# On the Feasibility of Unclonable Encryption, and More

Prabhanjan Ananth[1], Fatih Kaleoglu[2] Xingjian Li[2], Qipeng Liu[3], and Mark Zhandry[4]

[1] University of California, Santa Barbara, CA, USA
prabhanjan@cs.ucsb.edu,
WWW home page: http://users/~iekeland/web/welcome.html
[2] University of Claifornia, Santa Barbara, CA, USA
kaleoglu@ucsb.edu
[3] Tsinghua University, Beijing, China
lixj18@mails.tsinghua.edu.cn
[4] Simons Institute for the Theory of Computing, CA, USA
qipengliu0@gmail.com
[5] NTT Research & Princeton University, NJ, USA
mzhandry@gmail.com

**Abstract.** Unclonable encryption, first introduced by Broadbent and Lord (TQC'20), is a one-time encryption scheme with the following security guarantee: any non-local adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ cannot simultaneously distinguish encryptions of two equal length messages. This notion is termed as unclonable indistinguishability. Prior works focused on achieving a weaker notion of unclonable encryption, where we required that any non-local adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ cannot simultaneously recover the entire message $m$. Seemingly innocuous, understanding the feasibility of encryption schemes satisfying unclonable indistinguishability (even for 1-bit messages) has remained elusive.

We make progress towards establishing the feasibility of unclonable encryption.

- We show that encryption schemes satisfying unclonable indistinguishability exist unconditionally in the quantum random oracle model.
- Towards understanding the necessity of oracles, we present a negative result stipulating that a large class of encryption schemes cannot satisfy unclonable indistinguishability.
- Finally, we also establish the feasibility of another closely related primitive: copy-protection for single-bit output point functions. Prior works only established the feasibility of copy-protection for multi-bit output point functions or they achieved constant security error for single-bit output point functions.

## 1 Introduction

Quantum information ushers in a new era for cryptography. Cryptographic constructs that are impossible to achieve classically can be realized using quantum information. In particular, the no-cloning principle of quantum mechanics has given rise to many wonderful primitives such as quantum money [24]

and its variants [2, 25, 18], tamper detection [14], quantum copy-protection [1], one-shot signatures [4], single-decryptor encryption [13, 10], secure software leasing [6], copy-detection [3] and many more.

*Unclonable Encryption.* Of particular interest is a primitive called unclonable encryption, introduced by Broadbent and Lord [9]. Roughly speaking, unclonable encryption is a one-time secure encryption scheme with *quantum* ciphertexts having the following security guarantee: any adversary given a ciphertext, modeled as a quantum state, cannot produce two (possibly entangled) states that both encode some information about the original message. This is formalized in terms of a splitting game.

A splitting adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ first has $\mathcal{A}$ receive as input an encryption of $m_b$, for two messages $m_0$ and $m_1$. $\mathcal{A}$ then outputs a bipartite state to $\mathcal{B}$ and $\mathcal{C}$. $\mathcal{B}$ and $\mathcal{C}$ additionally receive as input the classical decryption key and respectively output $b_B$ and $b_C$. They win if $b = b_B = b_C$. Clearly, $\mathcal{A}$ could give $\mathcal{B}$ the entire ciphertext and $\mathcal{C}$ nothing, in which case $b_B = b$ but $b_C$ would be independent of $b$, giving an overall winning probability of $1/2$. Security therefore requires that the splitting adversary wins with probability only negligibly larger than $1/2$. This security property, introduced by [9], is called *unclonable indistinguishability*. Unclonable indistinguishability clearly implies plain semantic security, as $\mathcal{A}$ could use any semantic security adversary to make a guess $b_A$ for $b$, and then simply send $b_A$ to $\mathcal{B}$ and $\mathcal{C}$, who set $b_B = b_C := b_A$.

Unclonable encryption is motivated by a few interesting applications. Firstly, unclonable encryption implies private-key quantum money. It is also useful for preventing storage attacks where malicious entities steal ciphertexts in the hope that they can decrypt them when the decryption key is compromised later. Recently, the works of [11, 5] showed that unclonable encryption implies copy-protection for a restricted class of functions with computational correctness guarantees.

Despite being a natural primitive, actually constructing unclonable encryption (even for 1-bit messages!) and justifying its security has remained elusive. Prior works [9, 5] established the feasibility of unclonable encryption satisfying a weaker property simply called *unclonability*: this is modeled similar to unclonable indistinguishability, except that the message $m$ encrypted is sampled uniformly at random and both $\mathcal{B}$ and $\mathcal{C}$ are expected to guess the entire message $m$. This weaker property is far less useful, and both applications listed above – preventing storage attacks and copy-protection – crucially rely on indistinguishability security. Moreover, unclonability does not on its own even imply plain semantic security, meaning the prior works must separately posit semantic security.

The following question has been left open from prior works:

*Q1. Do encryption schemes satisfying unclonable indistinguishability, exist?*

*Copy-Protection for Point Functions.* Copy-protection, first introduced by Aaronson [1], is another important primitive closely related to unclonable encryption.

Copy-protection is a compiler that converts a program into a quantum state that not only retains the original functionality but also satisfies the following property: a splitting adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ first has $\mathcal{A}$ receive as input a copy-protected state that can be used to compute a function $f$. $\mathcal{A}$ then outputs a bipartite state to $\mathcal{B}$ and $\mathcal{C}$. As part of the security guarantee, we require that both $\mathcal{B}$ and $\mathcal{C}$ should not be able to simultaneously compute $f$.

While copy-protection is known to be impossible for general unlearnable functions [6], we could still hope to achieve it for simple classes of functions. Of particular interest to us is the class of point functions. A single-bit output point function is of the form $f_y(\cdot)$: it takes as input $x$ and outputs $1$ if and only if $x = y$. One could also consider the notion of multi-bit output point functions, where the function outputs a large string, rather than 0 or 1.

Prior works [11, 5] either focus on constructing copy-protection for *multi*-bit output point functions or they construct copy-protection for single-bit output point functions with constant security, rather than optimal security, where the adversary can only do negligibly better than a trivial guess.

Yet another important question that has been left open from prior works is the following:

> *Q2. Does copy-protection for single-bit output point functions, with optimal security, exist?*

As we will see later, the techniques used in resolving Q1 will shed light on resolving Q2. Hence, we focus on highlighting challenges in resolving Q1. The reader familiar with the challenges involved in constructing unclonable encryption could skip Section 1.1 and directly go to Section 1.2.

### 1.1 Achieving Unclonable Indistinguishability: Challenges

We need to achieve a *one-time* secure encryption scheme for *1-bit* messages satisfying unclonable indistinguishability: *how hard can this problem be?* Indeed one might be tempted to conclude that going from the weaker unclonability property to the stronger unclonable indistinguishability notion is a small step. The former is a search problem while the latter is a decision problem, and could hope to apply known search-to-decision reductions. As we will now explain, unfortunately this intuition is false, due both to the effects of quantum information and also to the fact that unclonable encryption involves multiple interacting adversaries.

- Recall that in an unclonable encryption scheme, the secret key is revealed to both $\mathcal{B}$ and $\mathcal{C}$. As a consequence, the secret information of any underlying cryptographic tool we use to build unclonable encryption could be revealed. For example, consider the following construction: to encrypt $m \in \{0,1\}$, compute $(r, \mathsf{PRF}(k, r) \oplus m)$, where $k \xleftarrow{\$} \{0,1\}^\lambda$ is the pseudorandom function key and $r \xleftarrow{\$} \{0,1\}^\lambda$ is a random tag. In the security experiment, the secret key, namely $k$, will be revealed to both $\mathcal{B}$ and $\mathcal{C}$. This restricts the type of cryptographic tools we can use to build unclonable encryption.

- Another challenge is to perform security reductions. Typically, we use the adversary to come up with a reduction that breaks a cryptographic game that is either conjectured to be or provably hard. However, this is tricky when there are two adversaries, $\mathcal{B}$ and $\mathcal{C}$. Which of the two adversaries do we use to break the underlying game? Suppose we decide to use $\mathcal{B}$ to break the game. For all we know, $\mathcal{A}$ could have simply handed over the ciphertext it received to $\mathcal{B}$ and clearly, $\mathcal{B}$ cannot be used to break the underlying game. Even worse, Alice can send a superposition of $\mathcal{B}$ getting the ciphertext and $\mathcal{C}$ receiving nothing v.s. $\mathcal{C}$ receiving the ciphertext and $\mathcal{B}$ getting nothing.
- Even if we somehow manage to achieve unclonable indistinguishability for 1-bit messages, it is a priori unclear how to achieve unclonable indistinguishability for multi-bit messages. In classical cryptography, the standard transformation goes from encryption of 1-bit messages to encryption of multi-bit messages via a hybrid argument. This type of argument fails in the setting of unclonable encryption. Let us illustrate why: suppose we encrypt a 2-bit message $m = m_1||m_2$ by encrypting 1-bit messages $m_1$ and $m_2$, denoted respectively by $\rho_1$ and $\rho_2$. This scheme is unfortunately insecure. An encryption of $11$ can be (simultaneously) distinguished from an encryption of $00$ by a non-local adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$: $\mathcal{A}$ can send $\rho_1$ to $\mathcal{B}$ and $\rho_2$ to $\mathcal{C}$. Since, both $\mathcal{B}$ and $\mathcal{C}$ receive the secret key, they can check whether the underlying message was 1 or 0.
- A recent result by Majenz, Schaffner and Tahmasbi [16] explores the difficulties in constructing unclonable encryption schemes. They show that any unclonable encryption scheme satisfying indistinguishability property needs to have ciphertexts, when represented as density matrices, with sufficiently large eigenvalues. As a consequence, it was shown that [9] did not satisfy unclonable-indistinguishability property. Any unclonable encryption scheme we come up with needs to overcome the hurdles set by [16].

