C,\lambda}=\mathcal{Q}(\alpha(\lambda))$ for some functions $s,\alpha,\beta:\mathbb{N}^+\to\mathbb{N}^+$ and all other Hilbert spaces are as defined by $\mathcal{S}$.

Definition 11 (Uncloneable-Indistinguishable Security)**.**
Let $\mathcal{S}$ be a QECM scheme and define Enc_k^0 and Enc_k^1 as in Definition 6.

We say that $\mathcal{S}$ is *uncloneable-indistinguishable secure* if for all cloning-distinguishing attacks $\mathcal{A}$ there exists a negligible function η such that

$$\mathop{\mathbb{E}}_{b}\mathop{\mathbb{E}}_{k\leftarrow\mathcal{K}}\operatorname{Tr}\left[(|b\rangle\langle b|\otimes|b\rangle\langle b|)\,(B_k\otimes C_k)\circ A\circ\left(\mathbb{1}_S\otimes Enc_k^b\right)\circ G(1)\right]\leq\frac{1}{2}+\eta(\lambda) \qquad (23)$$

where λ is implicit on the left-hand side, $\mathcal{K}_\lambda$ is distributed on $\{0,1\}^{\kappa(\lambda)}$ such that $\Pr[\mathcal{K}=k]=\operatorname{Tr}[|k\rangle\langle k|\,K(1)]$, B_k is the CPTP map defined by $\rho\mapsto B(|k\rangle\langle k|\otimes\rho)$, and similarly for C_k.

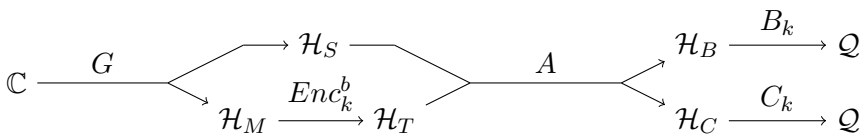

Figure 3: Relation between the CPTP maps and Hilbert spaces considered in a cloning-distinguishing attack as described in Definition 10.

It is trivial to see, but worth noting, that uncloneable-indistinguishable security implies indistinguishable security. We now briefly sketch the proof.

Let $\mathcal{S}$ be an QECM and $\mathcal{A} = (\mathtt{G}, \mathtt{A})$ be a distinguishing attack which shows that $\mathcal{S}$ is not indistinguishable secure. Then, we can construct a cloning-distinguishing attack $\mathcal{A}' = (\mathtt{G}', \mathtt{A}', \mathtt{B}', \mathtt{C}')$ which implies that $\mathcal{S}$ is not uncloneable-indistinguishable secure. Set $\mathtt{G}' = \mathtt{G}$ and $\mathtt{B}$ and $\mathtt{C}$ be the circuits which do nothing on a single qubit input. Then, we define $\mathtt{A}'$ to first run $\mathtt{A}$ and measure the output in the computational basis state. The result is a single classical bit which may then be copied and given to both $\mathtt{B}$ and $\mathtt{C}$. We then observe that the winning probability of $\mathcal{A}$ in the indistinguishable scenario is the same as the winning probability of $\mathcal{A}'$ in the uncloneable-indistinguishable scenario.

Finally, it can also be shown that any 0-uncloneable secure QECM $\mathcal{S}$ is uncloneable-indistinguishable secure. The proof of Theorem 12 can be found in Appendix A.

Theorem 12.
Let $\mathcal{S}$ be an QECM. If $\mathcal{S}$ is 0-uncloneable secure and has constant message size, i.e.: $n(\lambda) = n$, then it is also uncloneable-indistinguishable secure.

4 Two Protocols

In this section, we first present a protocol for the encryption of classical messages into quantum ciphertexts based on Wiesner's conjugate encoding (Section 4.1). This will also include a simple proof of its uncloneable security. Then, in Section 4.2, we present a refinement of this first protocol which uses quantum secure pseudorandom functions. The proof of the uncloneable security of this protocol is more involved and so we present some technical lemmas in Section 4.3 before we give our final main results in Section 4.4.

4.1 Conjugate Encryption

Our first QECM scheme is a one-time pad encoded into Wiesner states. We emphasize that this scheme will not offer much in terms of uncloneable security but it remains an instructive example.

Definition 13 (Conjugate Encryption)**.**
We define the *conjugate encryption* QECM scheme by the following circuits, each implicitly parametrized by λ. Note that the message size is $n(\lambda) = \lambda$, the key size is $\kappa(\lambda) = 2\lambda$ and the ciphertext size is $\ell(\lambda) = \lambda$.

Circuit 1: The key generation circuit `Key`.

Input : None.
Output: A state $\rho \in \mathcal{D}(\mathcal{Q}(\kappa))$.

1 Sample $r \leftarrow \{0,1\}^n$ uniformly at random.
2 Sample $\theta \leftarrow \{0,1\}^n$ uniformly at random.
3 Output $\rho = |r\rangle\langle r| \otimes |\theta\rangle\langle\theta|$.

Circuit 2: The encryption circuit `Enc`.

Input : A plaintext $m \in \{0,1\}^n$ and a key $(r,\theta) \in \{0,1\}^\kappa$.
Output: A ciphertext $\rho \in \mathcal{D}(\mathcal{Q}(n))$.

1 Output $\rho = \left|(m \oplus r)^\theta\right\rangle\!\left\langle(m \oplus r)^\theta\right|$.

Circuit 3: The decryption circuit `Dec`.

Input : A ciphertext $\rho \in \mathcal{D}(\mathcal{Q}(n))$ and a key $(r,\theta) \in \{0,1\}^\kappa$.
Output: A plaintext $m \in \{0,1\}^n$.

1 Compute $\rho' = H^\theta \rho H^\theta$.
2 Measure ρ' in the computational basis. Call the result c. Output $c \oplus r$.

The correctness of this scheme is trivial to verify and it is indistinguishable secure. The latter follows from the fact that if $Enc^0_{r,\theta}$ and $Enc^1_{r,\theta}$ are as defined in Definition 6, then for any $\rho \in \mathcal{D}(\mathcal{H}_S \otimes \mathcal{Q}(n))$ we have that

$$\mathop{\mathbb{E}}_{r}\mathop{\mathbb{E}}_{\theta}\left(\mathbb{1}_S \otimes Enc^1_{(r,\theta)}\right)(\rho) = \mathop{\mathbb{E}}_{r}\mathop{\mathbb{E}}_{\theta}\left(\mathbb{1}_S \otimes Enc^0_{(r,\theta)}\right)(\rho). \tag{24}$$

We will need one small technical lemma before proceeding to the proof of uncloneable security for this scheme. The proof can be found in Appendix A.

Lemma 14.
Let $n \in \mathbb{N}^+$, $f : \{0,1\}^n \times \{0,1\}^n \to \mathbb{R}$ be a function and $s \in \{0,1\}^n$ be a string. Then,

$$\mathop{\mathbb{E}}_{x} f(x, x \oplus s) = \mathop{\mathbb{E}}_{x} f(x \oplus s, x). \tag{25}$$

Theorem 15.
The scheme in Definition 13 is $\lambda \log_2\left(1 + \frac{1}{\sqrt{2}}\right)$-uncloneable secure.