We take an example below that concretely highlights some of the challenges explained above.

*Example: Issues with using Extractors.* For instance, we could hope to use randomness extractors. To encrypt a message $m$, we output $(\rho_x, c_r, \mathsf{Ext}(r, x) \oplus m)$, where $\rho_x$ is an unclonable encryption of $x$ satisfying the weaker unclonability property, $c_r$ is a classical encryption of a random seed $r$, and $\mathsf{Ext}$ is an extractor using seed $r$. The intuition for this construction is that unclonable security implies that at least one of the two parties, say $\mathcal{B}$ cannot predict $x$, and therefore $x$ has min-entropy conditioned on $\mathcal{B}$'s view. Therefore, $\mathsf{Ext}(r, x)$ extracts bits that are statistically random against $\mathcal{B}$, and thus completely hides $m$.

There are a few problems with this proposal. First, since $\mathcal{A}$ generates $\mathcal{B}$'s state and has access to the entire ciphertext, the conditional distribution of $x$ given Bob's view will depend on $c_r$. This breaks the extractor application, since it requires $r$ to be independent. One could hope to perform a hybrid argument to replace $c_r$ with a random ciphertext, but this is not possible: $\mathcal{B}$ eventually

learns the decryption key for $c_r$ and would be able to distinguish such a hybrid. This example already begins to show how the usual intuition fails.

A deeper problem is that extractor definitions deal with a single party, whereas unclonable encryption has two recipient parties. To illustrate the issue, note that it is actually *not* the case that $x$ has min-entropy against one of the parties: if $\mathcal{A}$ randomly sends the ciphertext to $\mathcal{B}$ or $\mathcal{C}$, each one of them can predict $x$ with probability $1/2$, so the min-entropy is only 1. In such a case the extractor guarantee is meaningless. Now, in this example one can condition on the message $\mathcal{A}$ sends to $\mathcal{B}, \mathcal{C}$, and once conditioned it will in fact be the case that one of the two parties has high min-entropy. But other strategies are possible which break such a conditioning argument. For example, $\mathcal{A}$ could send messages that are *superposition* v.s. $\mathcal{B}$ getting the ciphertext (and $\mathcal{C}$ nothing) v.s. $\mathcal{C}$ getting the ciphertext (and $\mathcal{B}$ nothing). By being in superposition, we can no longer condition on which party receives the ciphertext.

### 1.2 Our Results

We overcome the aforementioned challenges and make progress on addressing both questions Q1 and Q2. We start with our results on unclonable encryption before moving onto copy-protection.

*Unclonable Encryption.* For the first time, we establish the feasibility of unclonable encryption. Our result is in the quantum random oracle model. Specifically, we prove the following.

**Theorem 1 (Informal).** *There exists an unconditionally secure one-time encryption scheme satisfying unclonable indistinguishability in the quantum random oracle model.*

Our construction is simple: we make novel use of coset states considered in recent works [10]. However, our analysis is quite involved: among many other things, we make use of threshold projective implementation introduced by Zhandry [25].

A recent work [5] showed a generic transformation from one-time unclonable encryption to public-key unclonable encryption[6]. By combining the above theorem with the generic transformation of [5], we obtain a public-key unclonable encryption satisfying the unclonable indistinguishability property.

**Theorem 2 (Informal).** *Assuming the existence of post-quantum public-key encryption, there exists a post-quantum public-key encryption scheme satisfying the unclonable indistinguishability property in the quantum random oracle model.*

It is natural to understand whether we can achieve unclonable encryption in the plain model. Towards understanding this question, we show that a class of

[6] While their result demonstrates that the generic transformation preserves the unclonability property, we note that the same transformation preserves unclonable indistinguishability.

unclonable encryption schemes, that we call *deterministic* schemes, are impossible to achieve. By 'deterministic', we mean that the encryptor is a unitary $U$ and the decryptor is $U^\dagger$. Moreover, the impossibility holds even if the encryptor and the decryptor are allowed to run in exponential time!

In more detail, we show the following.

**Theorem 3 (Informal).** *There do not exist unconditionally secure deterministic one-time encryption schemes satisfying the unclonable indistinguishability property.*

In light of the fact that any classical one-time encryption scheme can be made deterministic without loss of generality[7], we find the above result to be surprising. An interesting consequence of the above result is an alternate proof that the conjugate encryption scheme of [9] does not satisfy unclonable indistiguishability[8]. This was originally proven by [16].

We can overcome the impossibility result by either devising an encryption algorithm that traces out part of the output register (in other words, performs non-unitary operations) or the encryption scheme is based on computational assumptions.

*Copy-Protection for Point Functions.* We also make progress on Q2. We show that there exists copy-protection for single-bit output functions with optimal security. Prior work by Coladangelo, Majenz and Poremba [11] achieved a copy-protection scheme for single-bit output point functions that only achieved constant security.

We show the following.

**Theorem 4 (Informal).** *There exists a copy-protection scheme for single-bit output point functions in the quantum random oracle model.*

While there are generic transformations from unclonable encryption to copy-protection for point functions explored in the prior works [11, 5], the transformations only work for multi-bit point functions. Our construction extensively makes use of the techniques for achieving unclonable encryption (Theorem 1). Our result takes a step closer in understanding the classes of functions for which the feasibility of copy-protection can be established in the plain model.

### 1.3 Organization

The rest of the paper is organized as follows. In Section 2, we cover all the necessary preliminaries, including Jordan's lemma, measuring success probability of a quantum adversary and the definitions of unclonable encryption schemes. Followed by Section 3, we recall coset states and their properties. We introduce a new game called "strengthened MOE games in the QROM" and prove

[7] We can always include the randomness used in the encryption as part of the secret key.

[8] It is easy to see why conjugate encryption of multi-bit messages is insecure. The insecurity of conjugate encryption of 1-bit messages was first established by [16] .

security in this game. This part is our main result and consists of most technique novelties. In Section 4, we build our unclonable encryption on the new property. In the final section (Section 5), we present our construction for copy-protection of single-output point functionsSimilar techniques as in Section 3 are used. Most details are omitted and can be found in the full version, as well as our impossibility result..

### 1.4 Technical Overview

*Attempts based on Wiesner States.* We start by recalling the unclonable encryption scheme proposed by Broadbent and Lord [9]. The core idea is to encrypt a message $m$ under a randomly chosen secret key $x$ and encode $x$ into an unclonable quantum state $\rho_x$. Intuitively, for any splitting adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$, there is no way for $\mathcal{A}$ to split $\rho_x$ into two quantum states, such that no-communicating $\mathcal{B}$ and $\mathcal{C}$ can both recover enough information about $x$ to decrypt $\mathsf{Enc}(x, m)$.

A well-known choice of no-cloning states is the famous Wiesner conjugate coding [24]. For a string $x = x_1 x_2 \cdots x_\lambda \in \{0,1\}^\lambda$, $\lambda$ bases are chosen uniformly at random, one for each $x_i$. Let $\theta_i$ denote the basis for $x_i$. If $\theta_i$ is 0, $x_i$ is encoded under the computational basis $\{|0\rangle, |1\rangle\}$; otherwise, $x_i$ is encoded under the Hadamard basis $\{|+\rangle, |-\rangle\}$. The conjugate coding of $x$ under basis $\theta$ is then denoted by $|x^\theta\rangle$. By knowing $\theta$, one can easily recover $x$ from the Wiesner state.

The unclonability of Wiesner conjugate coding (or Wiesner states for short) is well understood and characterized by *monogamy-of-entanglement games* (MOE games) in [20, 9]. In the same paper, Broadbent and Lord show that no strategy wins the following MOE game[9] with probability more than $0.85^\lambda$.

- A challenger samples uniformly at random $x, \theta \in \{0,1\}^\lambda$ and sends $|x^\theta\rangle$ to $\mathcal{A}$.
- $\mathcal{A}$ taking the input from the challenger, produces a bipartite state to $\mathcal{B}$ and $\mathcal{C}$.
- The non-communicating $\mathcal{B}$ and $\mathcal{C}$ then additionally receive the secret basis information $\theta$ and make a guess $x_\mathcal{B}, x_\mathcal{C}$ for $x$ respectively.
- The splitting adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ wins the game if and only if $x_\mathcal{B} = x_\mathcal{C} = x$.

**Fig. 1.** MOE Games for Wiesner States.

A natural attempt to construct unclonable encryption schemes is by composing one-time pad with Wiesner states. A secret key is the basis information $\theta \in \{0,1\}^n$. An encryption algorithm takes the secret key $\theta$ and a plaintext $m$,

[9] This is a variant of MOE games discussed in [20]. We will be using this notation throughout the paper.

it samples a $x \in \{0,1\}^n$ and outputs $m \oplus x$ together with the Wiesner conjugate coding of $x$, i.e. $|x^\theta\rangle$. However, such scheme can never satisfy unclonable indistinguishability. Recall that unclonable indistinguishability requires either $\mathcal{B}$ or $\mathcal{C}$ can not distinguish whether the ciphertext is an encryption of message $m_0$ or $m_1$. Broadbent and Lord observe that although it is hard for $\mathcal{B}$ and $\mathcal{C}$ to completely recover the message, they can still recover half of the message and hence simultaneously distinguish with probability 1.

Towards unclonable indistinguishability, they introduce a random oracle $H : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^n$ in their construction (Figure 2). If an adversary can distinguish between $m_0 \oplus H(\alpha, x)$ and $m_1 \oplus H(\alpha, x)$, it must query $H(\alpha, x)$ at some point; hence, one can extract $x$ from this adversary by measuring a random query. Following the same reasoning, one may hope to base the security (of Figure 2) on the MOE games (Figure 1), by extracting $x$ from both parties.

$\mathsf{Gen}(1^\lambda)$: on input $\lambda$, outputs uniformly random $(\alpha, \theta) \in \{0,1\}^{2\lambda}$.
$\mathsf{Enc}^H((\alpha,\theta), m)$: samples $x \in \{0,1\}^\lambda$, outputs $(|x^\theta\rangle, m \oplus H(\alpha, x))$.
$\mathsf{Dec}^H((\alpha,\theta), (|x^\theta\rangle, c))$: recovers $x$ from $|x^\theta\rangle$, outputs $c \oplus H(\alpha, x)$.

**Fig. 2.** Unclonable Encryption by Broadbent and Lord.

The above idea, thought intuitive, is hard to instantiate. It will require simultaneous extraction of the secret $x$ from both $\mathcal{B}$ and $\mathcal{C}$. Since $\mathcal{B}$ and $\mathcal{C}$ can be highly entangled with each other, a successful extraction of $x$ on $\mathcal{B}$'s register may always result in an extraction failure on the other register. Broadbent and Lord use a "simultaneous" variant of the so called "O2H" (one-way-to-hiding) lemma [21] to prove their scheme satisfy unclonable indistinguishability for unentangled adversaries $\mathcal{B}, \mathcal{C}$, or for messages with constant length. The unclonable indistinguishability for general adversaries and message spaces remains quite unknown.

Even worse, Majenz, Schaffner and Tahmasbi [16] show that there is an inherent limitation to this simultaneous variant of O2H lemma. They give an explicit example that shatters the hope of proving unclonable indistinguishability of the construction in [9] using this lemma.

*Instantiating [9] using Coset States.* Facing with the above barrier, we may resort to other states that possess some forms of unclonability. One candidate is the so called "coset states", first proposed by Vidick and Zhang [23] in the context of proofs of quantum knowledge and later studied by Coladangelo et al. [10] for copy-protection schemes.

A coset state is described by three parameters: a subspace $A \subseteq \mathbb{F}_2^\lambda$ of dimension $\lambda/2$ and two vectors $s, s' \in \mathbb{F}_2^\lambda$ denoting two cosets $A + s$ and $A^\perp + s'$[10]; we write the state as $|A_{s,s'}\rangle$. Coset states have many nice properties, among those we only need the followings:

1. Given $|A_{s,s'}\rangle$ and a classical description of subspace $A$, an efficient quantum algorithm can compute both $s$ and $s'$.
2. No adversary can win the MOE game (Figure 3) for coset states with probability more than $\sqrt{e} \cdot (\cos(\pi/8))^\lambda$ (first proved in [10] and later improved by Culf and Vidick [12]).

- A challenger samples uniformly at random a subspace $A \subseteq \mathbb{F}_2^\lambda$ of dimension $\lambda/2$ $s, s' \in \mathbb{F}_2^\lambda$ and sends $|A_{s,s'}\rangle$ to $\mathcal{A}$.
- $\mathcal{A}$ taking the input from the challenger, produces a bipartite state to $\mathcal{B}$ and $\mathcal{C}$.
- The non-communicating $\mathcal{B}$ and $\mathcal{C}$ then additionally receive a classical description of the subspace $A$ and make a guess $s_\mathcal{B}, s'_\mathcal{B}, s_\mathcal{C}, s'_\mathcal{C}$ for $s, s'$ respectively.
- The splitting adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ wins the game if and only if $s_\mathcal{B} = s_\mathcal{C} = s, s'_\mathcal{B} = s'_\mathcal{C} = s'$.

**Fig. 3.** MOE Games for Coset States.

Readers may already notice the similarity between Wiesner states and coset states. If we substitute the basis information $\theta$ with $A$ and the secret $x$ with $s||s'$, we get coset states and their corresponding MOE games. Hence, we can translate the construction in [9] using the languages of coset states. A question naturally rises: if these two kinds of states are very similar, why replacing Wiesner states with coset states even matters?

Indeed, they differ on one crucial place. Let us come back to Wiesner states. As shown by [15] in the setting of private key quantum money, given $|x^\theta\rangle$ together with an oracle $P_x$ that outputs 1 only if input $y = x$, there exists an efficient quantum adversary that learns $x$ without knowing $\theta$. This further applies to the MOE games for Wiesner states: if $\mathcal{A}$ additionally gets oracle access to $P_x$, the MOE game is no longer secure.

MOE games for coset states remain secure if oracles for checking $s$ and $s'$ are given. More formally, let $P_{A+s}$ be an oracle that outputs 1 only if the input $y \in A + s$, similarly for $P_{A^\perp + s'}$. No adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ can win the MOE games for coset states with more than some exponentially small probability in $\lambda$, even

[10] There are many vectors in $A + s$. In the rest of the discussion, we assume $s$ is the lexicographically smallest vector in $A + s$. Similarly for $s'$.

if $\mathcal{A}, \mathcal{B}, \mathcal{C}$ all query $P_{A+s}$ and $P_{A^\perp+s'}$ polynomially many times. We call this game *MOE game for coset states with membership checking oracles*.

We now give our construction of unclonable encryption that satisfies unclonable indistinguishability in Figure 4. In our construction, we get rid of the extra input $\alpha$ in [9] construction. We believe $\alpha$ can be similarly removed in their construction as well. Also note that in our construction, we only require coset states and random oracles. The membership checking oracles will only be given to the adversary when we prove its security. We indeed prove a stronger security guarantee. Due to this, we can not prove the security of their construction using Wiesner states following the same idea; nonetheless, we do not know how to disprove it. We leave it as an interesting open question.

$\mathsf{Gen}(1^\lambda)$: on input $\lambda$, outputs uniformly random subspace $A \subseteq \mathbb{F}_2^\lambda$ of dimension $\lambda/2$.
$\mathsf{Enc}^H(A, m)$: samples $s, s' \in \mathbb{F}_2^\lambda$[a], outputs $(|A_{s,s'}\rangle, m \oplus H(s, s'))$.
$\mathsf{Dec}^H(A, (|A_{s,s'}\rangle, c))$: recovers $s, s'$ from the coset state, outputs $c \oplus H(s, s')$.

[a] We again require $s, s'$ to be the lexicographically smallest vector in $A + s$ and $A^\perp + s'$.

**Fig. 4.** Our Unclonable Encryption Scheme.

*Basing Security on Reprogram Games.* Now we look at what property we require for coset states to establish unclonable indistinguishability. We will focus on the case $n = 1$ for length-1 messages in this section. By a sequence of standard variable substitution, unclonable indistinguishability of our scheme can be based on the following security game (Figure 5) in the identical challenge mode, where each of $\mathcal{B}, \mathcal{C}$ tries to identify whether the oracle has been reprogrammed or not. We want to show any adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ only achieves successful probability $1/2 + \mathsf{negl}$; when $\mathcal{B}$ gets the coset state and $\mathcal{C}$ makes a random guess, they win with probability $1/2$.

Note that in the above reprogram game (Figure 5), $\mathcal{A}$ has no access to $H$. This is different from unclonable indistinguishability games or MOE games. Nevertheless, we show the oracle access to $H$ does not help $\mathcal{A}$ and thus can be safely removed by introducing a small loss.

The security of the reprogram games in the identical challenge mode can be reduced to the security in the independent challenge mode. A careful analysis of Jordan's lemma (Section 2.3) is required to show such a reduction. We believe that this reduction is highly non-trivial. However, since it is not the place that highlights the difference between Wiesner states and coset states, we leave it to the main body (Section 3.3).

- $H$ be a random oracle with binary range, $H : \mathbb{F}_2^\lambda \times \mathbb{F}_2^\lambda \to \{0,1\}$. Additionally, $\mathcal{A}, \mathcal{B}, \mathcal{C}$ get oracle access to $P_{A+s}$ and $P_{A^\perp+s'}$.
- A challenger samples a coset state $|A_{s,s'}\rangle$ and sends $(|A_{s,s'}\rangle, H(s,s'))$ to $\mathcal{A}$.
- $\mathcal{A}$ (having *no access* to the random oracle $H$) taking the input from the challenger, produces a bipartite state to $\mathcal{B}$ and $\mathcal{C}$.
- The non-communicating $\mathcal{B}$ and $\mathcal{C}$ then receive a classical description of the subspace $A$:
  - Let $H_0 := H$ be the original random oracle.
  - Let $H_1$ be identical to $H$, except the outcome on $(s,s')$ is flipped.
  - (Identical Challenge Mode): Flip a coin $b$, both $\mathcal{B}$ and $\mathcal{C}$ get oracle access to $H_b$.
  - (Independent Challenge Mode): Flip two coins $b_\mathcal{B}, b_\mathcal{C}$, $\mathcal{B}$ has oracle access to $H_{b_\mathcal{B}}$ and $\mathcal{C}$ gets oracle access to $H_{b_\mathcal{C}}$.
- $\mathcal{B}, \mathcal{C}$ makes a guess $b', b''$ respectively.
- The adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ wins the game if and only if $b' = b'' = b$ (in the identical challenge mode), or $b' = b_\mathcal{B}$ and $b'' = b_\mathcal{C}$ (in the independent challenge mode).

**Fig. 5.** Reprogram Games for Coset States in the QROM

The remaining is to show the security of the game in the independent challenge mode. Inspired by the work of [26] which initiates the study of measuring success probability of a quantum program, we show there is an efficient procedure that operates locally on both the entangled adversaries $(\mathcal{B}, \mathcal{C})$ and outputs $(\mathcal{B}', p_\mathcal{B})$, $(\mathcal{C}', p_\mathcal{C})$ such that: informally,

- $\mathcal{B}'$ and $\mathcal{C}'$ are un-entangled[11].
- The success probability of $\mathcal{B}'$ on guessing $H_0$ or $H_1$ is $p_\mathcal{B}$.
- The success probability of $\mathcal{C}'$ on guessing $H_0$ or $H_1$ is $p_\mathcal{C}$.
- The expectation of $p_\mathcal{B} \cdot p_\mathcal{C}$ is equal to $(\mathcal{B}, \mathcal{C})$'s success probability in the reprogram game in the independent challenge mode.