Proof. It suffices to show that for any cloning attack $\mathcal{A}$ the quantity

$$\mathop{\mathbb{E}}_{m}\mathop{\mathbb{E}}_{r}\mathop{\mathbb{E}}_{\theta}\mathrm{Tr}\left[\left(|m\rangle\langle m| \otimes |m\rangle\langle m|\right)\left(B_{(r,\theta)} \otimes C_{(r,\theta)}\right) \circ A\left(\left|(m \oplus r)^\theta\right\rangle\!\left\langle(m \oplus r)^\theta\right|\right)\right] \tag{26}$$

is upper bounded by $\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^\lambda$. By applying Lemma 14 with respect to the expectation over m, this quantity is the same as

$$\mathop{\mathbb{E}}_{m}\mathop{\mathbb{E}}_{r}\mathop{\mathbb{E}}_{\theta}\mathrm{Tr}\left[\left(|m \oplus r\rangle\langle m \oplus r| \otimes |m \oplus r\rangle\langle m \oplus r|\right)\left(B_{(r,\theta)} \otimes C_{(r,\theta)}\right) \circ A\left(\left|m^\theta\right\rangle\!\left\langle m^\theta\right|\right)\right]. \tag{27}$$

We then see that for any fixed r, we can apply Corollary 2 to bound the expectation of the trace over m and θ by $\left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right)^{\lambda}$. Setting this quantity to be equal to 2^{-n+t}, recalling that $n=\lambda$, and solving for t completes the proof. □

Finally, note that this scheme cannot be uncloneable-indistinguishable secure if $n \geq 2$. Indeed, the adversaries could submit the all 1 plaintext to be encrypted and split the ciphertext such that each adversary gets half of the qubits. Once the key is revealed, the adversaries can then each obtain half of the message with probability 1. This is sufficient to distinguish between the two possible messages.

4.2 Our Protocol

As discussed in Section 1.1, the motivation for our second QECM scheme is to use quantum-secure pseudorandom functions to attempt to "distill" the uncloneability found in the Wiesner state.

Definition 16 ($\mathcal{F}$-Conjugate Encryption)**.**
For a function $n : \mathbb{N}^+ \to \mathbb{N}^+$, let

$$\mathcal{F} = \left\{ f_\lambda : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^{n(\lambda)} \right\}_{\lambda \in \mathbb{N}^+} \tag{28}$$

be a quantum-secure pseudorandom function. We define the $\mathcal{F}$-conjugate encryption QECM scheme by the following circuits which are implicitly parametrized by λ. Note that the message size is the output size of the qPRF, $n(\lambda)$, the key size is $\kappa(\lambda) = 2\lambda$, and the ciphertext size is $\ell(\lambda) = \lambda + n(\lambda)$.

Circuit 4: The key generation circuit `Key`.

Input : None.
Output: A state $\rho \in \mathcal{D}(\mathcal{Q}(\kappa(\lambda)))$.
1 Sample $s \leftarrow \{0,1\}^\lambda$ uniformly at random.
2 Sample $\theta \leftarrow \{0,1\}^\lambda$ uniformly at random.
3 Output $\rho = |s\rangle\langle s| \otimes |\theta\rangle\langle\theta|$.

Circuit 5: The encryption circuit `Enc`.

Input : A plaintext $m \in \{0,1\}^n$ and a key $(s,\theta) \in \{0,1\}^\kappa$.
Output: A ciphertext $\rho \in \mathcal{D}(\mathcal{Q}(\ell(\lambda)))$.
1 Sample $x \leftarrow \{0,1\}^\lambda$ uniformly at random.
2 Compute $c = m \oplus f_\lambda(s,x)$.
3 Output $\rho = |c\rangle\langle c| \otimes \left|x^\theta\right\rangle\left\langle x^\theta\right|$.

Circuit 6: The decryption circuit `Dec`.

Input : A ciphertext $|c\rangle\langle c| \otimes \rho \in \mathcal{D}(\mathcal{Q}(\ell))$ and a key $(s, \theta) \in \{0,1\}^\kappa$.
Output: A plaintext $m \in \{0,1\}^n$.

1 Compute $\rho' = H^\theta \rho H^\theta$.
2 Measure ρ' in the computational basis. Call the result r.
3 Output $m = c \oplus f_\lambda(s, r)$.

It is trivial to see that this scheme is correct and we can also show that it is indistinguishable secure. The latter follows from the fact that if we use a truly random function instead of the qPRF then, for any state ρ we have

$$\mathop{\mathbb{E}}_{r} \mathop{\mathbb{E}}_{H \in \mathrm{Bool}(\lambda,n)} \left(\mathbb{1}_S \otimes Enc^0_{(r,H)} \right)(\rho) = \mathop{\mathbb{E}}_{r} \mathop{\mathbb{E}}_{H \in \mathrm{Bool}(\lambda,n)} \left(\mathbb{1}_S \otimes Enc^1_{(r,H)} \right)(\rho) \tag{29}$$

where $Enc^0_{(r,H)}$ and $Enc^1_{(r,H)}$ are as given in Definition 6 except that they use a truly random function H instead of a keyed qPRF. Thus, any adversary has no advantage in distinguishing the cases. When the truly random functions are replaced by a qPRF, the adversary may have at most a negligible advantage in distinguishing these two cases.

4.3 Technical Lemmas

We first present a few technical lemmas which will be used in our proof of security. The proof of Lemmas 17 and 18 appear in Appendix A.

Lemma 17.
Let R be a ring with $a, b \in R$ and $c = a + b$. Then, for all $n \in \mathbb{N}^+$, we have that

$$c^n = a^n + \sum_{k=0}^{n-1} a^{n-k-1} b c^k. \tag{30}$$

Lemma 18.
Let $\mathcal{H}$ be a Hilbert space, $n \in \mathbb{N}^+$, and $\{v_0, v_1, \ldots, v_n\}$ be $n+1$ vectors in $\mathcal{H}$ such that $\|v_i\| \leq 1$ for all $i \in \{1, \ldots, n\}$ and $\|\sum_{i=0}^n v_i\| \leq 1$. Then,

$$\left\| \sum_{i=0}^{n} v_i \right\|^2 \leq \|v_0\|^2 + (3n+2) \sum_{i=1}^{n} \|v_i\|. \tag{31}$$

The following implicitly appears in [Unr15].

Lemma 19.
Let $f : \mathrm{Bool}(n, m) \to \mathbb{R}$ be a function and $x \in \{0,1\}^n$ be a string. For any $H \in \mathrm{Bool}(n, m)$ and $y \in \{0,1\}^m$, define $H_{x,y} \in \mathrm{Bool}(n, m)$ by

$$s \mapsto \begin{cases} H(s) & \text{if } s \neq x, \\ y & \text{if } s = x. \end{cases} \tag{32}$$

Then,

$$\mathop{\mathbb{E}}_{H} f(H) = \mathop{\mathbb{E}}_{H} \mathop{\mathbb{E}}_{y} f(H_{x,y}). \tag{33}$$

The following two lemmas form the core of the upcoming proofs of uncloneable security and they may be interpreted as follows. We consider two adversaries who have oracle access to a function $H \in \mathrm{Bool}(\lambda, n)$ which is chosen uniformly at random. Their goal is to simultaneously guess the value $H(x)$ for some value of x. The adversaries share some quantum state which we interpret as representing all the information they may initially have on x. The lemmas relate the probability of both parties simultaneously guessing $H(x)$ to their probability of being able to both simultaneously guess x.

The first of these lemmas, Lemma 20, considers this problem in a setting where the adversaries do not share any entanglement. The second, Lemma 21 imposes no such restriction.

We show that the probability that both adversaries correctly guess $H(x)$ is upper bounded by

$$\frac{1}{2^n} + Q \cdot G \qquad \text{or} \qquad 9 \cdot \frac{1}{2^n} + Q' \cdot G' \tag{34}$$

where Q and Q' are polynomial functions of the number of queries the adversaries make to the oracle and G and G' quantify their probability of guessing x with a particular strategy. The factor of 9 is present only if we allow the adversaries to share entanglement.