The above procedure requires to run $\mathcal{B}'$ and $\mathcal{C}'$ on $H$ and $H_{s,s'}$. In other words, the procedure should be able to reprogram $H$ on the input $(s,s')$. Since the procedure will be used in the reduction for breaking MOE games for coset states, it should not know $s$ or $s'$, but only knows $A$ and $P_{A+s}, P_{A^\perp+s'}$. Nonetheless, we show with the membership checking oracle, such reprogramming is possible:

$$H_1 = \begin{cases} \neg H(z,z') & Q_s(z) = 1 \text{ and } Q_{s'}(z') = 1 \\ H(z,z') & \text{Otherwise} \end{cases},$$

[11] Indeed, $\mathcal{B}'$ and $\mathcal{C}'$ satisfy a weaker guarantee than being un-entangled. They can still be entangled but the same analysis we discuss applies to this weaker guarantee. For ease of presentation, we assume that they are un-entangled.

where $Q_s$ is the point function that only outputs 1 on $s$, similarly for $Q_{s'}$. The remaining is to show $Q_s$ (or $Q_{s'}$) can be instantiated by the classical description of $A$ and $P_{A+s}$ (or $P_{A^\perp+s'}$ respectively). $Q_s$ can be implemented by (1) check if the input $z$ is in $A+s$, (2) check if the input $z$ is the lexicographically smallest in $A+s$. Step (1) can be done via $P_{A+s}$. Step (2) can be done by knowing $A$ and some $z \in A+s$ (which is known from step (1)): one can check if there exists some lexicographically smaller $z^*$ such that $(z-z^*) \in \mathsf{span}(A)$; this can be done efficiently by enumerating each coordinate and Gaussian elimination. Thus, both $Q_s$ and $Q_{s'}$ can be implemented.

Without membership checking oracle, we do not know how to reprogram a random oracle, or run the above procedure. Thus the proof fails for Wiesner states.

Finally, we prove the security of reprogram games in the independent challenge mode. If $(\mathcal{A},\mathcal{B},\mathcal{C})$ has non-trivial success probability $1/2+\gamma$ for some large $\gamma$, the above procedure must output large $p_{\mathcal{B}}, p_{\mathcal{C}} > 1/2+\gamma/2$ with non-negligible probability. If $\mathcal{B}'$ never queries $H_0$ or $H_1$ on $(s,s')$, the best probability it can achieve is $1/2$. Thus, by measuring a random query of $\mathcal{B}'$, we can extract $s, s'$ with non-negligible probability. Similarly for $\mathcal{C}'$. This violates the MOE games for coset states with membership checking oracles, a contradiction. Therefore, the security of the reprogram in the independent mode is established.

### 1.5 Related Work

*Unclonable Encryption.* Broadbent and Lord [9] demonstrated the feasibility of unclonable encryption satisfying the weaker unclonability property. They present two constructions. The first construction based on Wiesner states achieve $0.85^n$-security (i.e., the probability that both $\mathcal{B}$ and $\mathcal{C}$ simultaneously guess the message is at most $0.85^n$), where $n$ is the length of the message being encrypted. Their second construction, in the quantum random oracle model, achieves $\frac{9}{2^n} + \mathsf{negl}(\lambda)$-security. In the same work, they show that any construction satisfying $2^{-n}$-unclonability implies unclonable indistinguishability property. Following Broadbent and Lord, Ananth and Kaleoglu [5] construct public-key and private-key unclonable encryption schemes from computational assumptions. Even [5] only achieve unclonable encryption with the weaker unclonability guarantees.

Majenz, Schaffner and Tahmasbi [16] explore the difficulties in constructing unclonable encryption schemes. In particular, they show that any scheme achieving unclonable indistinguishability should have ciphertexts with large eigenvalues. Towards demonstrating a better bound for unclonability, they also showed inherent limitations in the proof technique of Broadbent and Lord.

*Copy-Protection.* Copy-protection was first introduced by Aaronson [1]. Recently, Aaronson, Liu, Liu, Zhandry and Zhang [3] demonstrated the existence of copy-protection in the presence of classical oracles. Coladangelo, Majenz and Poremba

[11] showed that copy-protection for multi-bit output point functions exists in the quantum random oracle model. They also showed that copy-protection for single-bit output point functions exists in the quantum random oracle model with constant security.

Ananth and La Placa [6] showed a conditional result that copy-protection for arbitrary unlearnable functions, without the use of any oracles, does not exist. Recently, Coladangelo, Liu, Liu and Zhandry [10], assuming post-quantum indistinguishability obfuscation and one-way functions, demonstrated the first feasibility of copy-protection for a non-trivial class of functions (namely, pseudorandom functions) in the plain model. Another recent work by Broadbent, Jeffrey, Lord, Podder and Sundaram [8] studies copy-protection for a novel (but weaker) variant of copy-protection.

## 2 Preliminaries

### 2.1 Basics

We will briefly introduce some basic notations in our work and some preliminaries on quantum computing in this section.

We denote by $\lambda$ the security parameter. We write $\mathsf{poly}(\cdot)$ to denote an arbitrary polynomial and $\mathsf{negl}(\cdot)$ to denote an arbitrary negligible function. We say that an event happens with *overwhelming probability* if the probability is at least $1 - \mathsf{negl}(\lambda)$.

Readers unfamiliar with quantum computation and quantum information could refer to [17] for a comprehensive introduction.

Given Hilbert space $\mathcal{H}$, we write $\mathcal{S}(\mathcal{H})$ for the unit sphere set $\{x : ||x||_2 = 1\}$ in $\mathcal{H}$, $\mathcal{U}(\mathcal{H})$ for the set of unitaries acting on Hilbert space $\mathcal{H}$, $\mathcal{D}(\mathcal{H})$ for the set of density operators on $\mathcal{H}$. We write $\mathcal{H}_X$ to denote the Hilbert space associated with a quantum register $X$. Given two quantum states $\rho, \sigma$, we denote the (normalized) trace distance between them by

$$\mathsf{TD}(\rho, \sigma) := \frac{1}{2} \|\rho - \sigma\|_{\mathsf{tr}} .$$

We say that two states $\rho, \sigma$ are $\delta$-*close* if $\mathsf{TD}(\rho, \sigma) \leq \delta$.

A positive operator-valued measurement (POVM) on the Hilbert space $\mathcal{H}$ is defined as a set of positive semidefinite operators $\{E_i\}$ on $\mathcal{H}$ that satisfies $\sum_i E_i = I$. A projective measurement means the case that $E_i$s are projectors.

A common technique in quantum computation is uncomputing [7]. A quantum algorithm could be modeled as a unitary $U$ acting on some hilbert space $\mathcal{H}$, then perform measurement on output registers on without loss of generality. By uncomputation we mean that acting $U^\dagger$ on the same hilbert space after the measurement. It is easy to examine that if the measurement outputs same result with overwhelming probability, the trace distance between the final state and the original state is negligible.

*Quantum Oracle Algorithms* A quantum oracle for a function $f$ is defined as the controlled unitary $O_f$: $O_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$. We define a query to the quantum oracle as applying $O_f$ on the given quantum state once.

We say that a quantum adversary $\mathcal{A}$ with access to oracle(s) is *query-bounded* if it makes at most $p(\lambda)$ queries to each oracle for some polynomial $p(\cdot)$.

### 2.2 Quantum Random Oracle Model (QROM)

This is the quantum analogue of Random Oracle Model, where we model a hash function $H$ as a random classical function, and it can be accessed by an adversary in superposition, modeled by the unitary $O_H$.

The following theorem, paraphrased from [7], will be used for reprogramming oracles without adversarial detection on inputs which are not queried with large weight:

**Theorem 5 ([7]).** *Let $\mathcal{A}$ be an adversary with oracle access to $H : \{0,1\}^m \to \{0,1\}^n$ that makes at most $T$ queries. Define $|\phi_i\rangle$ as the global state after $\mathcal{A}$ makes $i$ queries, and $W_y(|\phi_i\rangle)$ as the sum of squared amplitudes in $|\phi_i\rangle$ of terms in which $\mathcal{A}$ queries $H$ on input $y$. Let $\epsilon > 0$ and let $F \subseteq [0, T-1] \times \{0,1\}^m$ be a set of time-string pairs such that $\sum_{(i,y)\in F} W_y(|\phi_i\rangle) \leq \epsilon^2/T$.*

*Let $H'$ be an oracle obtained by reprogramming $H$ on inputs $(i, y) \in F$ to arbitrary outputs. Define $|\phi'_i\rangle$ as above for $H'$. Then, $\mathsf{TD}(|\phi_T\rangle, |\phi'_T\rangle) \leq \epsilon/2$.*

Note that the theorem can be straightforwardly generalized to mixed states by convexity.

### 2.3 More on Jordan's lemma

We first recall the following version of Jordan's lemma, adapted from [19] and [22]:

**Lemma 1.** *Let $\mathcal{H}$ be a finite-dimensional Hilbert space and let $\Pi_0, \Pi_1$ be any two projectors in $\mathcal{H}$, then there exists an orthogonal decomposition of $\mathcal{H}$ into one-dimensional and two dimensional subspaces $\mathcal{H} = \oplus_i \mathcal{S}_i$ that are invariant under both $\Pi_0$ and $\Pi_1$; each $\mathcal{S}_i$ is spanned by one or two eigenvectors of $(\Pi_0 + \Pi_1)/2$.*

*Whenever $\mathcal{S}_i$ is 2-dimensional, there is a basis for it in which $\Pi_0$ and $\Pi_1$ (restricting on $\mathcal{S}_i$) take the form:*

$$\Pi_{0,\mathcal{S}_i} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad \Pi_{1,\mathcal{S}_i} = \begin{pmatrix} c_i^2 & c_i s_i \\ c_i s_i & s_i^2 \end{pmatrix},$$

*where $c_i = \cos\theta_i$ and $s_i = \sin\theta_i$ for some principal angle $\theta_i \in [0, \pi/2]$.*

*Proof.* The proof can be found in the references above.

We additionally show a relation between two eigenvalues in the same Jordan block.

**Lemma 2.** *For any two projectors $\Pi_0, \Pi_1$, let $\mathcal{S}_i$ be a 2-dimensional subspace in the above decomposition. Let $|\phi_0\rangle, |\phi_1\rangle$ be two eigenvectors of $(\Pi_0 + \Pi_1)/2$ that span $\mathcal{S}_i$ and $\lambda_0, \lambda_1$ be their eigenvalues. We have $\lambda_0 + \lambda_1 = 1$.*

*Proof.* Restricting on $\mathcal{S}_i$, we have:

$$\lambda_0 + \lambda_1 = \mathrm{Tr}\left[(\Pi_{0,\mathcal{S}_i} + \Pi_{1,\mathcal{S}_i})/2\right] = (1 + c_i^2 + s_i^2)/2 = 1.$$

**Corollary 1.** *For any two projectors $\Pi_0, \Pi_1$, let $|\phi_0\rangle$ and $|\phi_1\rangle$ be two eigenvectors of $(\Pi_0 + \Pi_1)/2$ with eigenvalues $\lambda_0, \lambda_1$. If $\lambda_0 + \lambda_1 \neq 1$, then*

$$\langle\phi_0|\Pi_0|\phi_1\rangle = \langle\phi_0|\Pi_1|\phi_1\rangle = 0.$$

*Proof.* If $\lambda_0 + \lambda_1 \neq 1$, by Lemma 2, $|\phi_0\rangle$ and $|\phi_1\rangle$ can not be in the same Jordan block. Because $|\phi_0\rangle$ still belongs to the corresponding subspace $\mathcal{S}_0$ of its Jordan block after the action of $\Pi_0$, $\Pi_0 |\phi_0\rangle$ is orthogonal to $|\phi_1\rangle$. Similarly, $\Pi_1 |\phi_0\rangle$ is orthogonal to $|\phi_1\rangle$.

### 2.4 Measuring Success Probability

In this section we list theorems about simultaneously approximating the eigenvalues of a bipartite quantum program which are crucial tools in our security proofs.

**Theorem 6 (Inefficient Measurement).** *Let $\mathcal{P} = (P, Q)$ be a binary outcome POVM. Let $\mathcal{D}$ be the set of eigenvalues of $P$. There exists a projective measurement $\mathcal{E} = \{E_p\}_{p\in\mathcal{D}}$ with index set $\mathcal{D}$ that satisfies the following: for every quantum state $\rho$, let $\rho_p$ be the sub-normalized post-measurement state obtained after measuring $\rho$ with respect to $E_p$. That is, $\rho_p = E_p \rho E_p$. We have,*

*(1) For every $p \in \mathcal{D}$, $\rho_p$ is an eigenvector of $P$ with eigenvalue $p$;*
*(2) The probability of $\rho$ when measured with respect to $P$ is $\mathrm{Tr}[P\rho] = \sum_{p\in\mathcal{D}} \mathrm{Tr}[P\rho_p]$.*

A measurement $\mathcal{E}$ which satisfies these properties is the measurement in the common eigenbasis of $P$ and $Q = I - P$ (due to simultaneous diagonalization theorem, such common eigenbasis exists since $P$ and $Q$ commute). Let $P$ have eigenbasis $\{|\psi_i\rangle\}$ with eigenvalues $\{\lambda_i\}$. Without loss of generality, let us assume $\rho$ is a pure state $|\psi\rangle\langle\psi|$ and $\{\lambda_i\}$ has no duplicated eigenvalues. We write $|\psi\rangle$ in the eigenbasis of $P$: $|\psi\rangle = \sum_i \alpha_i |\psi_i\rangle$. Applying $\mathcal{E}$ will result in an outcome $\lambda_i$ and a leftover state $|\psi_i\rangle$ with probability $|\alpha_i|^2$.

Looking ahead, we will write a quantum program under the eigenbasis of $P$ in the proof of the strengthened MOE game.

**Theorem 7 (Inefficient Threshold Measurement).** *Let $\mathcal{P} = (P, Q)$ be a binary outcome POVM. Let $P$ have eigenbasis $\{|\psi_i\rangle\}$ with eigenvalues $\{\lambda_i\}$. Then, for every $\gamma \in (0, 1)$ there exists a projective measurement $\mathcal{E}_\gamma = (E_{\leq\gamma}, E_{>\gamma})$ such that:*

*(1) $E_{\leq\gamma}$ projects a quantum state into the subspace spanned by $\{|\psi_i\rangle\}$ whose eigenvalues $\lambda_i$ satisfy $\lambda_i \leq \gamma$;*

*(2) $E_{>\gamma}$ projects a quantum state into the subspace spanned by $\{|\psi_i\rangle\}$ whose eigenvalues $\lambda_i$ satisfy $\lambda_i > \gamma$.*

*Similarly, for every $\gamma \in (0, 1/2)$, there exists a projective measurement $\mathcal{E}'_\gamma = (\widetilde{E}_{\leq\gamma}, \widetilde{E}_{>\gamma})$ such that:*

*(1) $\widetilde{E}_{\leq\gamma}$ projects a quantum state into the subspace spanned by $\{|\psi_i\rangle\}$ whose eigenvalues $\lambda_i$ satisfy $|\lambda_i - \frac{1}{2}| \leq \gamma$;*
*(2) $\widetilde{E}_{>\gamma}$ projects a quantum state into the subspace spanned by $\{|\psi_i\rangle\}$ whose eigenvalues $\lambda_i$ satisfy $|\lambda_i - \frac{1}{2}| > \gamma$.*

It is easy to see how to construct $\mathcal{E}_\gamma, \mathcal{E}'_\gamma$ from $\mathcal{E}$, e.g. by setting

$$\widetilde{E}_{\leq\gamma} = \sum_{i:|\lambda_i - 1/2| \leq \gamma} E_{\lambda_i}.$$

Note that for any quantum state $\rho$, $\mathrm{Tr}[\widetilde{E}_{>\gamma}\rho]$ is the weight over eigenvectors with eigenvalues $\lambda$ that are $\gamma$ away from $1/2$.

Below, we give the formal theorem statement about efficient approximated threshold measurement, which is adapted from Theorem 6.2 in [26] and Lemma 3 in [3].

**Theorem 8 (Efficient Threshold Measurement).** *Let $\mathcal{P}_b = (P_b, Q_b)$ be a binary outcome POVM over Hilbert space $\mathcal{H}_b$ that is a mixture of projective measurements for $b \in \{1, 2\}$. Let $P_b$ have eigenbasis $\{|\psi_i^b\rangle\}$ with eigenvalues $\{\lambda_i^b\}$. For every $\gamma_1, \gamma_2 \in (0, 1), 0 < \epsilon < \min(\gamma_1/2, \gamma_2/2, 1-\gamma_1, 1-\gamma_2)$ and $\delta > 0$, there exist efficient binary-outcome quantum algorithms, interpreted as the POVM element corresponding to outcome 1, $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P}_b,\gamma}$ such that for every quantum program $\rho \in \mathcal{D}(\mathcal{H}_1) \otimes \mathcal{D}(\mathcal{H}_2)$ the following are true about the product algorithm $\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P}_1,\gamma_1} \otimes \mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P}_2,\gamma_2}$:*

*(0) Let $(E^b_{\leq\gamma}, E^b_{>\gamma})$ be the inefficient threshold measurement in Theorem 7 for $\mathcal{H}_b$.*
*(1) The probability of measuring 1 on both registers satisfies*

$$\mathrm{Tr}\left[\left(\mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P}_1,\gamma_1} \otimes \mathsf{ATI}^{\epsilon,\delta}_{\mathcal{P}_2,\gamma_2}\right)\rho\right] \geq \mathrm{Tr}\left[\left(E^1_{>\gamma_1+\epsilon} \otimes E^2_{>\gamma_2+\epsilon}\right) \cdot \rho\right] - 2\delta.$$

*(2) The post-measurement state $\rho'$ after getting outcome (1,1) is $4\delta$-close to a state in the support of $\left\{|\psi_i^1\rangle\,|\psi_j^2\rangle\right\}$ such that $\lambda_i^1 > \gamma_1 - 2\epsilon$ and $\lambda_j^2 > \gamma_2 - 2\epsilon$.*
*(3) The running time of the algorithm is polynomial in the running time of $P_1, P_2, 1/\epsilon$ and $\log(1/\delta)$.*

Intuitively the theorem says that if a quantum state $\rho$ has weight $p$ on eigenvectors of $(P_1, P_2)$ with eigenvalues greater than $(\gamma_1 + \epsilon, \gamma_2 + \epsilon)$, then the quantum algorithm will produce (with probability at least $p-2\delta$) a post-measurement state which has weight $1 - 4\delta$ on eigenvectors with eigenvalues greater than $(\gamma_1 - 2\epsilon, \gamma_2 - 2\epsilon)$.