We can interpret G and G' in a manner very similar to its analogous quantity in Unruh's one-way-to-hiding lemma [Unr15]. The adversaries, instead of continuing until the end of their computation, will stop immediately before a certain (randomly chosen) query to the oracle and measure their query register in the computational basis. Then, G is related to the probability that this procedure succeeds at letting both adversaries simultaneously obtain x, averaged over the possible stopping points and possible functions implemented by the oracle.

The key idea in the proof of these lemmas is that we can decompose the unitary operator representing each of the adversaries' computations into two "parts". Explicitly, this decomposition appears in Eqs. (40) and (47). One of these "parts" will never query the oracle on x and the other could query the oracle on x. We note that this idea was present in the proof of Unruh's one-way-to-hiding lemma [Unr15].

Recall from Section 2.3 that we model queries to an oracle implementing a function H as a unitary operator O^H acting on a query and a response register with Hilbert spaces $\mathcal{H}_Q$ and $\mathcal{H}_R$ respectively. This unitary is defined on the computational basis states by $|x\rangle_Q \otimes |y\rangle_R \mapsto |x\rangle_Q \otimes |y \oplus H(x)\rangle_R$. A party having access to an oracle may also have some other register with Hilbert space $\mathcal{H}_S$ with which they perform other computations. In general, their computation can then be modeled by an operator of the form $\left(UO^H\right)^q$ where U is a unitary operator on $\mathcal{H}_Q \otimes \mathcal{H}_R \otimes \mathcal{H}_S$ and q is the number of queries made to the oracle [BBC+01, BDF+11, Unr15].

Lemma 20.
Let $\lambda, n \in \mathbb{N}^+$. For $L \in \{B, C\}$, we let

- $s_L, q_L \in \mathbb{N}^+$,
- $\mathcal{H}_{L_Q} = \mathcal{Q}(\lambda)$, $\mathcal{H}_{L_R} = \mathcal{Q}(n)$, and $\mathcal{H}_{L_S} = \mathcal{Q}(s_L)$,
- $U_L \in \mathcal{U}(\mathcal{H}_{L_Q} \otimes \mathcal{H}_{L_R} \otimes \mathcal{H}_{L_S})$, and
- $\{\pi_L^y\}_{y \in \{0,1\}^n}$ be a projective measurement on $\mathcal{H}_{L_Q} \otimes \mathcal{H}_{L_R} \otimes \mathcal{H}_{L_S}$.

Finally, let $|\psi\rangle = |\psi_B\rangle \otimes |\psi_C\rangle$ be a separable unit vector with $|\psi_L\rangle \in \mathcal{Q}(n + \lambda + s_L)$ for $L \in \{B, C\}$ and $x \in \{0,1\}^\lambda$. Then, we have

$$\mathop{\mathbb{E}}_{H} \left\| \Pi^{H(x)} \left(\left(U_B O_B^H\right)^{q_B} \otimes \left(U_C O_C^H\right)^{q_C} \right) |\psi\rangle \right\|^2 \leq \frac{1}{2^n} + (3q+2)q\sqrt[4]{M} \tag{35}$$

where $\Pi^{H(x)} = \pi_B^{H(x)} \otimes \pi_C^{H(x)}$, $q = q_B + q_C$ and

$$M = \mathop{\mathbb{E}}_{k} \mathop{\mathbb{E}}_{\ell} \mathop{\mathbb{E}}_{H} \mathop{\mathbb{E}}_{H'} \left\| \left(|x\rangle\langle x|_{B_Q} \otimes |x\rangle\langle x|_{C_Q} \right) \left(\left(U_B O_B^H\right)^k \otimes \left(U_C O_C^{H'}\right)^\ell \right) |\psi\rangle \right\|^2 \tag{36}$$

with $k \in \{0, \ldots, q_B - 1\}$, $\ell \in \{0, \ldots, q_C - 1\}$, and $H \in \mathrm{Bool}(\lambda, n)$.

Proof. Note that since $|\psi\rangle$ is separable, we have that

$$M = \underbrace{\left(\mathop{\mathbb{E}}_{H} \mathop{\mathbb{E}}_{k} \left\| |x\rangle\langle x|_{B_Q} \, \mathcal{O}^{U_B, H, k} |\psi_B\rangle \right\|^2 \right)}_{=M_B} \cdot \underbrace{\left(\mathop{\mathbb{E}}_{H'} \mathop{\mathbb{E}}_{\ell} \left\| |x\rangle\langle x|_{C_Q} \, \mathcal{O}^{U_C, H', \ell} |\psi_C\rangle \right\|^2 \right)}_{=M_C}. \tag{37}$$

For the remainder of the proof, we fix $L \in \{B, C\}$ such that $M_L = \min\{M_B, M_C\}$. Note that $\sqrt{M_L} \leq \sqrt[4]{M}$. Once again using the fact that $|\psi\rangle$ is separable, we have that

$$\mathop{\mathbb{E}}_{H} \left\| \Pi^{H(x)} \left(\left(U_B O_B^H\right)^{q_B} \otimes \left(U_C O_C^H\right)^{q_C} \right) |\psi\rangle \right\|^2 \leq \mathop{\mathbb{E}}_{H} \left\| \pi_L^{H(x)} \left(U_B O_B^H\right)^{q_L} |\psi_L\rangle \right\|^2. \tag{38}$$

With all this, it suffices to show that

$$\mathop{\mathbb{E}}_{H} \left\| \pi_L^{H(x)} \left(U_B O_B^H\right)^{q_L} |\psi_L\rangle \right\|^2 \leq \frac{1}{2^n} + (3q_L + 2)q_L\sqrt{M_L} \tag{39}$$

to obtain our result.

Let $P_L = |x\rangle\langle x|_{L_Q}$. Using the fact that $U_L O_L^H = U_L O_L^H P_L + U_L O_L^H (\mathbb{1} - P_L)$ and Lemma 17, we have that

$$\begin{aligned} \left(U_L O_L^H\right)^{q_L} = & \overbrace{\left(U_L O_L^H \left(\mathbb{1} - P_L\right)\right)^{q_L}}^{=V_L^H} + \\ & \sum_{k=0}^{q_L - 1} \underbrace{\left(U_L O_L^H \left(\mathbb{1} - P_L\right)\right)^{q_L - k - 1} U_L O_L^H P_L \left(U_L O_L^H\right)^k}_{=W_L^{H,k}} \end{aligned} \tag{40}$$

and we define $W_L^H = \sum_{k=0}^{q_L-1} W_L^{H,k}$ so that $\left(U_L O_L^H\right)^{q_L} = V_L^H + W_L^H$.

Using Lemma 18, the definition of the various W operators, and properties of the operator norm on projectors and unitary operators, we have that

$$\left\|\pi_L^{H(x)}\left(V_L^H + W_L^H\right)|\psi_L\rangle\right\|^2 \leq \left\|\pi_L^{H(x)} V_L |\psi_L\rangle\right\|^2 + (3q_L+2)q_L \mathop{\mathbb{E}}_k \left\|P_L\left(U_L O_L^H\right)^k |\psi_L\rangle\right\|. \tag{41}$$

Using Jensen's inequality, the above inequality, and the definition of M_L, we have that

$$\mathop{\mathbb{E}}_H \left\|\pi_L^{H(x)}\left(\left(U_L O_L^H\right)^{q_L}\right)|\psi_L\rangle\right\|^2 \leq \mathop{\mathbb{E}}_H \left\|\pi_L^{H(x)} V_L |\psi_L\rangle\right\|^2 + (3q_L+2)q_L\sqrt{M_L} \tag{42}$$

and so it suffices to show that $\mathbb{E}_H \left\|\pi_L^{H(x)} V_L^H |\psi_L\rangle\right\|^2 \leq 2^{-n}$. By Lemma 19, it is then sufficient to show that

$$\mathop{\mathbb{E}}_H \mathop{\mathbb{E}}_y \left\|\pi_L^y V_L^{H_{x,y}} |\psi_L\rangle\right\|^2 \leq 2^{-n} \tag{43}$$

where $H_{x,y} \in \mathrm{Bool}(\lambda, n)$ is defined by $H_{x,y}(x) = y$ and $H_{x,y}(s) = H(s)$ for all $s \neq x$. Recall that V_L^H is independent of the value of $H(x)$, in the sense that $V_L^{H_{x,y}} = V_L^H$ for all $y \in \{0,1\}^n$. Indeed, prior to every query to H in V_L^H, we project the state on a subspace which does not query H on x. So, using the fact that each π_L^y projects on mutually orthogonal subspaces and that $\left\|V_L^H\right\| \leq 1$, we have that

$$\mathop{\mathbb{E}}_y \left\|\pi_L^y V_L^{H_{x,y}} |\psi_L\rangle\right\|^2 = \frac{1}{2^n}\left\|V_L^H |\psi_L\rangle\right\|^2 \leq \frac{1}{2^n} \tag{44}$$

which completes the proof. □

Lemma 21.
Let $\lambda, n \in \mathbb{N}^+$. For $L \in \{B, C\}$, we let

- $s_L, q_L \in \mathbb{N}^+$,
- $\mathcal{H}_{L_Q} = \mathcal{Q}(\lambda)$, $\mathcal{H}_{L_R} = \mathcal{Q}(n)$, and $\mathcal{H}_{L_S} = \mathcal{Q}(s_L)$,
- $U_L \in \mathcal{U}(\mathcal{H}_{L_Q} \otimes \mathcal{H}_{L_R} \otimes \mathcal{H}_{L_S})$, and
- $\{\pi_L^y\}_{y\in\{0,1\}^n}$ be a projective measurement on $\mathcal{H}_{L_Q} \otimes \mathcal{H}_{L_R} \otimes \mathcal{H}_{L_S}$.

Finally, let $|\psi\rangle \in \mathcal{Q}(2(\lambda+n) + s_B + s_C)$ be a unit vector and $x \in \{0,1\}^\lambda$. Then, we have

$$\mathop{\mathbb{E}}_H \left\|\Pi^{H(x)}\left(\left(U_B O_B^H\right)^{q_B} \otimes \left(U_C O_C^H\right)^{q_C}\right)|\psi\rangle\right\|^2 \leq \frac{9}{2^n} + (3q_B q_C + 2)q_B q_C \sqrt{M} \tag{45}$$

where $\Pi^{H(x)} = \pi_B^{H(x)} \otimes \pi_C^{H(x)}$ and

$$M = \mathop{\mathbb{E}}_k \mathop{\mathbb{E}}_\ell \mathop{\mathbb{E}}_H \left\|\left(|x\rangle\langle x|_{B_Q} \otimes |x\rangle\langle x|_{C_Q}\right)\left(\left(U_B O_B^H\right)^k \otimes \left(U_C O_C^H\right)^\ell\right)|\psi\rangle\right\|^2 \tag{46}$$

with $k \in \{0, \ldots, q_B - 1\}$, $\ell \in \{0, \ldots, q_C - 1\}$, and $H \in \mathrm{Bool}(\lambda, n)$.

Proof. For $L \in \{B, C\}$, we define $P_L = |x\rangle\langle x|_{L_Q}$. Using Lemma 17 and the fact that $U_L O_L^H = U_L O_L^H P_L + U_L O_L^H (\mathbb{1} - P_L)$, we have that

$$\begin{aligned}\left(U_L O_L^H\right)^{q_L} = &\overbrace{\left(U_L O_L^H \left(\mathbb{1} - P_L\right)\right)^{q_L}}^{=V_L^H} + \\ &\sum_{k=0}^{q_L-1} \underbrace{\left(U_L O^H \left(\mathbb{1} - P_L\right)\right)^{q_L-k-1} U_L O_L^H P_L \left(U_L O_L^H\right)^k}_{=W_L^{H,k}}\end{aligned} \tag{47}$$

and we define $W_L^H = \sum_{k=0}^{q_L-1} W_L^{H,k}$. This implies that

$$\begin{aligned}&\left\|\Pi^{H(x)} \left(\left(U_B O_B^H\right)^{q_B} \otimes \left(U_C O_C^H\right)^{q_C}\right) |\psi\rangle\right\|^2 \\ &= \left\|\Pi^{H(x)} \left(\left(O_B O_B^H\right)^{q_B} \otimes V_C^H + V_B^H \otimes W_C^H + W_B^H \otimes W_C^H\right) |\psi\rangle\right\|^2.\end{aligned} \tag{48}$$

We now claim that contribution from the $W_B^H \otimes W_C^H$ operator corresponds to the M in the upper bound provided in the statement. Indeed, using Lemma 18, the definition of the various W operators, and properties of the operator norm on projectors and unitary operators, we have that

$$\begin{aligned}&\left\|\Pi^{H(x)} \left(\left(O_B O_B^H\right)^{q_B} \otimes V_C^H + V_B^H \otimes W_C^H + W_B^H \otimes W_C^H\right) |\psi\rangle\right\|^2 \\ &\leq \left\|\Pi^{H(x)} \left(\left(O_B O_B^H\right)^{q_B} \otimes V_C^H + V_B^H \otimes W_C^H\right) |\psi\rangle\right\|^2 \\ &\quad + (3q_B q_C + 2) q_B q_C \mathop{\mathbb{E}}_k \mathop{\mathbb{E}}_\ell \left\|(P_B \otimes P_C) \left(\left(U_B O_B^H\right)^k \otimes \left(U_C O_C^H\right)^\ell\right) |\psi\rangle\right\|.\end{aligned} \tag{49}$$

Using Jensen's inequality, the above inequality and the definition of M, we have that

$$\begin{aligned}&\mathop{\mathbb{E}}_H \left\|\Pi^{H(x)} \left(\left(O_B O_B^H\right)^{q_B} \otimes V_C^H + V_B^H \otimes W_C^H + W_B^H \otimes W_C^H\right) |\psi\rangle\right\|^2 \\ &\leq \mathop{\mathbb{E}}_H \left\|\Pi^{H(x)} \left(\left(O_B O_B^H\right)^{q_B} \otimes V_C^H + V_B^H \otimes W_C^H\right) |\psi\rangle\right\|^2 + (3q_B q_C + 2) q_B q_C \sqrt{M}.\end{aligned} \tag{50}$$

It now suffices to show that

$$\mathop{\mathbb{E}}_H \left\|\Pi^{H(x)} \left(\left(O_B O_B^H\right)^{q_B} \otimes V_C^H + V_B^H \otimes W_C^H\right) |\psi\rangle\right\|^2 \leq \frac{9}{2^n}. \tag{51}$$

By Lemma 19, this is equivalent to showing that

$$\mathop{\mathbb{E}}_H \mathop{\mathbb{E}}_y \left\|\Pi^y \left(\left(U_B O_B^{H_{x,y}}\right)^{q_B} \otimes V_C^{H_{x,y}} + V_B^{H_{x,y}} \otimes W_C^{H_{x,y}}\right) |\psi\rangle\right\|^2 \leq \frac{9}{2^n} \tag{52}$$