In this paper, we will work with indistinguishability games. Therefore, we will particularly be interested in the projective measurement that projects onto

eigenvectors with eigenvalues away from $1/2$ (meaning its behavior is more than random guessing). For this reason, we will need the following symmetric version of Theorem 8:

**Theorem 9 (Efficient Symmetric Threshold Measurement).** *Let $\mathcal{P}_b = (P_b, Q_b)$ be a binary outcome POVM over Hilbert space $\mathcal{H}_b$ that is a mixture of projective measurements for $b \in \{1,2\}$. Let $P_b$ have eigenbasis $\{|\psi_i^b\rangle\}$ with eigenvalues $\{\lambda_i^b\}$. For every $\gamma_1, \gamma_2 \in (0, 1/2), 0 < \epsilon < \min(\gamma_1/2, \gamma_2/2)$, and $\delta > 0$, there exist efficient binary-outcome quantum algorithms, interpreted as the POVM element corresponding to outcome 1, $\mathsf{SATI}^{\epsilon,\delta}_{\mathcal{P}_b,\gamma}$ such that for every quantum program $\rho \in \mathcal{D}(\mathcal{H}_1) \otimes \mathcal{D}(\mathcal{H}_2)$ the following are true about the product algorithm $\mathsf{SATI}^{\epsilon,\delta}_{\mathcal{P}_1,\gamma_1} \otimes \mathsf{SATI}^{\epsilon,\delta}_{\mathcal{P}_2,\gamma_2}$:*

*(0) Let $(\widetilde{E}^b_{\leq\gamma_b}, \widetilde{E}^b_{>\gamma_b})$ be the inefficient threshold measurement in Theorem 7 for $\mathcal{H}_b$.*
*(1) The probability of measuring 1 on both registers satisfies*

$$\mathrm{Tr}\left[\left(\mathsf{SATI}^{\epsilon,\delta}_{\mathcal{P}_1,\gamma_1} \otimes \mathsf{SATI}^{\epsilon,\delta}_{\mathcal{P}_2,\gamma_2}\right)\rho\right] \geq \mathrm{Tr}\left[\left(\widetilde{E}^1_{>\gamma_1+\epsilon} \otimes \widetilde{E}^2_{>\gamma_2+\epsilon}\right)\cdot\rho\right] - 2\delta.$$

*(2) The post-measurement state $\rho'$ after getting outcome (1,1) is $4\delta$-close to a state in the support of $\left\{|\psi_i^1\rangle\,|\psi_j^2\rangle\right\}$ such that $|\lambda_i^1 - 1/2| > \gamma_1 - 2\epsilon$ and $|\lambda_j^2 - 1/2| > \gamma_2 - 2\epsilon$.*
*(3) The running time of the algorithm is polynomial in the running time of $P_1, P_2, 1/\epsilon$ and $\log(1/\delta)$.*

### 2.5 Unclonable Encryption

In this subsection, we provide the definition of unclonable encryption schemes. By unclonable encryption, we are refering to the security defined in [5]. This is a variant of the original security definition in [9], which forces one of $m_0, m_1$ to be uniformly random. We would remark that our security is stronger than the original one in [9], since in our definition $m_0, m_1$ can be arbitrarily chosen.

**Definition 1.** *An unclonable encryption scheme is a triple of efficient quantum algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with the following interface:*

- $\mathsf{Gen}(1^\lambda) : \mathsf{sk}$ *on input a security parameter $1^\lambda$, returns a classical key* $\mathsf{sk}$.
- $\mathsf{Enc}(\mathsf{sk}, |m\rangle\langle m|) : \rho_{ct}$ *takes the key* $\mathsf{sk}$ *and the message $|m\rangle\langle m|$ for $m \in \{0,1\}^{\mathrm{poly}(\lambda)}$, outputs a quantum ciphertext $\rho_{ct}$.*
- $\mathsf{Dec}(\mathsf{sk}, \rho_{ct}) : \rho_m$ *takes the key* $\mathsf{sk}$ *and the quantum ciphertext $\rho_{ct}$, outputs a message in the form of quantum states $\rho_m$.*

*Correctness. The following must hold for the encryption scheme. For $\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$, we must have $\mathrm{Tr}[|m\rangle\langle m| \, \mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{sk}, |m\rangle\langle m|))] \geq 1 - \mathsf{negl}(\lambda)$.*

*Unclonability. In the following sections, we focus on unclonable IND-CPA security. To define our unclonable security, we introduce the following security game.*

**Definition 2 (Unclonable IND-CPA game).** *Let $\lambda \in \mathbb{N}^+$. Given encryption scheme $\mathcal{S}$, consider the following game against the adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$.*

- *The adversary $\mathcal{A}$ generates $m_0, m_1 \in \{0,1\}^{n(\lambda)}$ and sends to the challenger as the chosen plaintext.*
- *The challenger randomly chooses a bit $b \in \{0,1\}$ and returns $\mathsf{Enc}(\mathsf{sk}, m_b)$ to $\mathcal{A}$. $\mathcal{A}$ produces a quantum state $\rho_{BC}$ in register $B$ and $C$, and sends corresponding registers to $\mathcal{B}$ and $\mathcal{C}$.*
- *$\mathcal{B}$ and $\mathcal{C}$ receive the key $\mathsf{sk}$, and output bits $b_{\mathcal{B}}$ and $b_{\mathcal{C}}$ respectively*

*and the adversary wins if $b_{\mathcal{B}} = b_{\mathcal{C}} = b$.*

We denote the advantage (success probability) of above game by $\mathsf{adv}_{\mathcal{G},\mathcal{A},\mathcal{B},\mathcal{C}}(\lambda)$. We say that scheme $\mathcal{S}$ is informational (computational) secure if for all(efficient) adversaries $(\mathcal{G}, \mathcal{A}, \mathcal{B}, \mathcal{C})$,

$$\mathsf{adv}_{\mathcal{G},\mathcal{A},\mathcal{B},\mathcal{C}}(\lambda) \leq \frac{1}{2} + \mathsf{negl}(\lambda).$$

## 3 More on Coset States

In this section, we will recall the basic properties of coset states. We will then introduce a strengthened unclonable game in the quantum random oracle model (QROM), upon which we will build our unclonable encryption scheme. The last subsection is devoted to prove the security of this strengthened game.

### 3.1 Preliminaries

In this subsection, we recall the basic definitions and properties of coset states in [10]. Let $A \subseteq \mathbb{F}_2^n$ be a subspace. Define its orthogonal complement of $A$ as $A^\perp = \{b \in \mathbb{F}_2^n \,|\, \langle a, b\rangle \bmod 2 = 0\,, \forall a \in A\}$. It satisfies $\dim(A) + \dim(A^\perp) = n$. We also let $|A| = 2^{\dim(A)}$ denote the size of $A$.

**Definition 3 (Coset States).** *For any subspace $A \subseteq \mathbb{F}_2^n$ and vectors $s, s' \in \mathbb{F}_2^n$, the coset state $|A_{s,s'}\rangle$ is defined as:*

$$|A_{s,s'}\rangle = \frac{1}{\sqrt{|A|}} \sum_{a \in A} (-1)^{\langle s', a\rangle} |a + s\rangle \ .$$

By applying $H^{\otimes n}$ to the state $|A_{s,s'}\rangle$, one obtains exactly $|A^\perp_{s',s}\rangle$. Given $A, s, s'$, the coset state is efficiently constructible.

For a subspace $A$ and vectors $s, s'$, we define $A + s = \{v + s : v \in A\}$, and $A^\perp + s' = \{v + s' : v \in A^\perp\}$. We define $P_{A+s}$ and $P_{A^\perp+s'}$ as the membership checking oracle for both cosets.

It is also convenient for later sections to define a canonical representation of a coset $A + s$, with respect to subspace $A$,

**Definition 4 (Canonical Representative of a Coset).** *For a subspace $A$, we define the function $\mathsf{Can}_A(\cdot)$ such that $\mathsf{Can}_A(s)$ is the lexicographically smallest vector contained in $A + s$. We call this the canonical representative of coset $A + s$.*

If $\tilde{s} \in A+s$, then $\mathsf{Can}_A(s) = \mathsf{Can}_A(\tilde{s})$. We also note that $\mathsf{Can}_A(\cdot)$ is polynomial-time computable given the description of $A$. Accordingly, we can efficiently sample from $\mathsf{CS}(A) := \{\mathsf{Can}_A(s) : s \in \mathbb{F}_2^n\}$, which denotes the set of canonical representatives for $A$.

For a fixed subspace $A$, the coset states $\{|A_{s,s'}\rangle\}_{s\in\mathsf{CS}(A),s'\in\mathsf{CS}(A^\perp)}$ form an orthonormal basis. (See Lemma C.2 in [10])

Next, we recall the regular direct product and MOE properties of coset states. These properties will be used to prove the strengthened unclonable property.

*Direct Product Hardness*

**Theorem 10 (Theorem 4.5,4.6 in [10]).** *Let $A \subseteq \mathbb{F}_2^\lambda$ be a uniformly random subspace of dimension $\frac{\lambda}{2}$, and $s, s'$ be two uniformly random vectors from $\mathbb{F}_2^\lambda$. Let $\epsilon > 0$ such that $1/\epsilon = o(2^{n/2})$. Given one copy of $|A_{s,s'}\rangle$ and oracle access to $P_{A+s}$ and $P_{A^\perp+s'}$, an adversary needs $\Omega(\sqrt{\epsilon}2^{\lambda/2})$ queries to output a pair $(v, w)$ that $v \in A + s$ and $w \in A^\perp + s'$ with probability at least $\epsilon$.*

An important corollary immediately follows.