In fact, it will be sufficient to show that for any particular H, the expectation over y is bounded by $9 \cdot 2^{-n}$. If, for any H, we define

$$\alpha = \mathop{\mathbb{E}}_{y} \left\| \Pi^y \left(\left(U_B O_B^{H_{x,y}} \right) \otimes V_C^{H_{x,y}} \right) |\psi\rangle \right\|^2 \tag{53}$$

and

$$\beta = \mathop{\mathbb{E}}_{y} \left\| \Pi^y \left(V_B^{H_{x,y}} \otimes W_C^{H_{x,y}} \right) |\psi\rangle \right\|^2 \tag{54}$$

then, using the triangle inequality and the fact that the operators in $\{\Pi^y\}_{y\in\{0,1\}^n}$ project on mutually orthogonal subspaces, we have that

$$\mathop{\mathbb{E}}_{y} \left\| \Pi^y \left(\left(O_B O_B^{H_{x,y}} \right)^{q_B} \otimes V_C^{H_{x,y}} + V_B^{H_{x,y}} \otimes W_C^{H_{x,y}} \right) |\psi\rangle \right\|^2 \leq \alpha + \beta + 2\sqrt{\alpha\beta}. \tag{55}$$

Now, noting that $V_B^{H_{x,y}}$ and $V_C^{H_{x,y}}$ do not depend on the value of y, as they always project on a subspace which does not query the oracle H on x, and using properties of the operator norm, we have that

$$\begin{aligned}
\alpha &= \mathop{\mathbb{E}}_{y} \left\| \Pi^y \left(\left(U_B O_B^{H_{x,y}} \right) \otimes V_C^{H_{x,y}} \right) |\psi\rangle \right\|^2 && (56)\\
&\leq \mathop{\mathbb{E}}_{y} \left\| \left(\mathbb{1}_B \otimes \pi_C^y \right) \left(\mathbb{1}_B \otimes V_C^{H_{x,y}} \right) |\psi\rangle \right\|^2 && (57)\\
&= \frac{1}{2^n} \left\| \left(\mathbb{1}_B \otimes V_C^H \right) |\psi\rangle \right\|^2 \leq \frac{1}{2^n}. && (58)
\end{aligned}$$

A similar reasoning yields that $\beta \leq 4 \cdot 2^{-n}$, where the 4 is a result of squaring the upper bound

$$\left\| W_C^{H_{x,y}} \right\| \leq \left\| \left(U_C O_C^{H_{x,y}} \right)^{q_C} \right\| + \left\| V_C^{H_{x,y}} \right\| \leq 2. \tag{59}$$

Finally, noting that $\alpha + \beta + 2\sqrt{\alpha\beta} \leq 9 \cdot 2^{-n}$ finishes the proof. □

4.4 Main Results

We now have all the necessary tools to prove our main results.

Theorem 22.
Let $\mathcal{S}$ be the QECM scheme defined in Definition 16. If the qPRF is modeled by a quantum oracle, then $\mathcal{S}$ is $\log_2(9)$-uncloneable secure.

When we say that we model a qPRF as a quantum oracle, we mean that we model the adversaries' evaluations of the qPRF as queries to an oracle. Specifically, if the key used in the encryption was (s, θ), we assume that the adversaries do not receive s when the key is broadcasted, but rather that they receive quantum oracle access to the function $f_\lambda(s, \cdot)$. Essentially, we are assuming that the adversaries only use s to compute the function $f_\lambda(s, \cdot)$ and that they treat it as a black box. Recall that we indicate that a circuit has oracle access to a function by placing this function in superscript to the circuit and its CPTP map.

Proof. Let $\mathcal{A} = (\mathtt{A}, \mathtt{B}, \mathtt{C})$ be a cloning attack against $\mathcal{S}$ as described in Definition 7. We need to show that the probability that the adversaries can simultaneously guess a message chosen uniformly at random is upper bounded by $9 \cdot 2^{-n} + \eta(\lambda)$ for a negligible function η. Furthermore, since the adversaries treat the qPRF as an oracle, it suffices to show that their winning probability is upper bounded by $9 \cdot 2^{-n} + \eta(\lambda)$ when averaged over all functions in $\mathrm{Bool}(\lambda, n)$ and not only the functions $\{f_\lambda(s,\cdot)\}_{s\in\{0,1\}^\lambda}$. Indeed, by definition of a qPRF, their winning probability in both cases can only differ by a negligible function of λ.

The remainder of the proof is an application of Lemma 21 followed by application of Corollary 2.

Accounting for the randomness of the encryption and for a fixed and implicit λ, the quantity we wish to bound is then given by

$$\omega = \mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{\theta}\mathop{\mathbb{E}}_{x}\mathop{\mathbb{E}}_{m} \mathrm{Tr}\left[P^m \left(B_\theta^H \otimes C_\theta^H\right) \circ A\left(|m \oplus H(x)\rangle\langle m \oplus H(x)| \otimes \left|x^\theta\right\rangle\left\langle x^\theta\right|\right)\right] \tag{60}$$

where $P^m = |m\rangle\langle m| \otimes |m\rangle\langle m|$ and $H \in \mathrm{Bool}(\lambda, n)$. Then, by using Lemma 14 with respect to the expectation over m to move the dependence on the string $H(x)$ from the state to the projector, we have that

$$\omega = \mathop{\mathbb{E}}_{H}\mathop{\mathbb{E}}_{\theta}\mathop{\mathbb{E}}_{x}\mathop{\mathbb{E}}_{m} \mathrm{Tr}\left[P^{m\oplus H(x)} \left(B_\theta^H \otimes C_\theta^H\right) \circ A\left(|m\rangle\langle m| \otimes \left|x^\theta\right\rangle\left\langle x^\theta\right|\right)\right]. \tag{61}$$

Using standard purification arguments, we add auxiliary states $|\text{aux-B}\rangle\langle\text{aux-B}|$ and $|\text{aux-C}\rangle\langle\text{aux-C}|$ to the state $A(|m\rangle\langle m| \otimes \left|x^\theta\right\rangle\left\langle x^\theta\right|)$, replace the CPTP maps B_θ^H and C_θ^H by unitary operators on the resulting larger Hilbert spaces and similarly replace the projectors $|m\rangle\langle m|$ by projectors $\{\pi_B^m\}_{m\in\{0,1\}^n}$ and $\{\pi_C^m\}_{m\in\{0,1\}^n}$ on these larger Hilbert spaces.

Following [BDF+11], these purified unitary operators will be of the form $\left(U_L^\theta O_L^H\right)^{q_L}$, acting on a Hilbert space of the form $\mathcal{Q}(\lambda)_{L_Q} \otimes \mathcal{Q}(n)_{L_R} \otimes \mathcal{Q}(s_L)_{L_S}$ for some $q_L, s_L \in \mathbb{N}^+$ as they model oracle computations. In particular, we note that q_L represents the number of queries made to the oracle by that particular party. We also assume that

$$\begin{aligned}\rho^{m,x,\theta} &= A(|m\rangle\langle m| \otimes \left|x^\theta\right\rangle\left\langle x^\theta\right|) \otimes |\text{aux-B}\rangle\langle\text{aux-B}| \otimes |\text{aux-C}\rangle\langle\text{aux-C}| \\ &\in \mathcal{D}(\mathcal{Q}(\lambda)_{B_Q} \otimes \mathcal{Q}(n)_{B_R} \otimes \mathcal{Q}(s_B)_{B_S} \otimes \mathcal{Q}(\lambda)_{C_Q} \otimes \mathcal{Q}(n)_{C_R} \otimes \mathcal{Q}(s_C)_{C_S}).\end{aligned} \tag{62}$$

Finally, we can write $\rho^{m,x,\theta}$ as an ensemble of pure states, which is to say that

$$\rho^{m,x,\theta} = \sum_{i\in I^{m,x,\theta}} p_i \left|\psi_i^{m,x,\theta}\right\rangle\left\langle\psi_i^{m,x,\theta}\right| \tag{63}$$

for some index set $I^{m,x,\theta}$, some non-zero p_i which sum to 1, and some unit vectors $\left|\psi_i^{m,x,\theta}\right\rangle$. It then follows that ω can be expressed as

$$\mathop{\mathbb{E}}_{m}\mathop{\mathbb{E}}_{\theta}\mathop{\mathbb{E}}_{x}\mathop{\mathbb{E}}_{H} \sum_{i\in I^{m,x,\theta}} p_i \left\| \left(\pi_B^{m\oplus H(x)} \otimes \pi_C^{m\oplus H(x)}\right) \left(\left(U_B^\theta O_B^H\right)^{q_B} \otimes \left(U_C^\theta O_C^H\right)^{q_C}\right) \left|\psi_i^{m,x,\theta}\right\rangle \right\|^2. \tag{64}$$

Noting that we can bring the expectation with respect to H into the summation, we can then use Lemma 21 to upper bound ω by

$$\frac{9}{2^n} + q \mathop{\mathbb{E}}_{m} \mathop{\mathbb{E}}_{\theta} \mathop{\mathbb{E}}_{x} \sum_{i \in I^{m,x,\theta}} p_i \sqrt{\mathop{\mathbb{E}}_{H} \mathop{\mathbb{E}}_{k} \mathop{\mathbb{E}}_{\ell} \left\| Q_x \left(\left(U_B O_B^H \right)^{q_B} \otimes \left(U_C O_C^H \right)^{q_C} \right) \left| \psi_i^{m,x,\theta} \right\rangle \right\|^2} \tag{65}$$

where $q = (3q_Bq_C + 2)q_Bq_C$ and $Q_x = |x\rangle\langle x|_{Q_B} \otimes |x\rangle\langle x|_{Q_C}$. Defining

$$\beta_x^{\theta,H,k} = \left(\left(U_B^\theta O_B^H \right)^{q_B} \right)^\dagger |x\rangle\langle x|_{Q_B} \left(\left(U_B^\theta O_B^H \right)^{q_B} \right), \tag{66}$$

and similarly for $\gamma_x^{\theta,H,\ell}$ by replacing every instance of B with C, we use Jensen's lemma to bring the remaining expectations and sums into the square root and obtain

$$\omega = \frac{9}{2^n} + q \sqrt{\mathop{\mathbb{E}}_{m} \mathop{\mathbb{E}}_{\theta} \mathop{\mathbb{E}}_{x} \mathop{\mathbb{E}}_{H} \mathop{\mathbb{E}}_{k} \mathop{\mathbb{E}}_{\ell} \operatorname{Tr} \left[\left(\beta_x^{\theta,H,k} \otimes \gamma^{\theta,H,k} \right) \rho^{m,x,\theta} \right]}. \tag{67}$$

Letting Φ_m to be the CPTP map defined by

$$\rho \mapsto A \left(|m\rangle\langle m| \otimes \rho \right) \otimes |\text{aux-B}\rangle\langle\text{aux-B}| \otimes |\text{aux-C}\rangle\langle\text{aux-C}| \tag{68}$$

we see that, for any fixed H, k, ℓ, and m, Corollary 2 implies that

$$\mathop{\mathbb{E}}_{x} \mathop{\mathbb{E}}_{\theta} \operatorname{Tr} \left[\left(\beta_x^{\theta,H,k} \otimes \gamma^{\theta,H,k} \right) \rho^{m,x,\theta} \right] \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}} \right)^\lambda \tag{69}$$

since $\rho^{m,x,\theta} = \Phi_m \left(|x^\theta\rangle\langle x^\theta| \right)$. Thus,

$$\omega \leq \frac{9}{2^n} + q \left(\sqrt{\frac{1}{2} + \frac{1}{2\sqrt{2}}} \right)^\lambda. \tag{70}$$

Finally, since `B` and `C` are efficient quantum circuits, they may query the oracle a number of time which grows at most polynomially in λ. Thus, $q \leq p(\lambda)$ for some polynomial p. Noting that $\lambda \mapsto p(\lambda) \cdot \left(\sqrt{\frac{1}{2} + \frac{1}{2\sqrt{2}}} \right)^\lambda$ is a negligible function completes the proof. □

We can strengthen this result if the adversaries do not share any entanglement.

Theorem 23.
Let $\mathcal{S}$ be the QECM scheme given in Definition 16. If the qPRF is modeled by a quantum oracle and the adversaries cannot share any entanglement, then $\mathcal{S}$ is 0-uncloneable secure.

Proof (Sketch). Follow the proof of Theorem 22 using the bound given by Lemma 20, instead of Lemma 21, in the step corresponding to Eq. (65). □

Corollary 24.
Let $\mathcal{S}$ be the QECM scheme given in Definition 16 with constant message size, i.e.: $n(\lambda) = n$. If the qPRF is modeled by a quantum oracle and the adversaries cannot share any entanglement, then $\mathcal{S}$ is indistinguishable-uncloneable secure.

Proof (Sketch). Use Theorem 23 with Theorem 12. □

Acknowledgments

This material is based upon work 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.

References

[Aar09] S. Aaronson. Quantum copy-protection and quantum money. In *24th Annual Conference on Computational Complexity—CCC 2009*, pages 229–242, 2009.
DOI: 10.1109/CCC.2009.42.

[ABF+16] G. Alagic, A. Broadbent, B. Fefferman, T. Gagliardoni, C. Schaffner, and M. St. Jules. Computational security of quantum encryption. In *Information Theoretic Security: 9th International Conference—ICITS 2016*, pages 47–71, 2016.
DOI: 10.1007/978-3-319-49175-2_3.

[AC12] S. Aaronson and P. Christiano. Quantum money from hidden subspaces. In *44th Annual ACM Symposium on Theory of Computing—STOC 2012*, pages 41–60, 2012.
DOI: 10.1145/2213977.2213983.

[AKN98] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *30th Annual ACM Symposium on Theory of Computing—STOC 1998*, pages 20–30, 1998.
DOI: 10.1145/276698.276708.

[Bar16] E. Barker. Recommendation for key management part 1: General (revision 4). Technical Report SP 800-57, National Institute of Standards and Technology, 2016.
DOI: 10.6028/NIST.SP.800-57pt1r4.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[BBB14] C. H. Bennett, G. Brassard, and S. Breidbart. Quantum cryptography II: How to re-use a one-time pad safely even if P=NP. *Natural Computing*, 13(4): 453–458, 2014.
DOI: 10.1007/s11047-014-9453-6.

[BBC+01] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48(4): 778–797, 2001.
DOI: 10.1145/502090.502097.

[BDF+11] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In *Advances in Cryptology—ASIACRYPT 2011*, pages 41–69, 2011.
DOI: 10.1007/978-3-642-25385-0_3.

[BS16] A. Broadbent and C. Schaffner. Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography*, 78(1): 351–382, 2016.
DOI: 10.1007/s10623-015-0157-4.