**Corollary 2.** *There exists an exponential function* exp *such that, for any query-bounded (polynomially many queries to $P_{A+s}, P_{A^\perp+s'}$) adversary, its probability to output a pair $(v, w)$ that $v \in A + s$ and $w \in A^\perp + s'$ is smaller than $1/\exp(\lambda)$.*

*Monogamy-of-Entanglement (with Membership Checking Oracles).*

**Definition 5.** *Let $\lambda \in \mathbb{N}^+$. Consider the following game between a challenger and an adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$.*

- *The challenger picks a uniformly random subspace $A \subseteq \mathbb{F}_2^\lambda$ of dimension $\frac{\lambda}{2}$, and uniformly random vectors $(s, s') \in \mathsf{CS}(A) \times \mathsf{CS}(A^\perp)$. It sends $|A_{s,s'}\rangle$ to $\mathcal{A}$.*
- *$\mathcal{A}, \mathcal{B}, \mathcal{C}$ get (quantum) oracle access to $P_{A+s}$ and $P_{A^\perp+s'}$.*
- *$\mathcal{A}$ creates a bipartite state on registers $\mathsf{B}$ and $\mathsf{C}$. Then, $\mathcal{A}$ sends register $\mathsf{B}$ to $\mathcal{B}$, and $\mathsf{C}$ to $\mathcal{C}$.*
- *The description of $A$ is then sent to both $\mathcal{B}, \mathcal{C}$.*
- *$\mathcal{B}$ and $\mathcal{C}$ return respectively $(s_1, s_1')$ and $(s_2, s_2')$.*

*$(\mathcal{A}, \mathcal{B}, \mathcal{C})$ wins if and only if for $i \in \{1, 2\}$, $s_i = s$ and $s_i' = s'$.*

We denote the advantage (success probability) of the above game by $\mathsf{adv}_{\mathcal{A},\mathcal{B},\mathcal{C}}(\lambda)$. We have the following theorem.

**Theorem 11 (Theorem 4.14, 4.15 in [10]).** *There exists an exponential function* exp *such that, for every $\lambda \in \mathbb{N}^+$, for any query-bounded (polynomially many queries to $P_{A+s}, P_{A^\perp+s'}$) adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$,*

$$\mathsf{adv}_{\mathcal{A},\mathcal{B},\mathcal{C}}(\lambda) \leq 1/\exp(\lambda)\,.$$

Note that in [10], the authors only proved the above theorem for a sub-exponential function and membership checking oracles are given in the form of indistinguishability obfuscation (iO). The proof trivially holds if we replace iO with VBB obfuscation (quantum access to these oracles). Culf and Vidick [12] further proved the theorem holds for an exponential function.

### 3.2 Strengthened MOE Game in the QROM

In this subsection, we will introduce the strengthened MOE game in the QROM and state our main theorem. We present the proof in the next section.

**Definition 6.** *Let $\lambda \in \mathbb{N}^+$. Consider the following security game between a challenger and an adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ with a random oracle $H : \mathbb{F}_2^\lambda \times \mathbb{F}_2^\lambda \to \{0,1\}^{n(\lambda)}$ .*

- *The adversary $\mathcal{A}$ generates $\Delta \in \{0,1\}^{n(\lambda)}$ and sends $\Delta$ to the challenger.*
- *The challenger samples a random subspace $A \subseteq \mathbb{F}_2^\lambda$ of dimension $\lambda/2$ and two random vectors $(s, s') \in \mathsf{CS}(A) \times \mathsf{CS}(A^\perp)$. The challenger also randomly chooses a bit $b \in \{0,1\}$ and calculates $w = H(s,s') \oplus (b \cdot \Delta)$.*
  *It gives $|A_{s,s'}\rangle$ and $w$ to $\mathcal{A}$.*
- *$\mathcal{A}, \mathcal{B}, \mathcal{C}$ get (quantum) oracle access to $P_{A+s}$ and $P_{A^\perp + s'}$.*
- *$\mathcal{A}$ produces a quantum state over registers $\mathsf{BC}$ and sends $\mathsf{B}$ to $\mathcal{B}$ and $\mathsf{C}$ to $\mathcal{C}$.*
- *$\mathcal{B}, \mathcal{C}$ are given the description of $A$, they try to produce bits $b_\mathcal{B}, b_\mathcal{C}$.*

*$(\mathcal{A}, \mathcal{B}, \mathcal{C})$ win if and only if $b_\mathcal{B} = b_\mathcal{C} = b$.*

We denote the advantage of the above game by $\mathsf{adv}_{\mathcal{A},\mathcal{B},\mathcal{C}}(\lambda)$. Note that since $s, s'$ is defined as the canonical vector of both cosets, they are uniquely defined; similarly, $H(s,s')$ is also uniquely defined.

We show the following theorem:

**Theorem 12.** *Let $n = \Omega(\lambda)$, then for every $\lambda \in \mathbb{N}^+$ and all query-bounded algorithms $(\mathcal{A}, \mathcal{B}, \mathcal{C})$, $\mathsf{adv}_{\mathcal{A},\mathcal{B},\mathcal{C}}(\lambda) \leq \frac{1}{2} + \mathsf{negl}(\lambda)$.*

### 3.3 Proof for Theorem 12

*Proof.* We prove the theorem by following hybrid arguments.

**Hybrid 0** *This hybrid is the original game.*

**Hybrid 1** *This hybrid follows Hybrid 0, but the oracle of $\mathcal{A}$ will be reprogrammed as $H_{s,s'}$ defined as follows:*

$$H_{s,s'}(z,z') = \begin{cases} u & \text{if } z = s, z' = s' \\ H(z,z') & \text{otherwise} \end{cases},$$

*where $u \in \{0,1\}^n$ is chosen uniformly at random.*

**Hybrid 2** *This hybrid will modify the access to random oracle of $\mathcal{B}$ and $\mathcal{C}$.*

- *The adversary $\mathcal{A}$ generates $\Delta \in \{0,1\}^{n(\lambda)}$ and sends $\Delta$ to the challenger.*

- *The challenger samples a random subspace* $A \subseteq \mathbb{F}_2^\lambda$ *of dimension* $\lambda/2$ *and two random vectors* $(s, s') \in \mathsf{CS}(A) \times \mathsf{CS}(A^\perp)$. *The challenger uniform randomly samples a bit* $b \in \{0,1\}$ *and* $r \in \{0,1\}^{n(\lambda)}$, *and defines the oracle* $H^b_{s,s'}$ *as follows:*

$$H^b_{s,s'}(z,z') = \begin{cases} r \oplus (b \cdot \Delta) & \text{if } z = s, z' = s' \\ H(z,z') & \text{otherwise} \end{cases},$$

  *It gives* $|A_{s,s'}\rangle$ *and* $r$ *to* $\mathcal{A}$.
- $\mathcal{A}, \mathcal{B}, \mathcal{C}$ *get (quantum) oracle access to* $P_{A+s}$ *and* $P_{A^\perp+s'}$.
- *With access to quantum random oracle* $H_{s,s'}$, $\mathcal{A}$ *produces a quantum state over registers* $\mathsf{BC}$ *and sends* $\mathsf{B}$ *to* $\mathcal{B}$ *and* $\mathsf{C}$ *to* $\mathcal{C}$.
- *With access to quantum random oracle* $H^b_{s,s'}$, $\mathcal{B}, \mathcal{C}$ *are given the description of* $A$, *they try to produce bits* $b_\mathcal{B}, b_\mathcal{C}$.

$(\mathcal{A}, \mathcal{B}, \mathcal{C})$ *win if and only if* $b_\mathcal{B} = b_\mathcal{C} = b$.

We denote by $p_i$ the optimal success probability of the game in **Hybrid i**. For the relations between different $p_i$, we have following lemmas:

**Lemma 3.** $|p_0 - p_1| \leq \mathsf{negl}(\lambda)$.

**Lemma 4.** $p_1 = p_2$.

**Lemma 5.** $p_2 \leq \frac{1}{2} + \mathsf{negl}(\lambda)$.

Combining the three lemmas, we have completed the proof of Theorem 12.

Now we provide proofs for lemmas beyond.

*Proof for Lemma 3.* We prove by contradiction. Suppose $p_0 \geq p_1 + 1/q(\lambda)$ for some polynomial $q(\lambda)$, then we can construct an adversary $\mathcal{A}'$ that violates the direct product hardness of coset states. $\mathcal{A}'$ will perform as follows:

- $\mathcal{A}'$ samples a random oracle $H : \mathbb{F}_2^\lambda \times \mathbb{F}_2^\lambda \to \{0,1\}^{n(\lambda)}$.
- $\mathcal{A}'$ simulates $\mathcal{A}$ using $H$ and applies computational basis measurement on a random quantum query made by $\mathcal{A}$ to the random oracle.

By Theorem 5, assuming $\mathcal{A}$ makes at most $T$ queries, then $\mathcal{A}'$ gets $(s, s')$ with probability at least $4/(q^2T)$, a contradiction to Corollary 2.

*Proof of Lemma 4.* Fixing $\Delta$ and $b$, the two games are identical by renaming the $w = H(s, s') \oplus (b \cdot \Delta)$ to $r$. Since $H(s, s')$ is uniformly random, its distribution is identical to $r$.

*Proof of Lemma 5.* Fixing $A, r, \Delta$, two canonical vectors $s, s'$, let $H_{-s,s'}$ be a partial random oracle that is defined on every input except $(s, s')$. Fix any partial random oracle $H_{-s,s'}$,

we define two *projectors* $\Pi^B_0, \Pi^B_1$ over register $\mathsf{B}$ as:

- $\Pi_0^B$: runs $\mathcal{B}$ on input $A$ with oracle access to $H^0_{s,s'}$ where $H^0_{s,s'}$ is the same as $H_{-s,s'}$ except on input $(s,s')$ it outputs $r$; it measures if the outcome is $r$; then it undoes all the computation.
- $\Pi_1^B$: similar to $\Pi_0^B$ except on input $(s,s')$, the random oracle $H^1_{s,s'}$ outputs $r \oplus \Delta$ and it checks if the outcome is $r \oplus \Delta$.

Let $\{|\phi_i\rangle\}_i$ be a set of the eigenvectors of $(\Pi_0^B + \Pi_1^B)/2$ with eigenvalues $\{\lambda_i\}_i$.

Fixing the same $A, s, s', r$ and $H_{-s,s'}$, we can similarly define $\Pi_0^C, \Pi_1^C$ for $\mathcal{C}$. Let $\{|\psi_j\rangle\}_j$ be a set of the eigenvectors of $(\Pi_0^C + \Pi_1^C)/2$ with eigenvalues $\{\mu_j\}_j$.