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

[DPS05] I. Damgård, T. B. Pedersen, and L. Salvail. A quantum cipher with near optimal key-recycling. In *Advances in Cryptology—CRYPTO 2005*, pages 494–510, 2005.
DOI: 10.1007/11535218_30.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review Letters*, 47(10): 777–780, 1935.
DOI: 10.1103/physrev.47.777.

[FS17] S. Fehr and L. Salvail. Quantum authentication and encryption with key recycling. In *Advances in Cryptology—EUROCRYPT 2017*, pages 311–338, 2017.
DOI: 10.1007/978-3-319-56617-7_11.

[GM84] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2): 270–299, 1984.
DOI: 10.1016/0022-0000(84)90070-9.

[Got03] D. Gottesman. Uncloneable encryption. *Quantum Information & Computation*, 3(6): 581–602, 2003.

[Lor19] S. Lord. Uncloneable quantum encryption via random oracles. Master's thesis, University of Ottawa, 2019.
DOI: 10.20381/ruor-23107.

[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.

[SP00] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2): 441–444, 2000.
DOI: 10.1103/physrevlett.85.441.

[TFKW13] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10): 103002, 2013.
DOI: 10.1088/1367-2630/15/10/103002.

[Unr15] D. Unruh. Revocable quantum timed-release encryption. *Journal of the ACM*, 62(6): 49, 2015.
DOI: 10.1145/2817206.

[Wat09] J. Watrous. Quantum computational complexity. In *Encyclopedia of complexity and systems science*, pages 7174–7201. Springer, 2009.
DOI: 10.1007/978-3-642-27737-5_428-3.

[Wat18] J. Watrous. *The Theory of Quantum Information*. Cambridge University Press, 1st edition, 2018.

[Wie83] S. Wiesner. Conjugate coding. *ACM SIGACT News*, 15(1): 78–88, 1983.
DOI: 10.1145/1008908.1008920.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299: 802–803, 1982.
DOI: 10.1038/299802a0.

[Zha12] M. Zhandry. How to construct quantum random functions. In *53rd Annual Symposium on Foundations of Computer Science—FOCS 2012*, pages 679–687, 2012.
DOI: 10.1109/FOCS.2012.37.

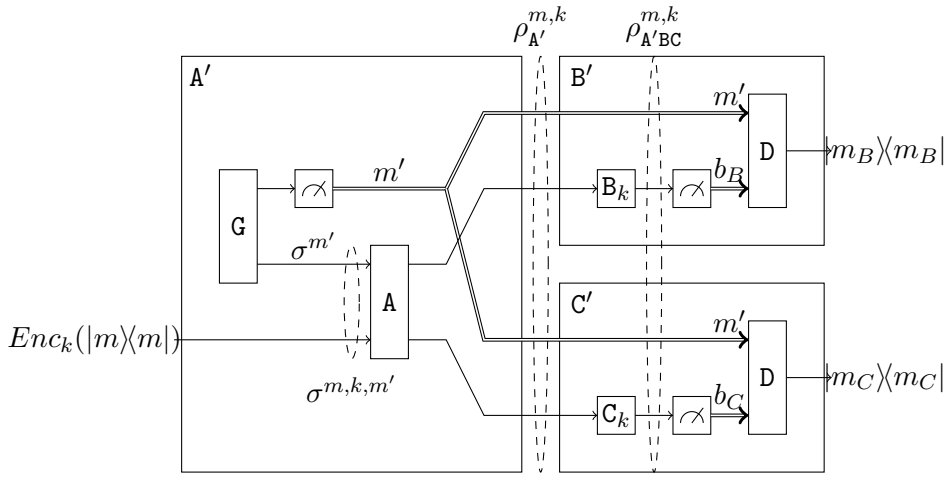

Figure 4: A cloning-distinguishing attack $\mathcal{A} = (\mathtt{G}, \mathtt{A}, \mathtt{B}, \mathtt{C})$ is used to construct a cloning attack $\mathcal{A}' = (\mathtt{A}', \mathtt{B}', \mathtt{C}')$. The $\mathtt{D}$ circuit outputs $|0^n\rangle\langle 0^n|$ if $b = 0$ and $|m'\rangle\langle m'|$ if $b = 1$.

A Technical Proofs

Proof (Theorem 12). Let $\mathcal{S}$ be a 0-uncloneable secure QECM scheme with constant message size, i.e.: $n(\lambda) = n$. Let $\mathcal{A} = (\mathtt{G}, \mathtt{A}, \mathtt{B}, \mathtt{C})$ be a cloning-distinguishing attack against $\mathcal{S}$. We will construct a cloning attack $\mathcal{A}' = (\mathtt{A}', \mathtt{B}', \mathtt{C}')$ and show that the winning probability of $\mathcal{A}$ is at most 2^{n-1} times the winning probability of $\mathcal{A}'$. Since $\mathcal{S}$ is uncloneable secure, $\mathcal{A}'$'s winning probability is bounded by $2^{-n} + \eta(\lambda)$, which is sufficient to prove this theorem.

We now describe the circuits in the $\mathcal{A}'$ attack. A schematic representation of this construction is given in Fig. 4.

$\mathtt{A}'$: Run $\mathtt{G}$ from $\mathcal{A}$ and obtain the state $G(1) \in \mathcal{D}(\mathcal{H}_S \otimes \mathcal{H}_M)$. Measure the M register in the computational basis and call the result m'. Discard the register M and keep the register S. Then, run $\mathtt{A}$ from $\mathcal{A}$ on the state received as input and the state that was kept in the register S. In addition, give a copy of m' to both $\mathtt{B}'$ and $\mathtt{C}'$.

$\mathtt{B}'$: Run $\mathtt{B}$ from $\mathcal{A}$ on the state obtained from $\mathtt{A}'$ and the encryption key. Measure the output in the computational basis and if the result is 0, output $|0^n\rangle\langle 0^n|$. If the result is 1, output the $|m'\rangle\langle m'|$ from the string which was given by $\mathtt{A}'$.

$\mathtt{C}'$: Analogous to $\mathtt{B}'$.

We want to obtain a description of the overall state up to the point immediately after the $\mathtt{B}$ and $\mathtt{C}$ circuits are applied by $\mathtt{B}'$ and $\mathtt{C}'$. Conditioned on the message m

being encrypted with the key k, we will denote this state by $\rho^{m,k}_{\mathtt{A'BC}}$. From this state, we will be able to determine the winning probability of $\mathcal{A}'$.

Note that $\mathtt{A}'$'s first step is to obtain $G(1)$ and measure the M register in the computational basis. We define $p_{m'} = \mathrm{Tr}\left[(I_S \otimes |m'\rangle\langle m'|_M)G(1)\right]$ to be the probability that m' is measured and

$$\sigma^{m'} = \mathrm{Tr}_M \left[\frac{(I_S \otimes |m'\rangle\langle m'|_M)G(1)(I_S \otimes |m'\rangle\langle m'|_M)}{p_{m'}} \right] \tag{71}$$

to be the post measurement state conditioned on this result and after tracing out the M register. Defining

$$\sigma^{m,k,m'} = \sigma_{m'} \otimes Enc_k(|m\rangle\langle m|) \tag{72}$$

allows us to write the output state of $\mathtt{A}'$, conditioned on m being originally encrypted with the key k, as

$$\rho^{m,k}_{\mathtt{A}'} = \sum_{m' \in \{0,1\}^n} p_{m'} A(\sigma^{m,k,m'}) \otimes \left|m'\right\rangle\!\left\langle m'\right| \otimes \left|m'\right\rangle\!\left\langle m'\right|. \tag{73}$$

Thus, we have that

$$\rho^{m,k}_{\mathtt{A'BC}} = \sum_{m' \in \{0,1\}^n} p_{m'} (B_k \otimes C_k) \circ A(\sigma^{m,k,m'}) \otimes \left|m'\right\rangle\!\left\langle m'\right| \otimes \left|m'\right\rangle\!\left\langle m'\right|. \tag{74}$$

To compute $\mathcal{A}'$'s winning probability on message m and key k, we define

$$q_{m,k} = \mathrm{Tr}\left[(|1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes |m\rangle\langle m| \otimes |m\rangle\langle m|)\rho^{m,k}_{\mathtt{A'BC}} \right] \tag{75}$$

$$= p_m \,\mathrm{Tr}\left[(|1\rangle\langle 1| \otimes |1\rangle\langle 1|)(B \otimes C) \circ A(\sigma^{m,k,m}) \right] \tag{76}$$

and note that if $m \neq 0^n$, then $\mathcal{A}'$'s winning probability is given by q_m. If $m = 0^n$, we must also account for the possibility that the measurements after the $\mathtt{B}$ and $\mathtt{C}$ circuits both output 0. Thus, $\mathcal{A}'$'s winning probability in this case is at least

$$q_{0^n,k} + \mathrm{Tr}\left[(|0\rangle\langle 0| \otimes |0\rangle\langle 0|) \left((B_k \otimes C_k) \circ A \left(\sum_{m' \in \{0,1\}^n} p_{m'} \sigma^{0^n,k,m'} \right) \right) \right] \tag{77}$$

as we ignore any winning scenarios where the measurement results are different.

We then have that $\mathcal{A}'$'s winning probability is at least

$$\mathop{\mathbb{E}}_{k \leftarrow \mathcal{K}} \frac{1}{2^n} \left(\sum_{m \in \{0,1\}^n} q_{m,k} + \mathrm{Tr}\left[(|0\rangle\langle 0| \otimes |0\rangle\langle 0|) \left((B_k \otimes C_k) \circ A\left(\sigma^{0^n,k} \right) \right) \right] \right) \tag{78}$$

where $\sigma^{0^n,k} = \sum_{m' \in \{0,1\}^n} p_{m'} \sigma^{0^n,k,m'}$. Since $\mathcal{S}$ is uncloneable secure, there exists a negligible function η such that Eq. (78) is upper bounded by $2^{-n} + \eta(\lambda)$. This implies that

$$\mathop{\mathbb{E}}_{k \leftarrow \mathcal{K}} \frac{1}{2} \left(\sum_{m \in \{0,1\}^n} q_{m,k} + \operatorname{Tr}\left[\left(|0\rangle\langle 0| \otimes |0\rangle\langle 0| \right) \left((B_k \otimes C_k) \circ A\left(\sigma^{0^n,k} \right) \right) \right] \right) \tag{79}$$

is upper bounded by $\frac{1}{2} + 2^{n-1}\eta(\lambda)$. Noting that Eq. (79) is precisely $\mathcal{A}$'s winning probability and that $\lambda \mapsto 2^{n-1}\eta(\lambda)$ is negligible completes the proof. □

Proof (Corollary 2). It suffices to apply Theorem 1 with the state

$$\rho = \left(\mathbb{1}_A \otimes \Phi_{A'} \right) |\mathrm{EPR}_\lambda\rangle\langle \mathrm{EPR}_\lambda|_{AA'} = \frac{1}{2^\lambda} \sum_{r,s \in \{0,1\}^\lambda} |r\rangle\langle s| \otimes \Phi\left(|r\rangle\langle s| \right), \tag{80}$$

which is the result of applying the map Φ to the second half of λ EPR pairs. Note that for all $\theta \in \{0,1\}^\lambda$ we have that

$$\frac{1}{2^\lambda} \sum_{r,s \in \{0,1\}^\lambda} |r\rangle\langle s| \otimes \Phi\left(|r\rangle\langle s| \right) = \frac{1}{2^\lambda} \sum_{r,s \in \{0,1\}^\lambda} \left| r^\theta \right\rangle\!\left\langle s^\theta \right| \otimes \Phi\left(\left| r^\theta \right\rangle\!\left\langle s^\theta \right| \right). \tag{81}$$

We then have that

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\theta} \sum_{x \in \{0,1\}^\lambda} \operatorname{Tr}\left[\left(\left| x^\theta \right\rangle\!\left\langle x^\theta \right| \otimes B_x^\theta \otimes C_x^\theta \right) \rho \right] \\
&= \mathop{\mathbb{E}}_{\theta} \frac{1}{2^\lambda} \sum_{x,r,s \in \{0,1\}^\lambda} \operatorname{Tr}\left[\left(\left| x^\theta \right\rangle\!\left\langle x^\theta \right| \otimes B_x^\theta \otimes C_x^\theta \right) \left(\left| r^\theta \right\rangle\!\left\langle s^\theta \right| \otimes \Phi\left(\left| r^\theta \right\rangle\!\left\langle s^\theta \right| \right) \right) \right] \\
&= \mathop{\mathbb{E}}_{\theta} \frac{1}{2^\lambda} \sum_{x \in \{0,1\}^\lambda} \operatorname{Tr}\left[\left(B_x^\theta \otimes C_x^\theta \right) \Phi\left(\left| x^\theta \right\rangle\!\left\langle x^\theta \right| \right) \right].
\end{aligned} \tag{82}$$

Thus the bound given in Theorem 1 is directly applicable. □

Proof (Lemma 14). Recall that for any fixed string $s \in \{0,1\}^n$, the map $x \mapsto x \oplus s$ is a permutation which is its own inverse. If we define the map $g : \{0,1\}^n \to \mathbb{R}$ by $x \mapsto f(x, x \oplus s)$, we then have that

$$\mathop{\mathbb{E}}_{x} f(x, x \oplus s) = \mathop{\mathbb{E}}_{x} g(x) = \mathop{\mathbb{E}}_{x} g(x \oplus s) = \mathop{\mathbb{E}}_{x} f(x \oplus s, x) \tag{83}$$

which concludes the proof. □

Proof (Lemma 17). Proceed by induction over n noting that

$$\left(a^n + \sum_{k=0}^{n-1} a^{n-k-1} b c^k \right) c = a^{n+1} + \sum_{k=0}^{(n+1)-1} a^{(n+1)-k-1} b c^k. \tag{84}$$

□

Proof (Lemma 18). We first note that $\|v_0\| \leq \|\sum_{i=0}^{n} v_i\| + \sum_{i=1}^{n} \|v_i\| \leq 1+n$. Then, using the triangle inequality, we have that

$$\left\| \sum_{i=0}^{n} v_i \right\|^2 \leq \left(\sum_{i=0}^{n} \|v_i\| \right)^2 = \sum_{i=0}^{n} \sum_{j=0}^{n} \|v_i\| \cdot \|v_j\|. \tag{85}$$

We consider the summands in the right hand side differently depending on the value of i. If $i = 0$, we note that

$$\sum_{j=0}^{n} \|v_0\| \cdot \|v_j\| \leq \|v_0\|^2 + (n+1) \sum_{j=1}^{n} \|v_j\|. \tag{86}$$

If $i \neq 1$, we note that

$$\sum_{j=0}^{n} \|v_i\| \cdot \|v_j\| \leq \|v_i\| \sum_{j=0}^{n} \|v_j\| \leq ((n+1)+n) \|v_i\|. \tag{87}$$

We obtain the result by adding each of these bounds. □