Let $|\phi_{\mathsf{BC}}\rangle$ be the state prepared by $\mathcal{A}$. Without loss of generality, we can assume the state is pure. We write the state under the basis $\{|\phi_i\rangle\}_i$ and $\{|\psi_j\rangle\}_j$:

$$|\phi_{\mathsf{BC}}\rangle = \sum_{i,j} \alpha_{i,j} |\phi_i\rangle_{\mathsf{B}} \otimes |\psi_j\rangle_{\mathsf{C}}.$$

**Lemma 6.** *Taken the randomness of $A, s, s'$ and $H_{-s,s'}$, for every polynomial $p(\cdot)$, there exists a negligible function* $\mathsf{negl}$ *such that with overwhelming probability the following weight is bounded:*

$$\sum_{\substack{i:\ |\lambda_i - 1/2| > 1/p \\ j:\ |\mu_j - 1/2| > 1/p}} |\alpha_{i,j}|^2 \leq \mathsf{negl}(n).$$

The proof for this lemma is given at the end of this section.

With the above lemma, we can claim that over the randomness of $A, s, s'$ and $H_{-s,s'}$, for every polynomial $p(\cdot)$, $|\phi_{\mathsf{BC}}\rangle$ is negligibly close to the following state $|\phi'_{\mathsf{BC}}\rangle$:

$$\sum_{i:|\lambda_i - 1/2| \leq 1/p} \alpha_{i,j} |\phi_i\rangle_{\mathsf{B}} \otimes |\psi_j\rangle_{\mathsf{C}} + \sum_{\substack{i:|\lambda_i - 1/2| > 1/p \\ j:|\mu_j - 1/2| \leq 1/p}} \alpha_{i,j} |\phi_i\rangle_{\mathsf{B}} \otimes |\psi_j\rangle_{\mathsf{C}}.$$

For convenience, we name the left part as $|\phi'_{\mathcal{B}}\rangle$ (indicating $\mathcal{B}$ can not win) and the right part as $|\phi'_{\mathcal{C}}\rangle$ (indicating $\mathcal{C}$ can not win). Thus, for every polynomial $p(\cdot)$, there exists a negligible function $\mathsf{negl}(\cdot)$, $|\,|\phi_{\mathsf{BC}}\rangle - (|\phi'_{\mathcal{B}}\rangle + |\phi'_{\mathcal{C}}\rangle)|_1$ is at most $\mathsf{negl}(\cdot)$ (in expectation, taken the randomness of $A, s, s', r$ and $H_{-s,s'}$).

The probability that $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ wins is at most:

$$\left(\left|(\Pi_0^B \otimes \Pi_0^C)\,|\phi'_{\mathsf{BC}}\rangle\right|^2 + \left|(\Pi_1^B \otimes \Pi_1^C)\,|\phi'_{\mathsf{BC}}\rangle\right|^2\right)/2.$$

$\Pi_0^B \otimes \Pi_0^C$ is the case that they both get access to $H_0$ and $\Pi_1^B \otimes \Pi_1^C$ for $H_1$.

The probability is at most

$$
\begin{aligned}
&\left(\left|(\Pi_0^B \otimes \Pi_0^C)(|\phi'_{\mathcal{B}}\rangle + |\phi'_{\mathcal{C}}\rangle)\right|^2 + \left|(\Pi_1^B \otimes \Pi_1^C)(|\phi'_{\mathcal{B}}\rangle + |\phi'_{\mathcal{C}}\rangle)\right|^2\right)/2 \\
=&\frac{1}{2}\cdot\left(\langle\phi'_{\mathcal{B}}|(\Pi_0^B \otimes \Pi_0^C)|\phi'_{\mathcal{B}}\rangle + \langle\phi'_{\mathcal{B}}|(\Pi_1^B \otimes \Pi_1^C)|\phi'_{\mathcal{B}}\rangle + \langle\phi'_{\mathcal{C}}|(\Pi_0^B \otimes \Pi_0^C)|\phi'_{\mathcal{C}}\rangle\right. \\
&\left.+\langle\phi'_{\mathcal{C}}|(\Pi_1^B \otimes \Pi_1^C)|\phi'_{\mathcal{C}}\rangle\right) + \mathsf{Re}\left(\langle\phi'_{\mathcal{B}}|(\Pi_0^B \otimes \Pi_0^C)|\phi'_{\mathcal{C}}\rangle + \langle\phi'_{\mathcal{B}}|(\Pi_1^B \otimes \Pi_1^C)|\phi'_{\mathcal{C}}\rangle\right) \\
\leq&\frac{1}{2}\cdot\left(\langle\phi'_{\mathcal{B}}|(\Pi_0^B \otimes I)|\phi'_{\mathcal{B}}\rangle + \langle\phi'_{\mathcal{B}}|(\Pi_1^B \otimes I)|\phi'_{\mathcal{B}}\rangle + \langle\phi'_{\mathcal{C}}|(I \otimes \Pi_0^C)|\phi'_{\mathcal{C}}\rangle\right. \\
&\left.+\langle\phi'_{\mathcal{C}}|(I \otimes \Pi_1^C)|\phi'_{\mathcal{C}}\rangle\right) + \mathsf{Re}\left(\langle\phi'_{\mathcal{B}}|(\Pi_0^B \otimes \Pi_0^C)|\phi'_{\mathcal{C}}\rangle + \langle\phi'_{\mathcal{B}}|(\Pi_1^B \otimes \Pi_1^C)|\phi'_{\mathcal{C}}\rangle\right).
\end{aligned}
$$

We bound each term separately.

- $\frac{1}{2}\left(\langle\phi'_{\mathcal{B}}|(\Pi_0^B \otimes I)|\phi'_{\mathcal{B}}\rangle + \langle\phi'_{\mathcal{B}}|(\Pi_1^B \otimes I)|\phi'_{\mathcal{B}}\rangle\right)$. It is equal to $\langle\phi'_{\mathcal{B}}|(\Pi_0^B+\Pi_1^B)/2\otimes I|\phi'_{\mathcal{B}}\rangle$; by the definition of $|\phi'_{\mathcal{B}}\rangle$, it will be at most $(\frac{1}{2}+\frac{1}{p})|\,|\phi'_{\mathcal{B}}\rangle\,|^2$.
- $\frac{1}{2}\left(\langle\phi'_{\mathcal{C}}|(I \otimes \Pi_0^C)|\phi'_{\mathcal{C}}\rangle + \langle\phi'_{\mathcal{C}}|(I \otimes \Pi_1^C)|\phi'_{\mathcal{C}}\rangle\right)$. Similar to the above case, it is at most $(\frac{1}{2}+\frac{1}{p})|\,|\phi'_{\mathcal{C}}\rangle\,|^2$.
- $\mathsf{Re}\left(\langle\phi'_{\mathcal{B}}|(\Pi_0^B \otimes \Pi_0^C)|\phi'_{\mathcal{C}}\rangle\right)$. By Corollary 1, the inner product will be 0:

$$
\begin{aligned}
&\langle\phi'_{\mathcal{B}}|(\Pi_0^B \otimes \Pi_0^C)|\phi'_{\mathcal{C}}\rangle \\
=&\sum_{i:|\lambda_i-1/2|\leq 1/p}\ \sum_{\substack{i':|\lambda_{i'}-1/2|>1/p \\ j':|\mu_{j'}-1/2|\leq 1/p}} \alpha^{\dagger}_{i,j}\alpha_{i',j'}\langle\phi_i|\Pi_0^B|\phi_{i'}\rangle\langle\psi_j|\Pi_0^C|\psi_{j'}\rangle;
\end{aligned}
$$

  since every possible $i, i'$ satisfy $\lambda_i + \lambda_{i'} \neq 1$, we have $\langle\phi_i|\Pi_0^B|\phi_{i'}\rangle = 0$.
- $\mathsf{Re}\left(\langle\phi'_{\mathcal{B}}|(\Pi_1^B \otimes \Pi_1^C)|\phi'_{\mathcal{C}}\rangle\right)$. By Corollary 1, the inner product will be 0 as well.

Therefore, the total probability will be at most $\left(\frac{1}{2}+\frac{1}{p}\right)(|\,|\phi'_{\mathcal{B}}\rangle\,|^2+|\,|\phi'_{\mathcal{C}}\rangle\,|^2)+\mathsf{negl}(n) \leq \frac{1}{2}+\frac{1}{p}+\mathsf{negl}(n)$.

Since the above statement holds for every polynomial $p(\cdot)$, it finishes the proof for Theorem 12.

Finally, we give the proof for Lemma 6.

*Proof of Lemma 6.* We prove by contradiction: suppose there exists an adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ such that the weight, which we call $W$, is non-negligible, i.e. $W > 1/q(\lambda)$ for some polynomial $q(\cdot)$, with some non-negligible probability $\eta(\lambda)$. For convenience, we will omit $\lambda$ in the proof when it is clear from the context.

We construct the following adversary $(\mathcal{A}', \mathcal{B}', \mathcal{C}')$ that breaks the regular MOE game in Definition 5:

1. $\mathcal{A}', \mathcal{B}', \mathcal{C}'$ get (quantum) oracle access to $P_{A+s}$ and $P_{A^{\perp}+s'}$.
2. $\mathcal{A}'$ first receives $\Delta$ from simulated $\mathcal{A}$, it samples $r \in \{0,1\}^{n(\lambda)}$ and a random oracle $H$. Given $|A_{s,s'}\rangle, r$ and two membership checking oracles, it simulates $\mathcal{A}$ via reprogrammed $H_{s,s'}$, and produces $|\phi_{\mathsf{BC}}\rangle$; it gives $\mathsf{B}$ to $\mathcal{B}'$ and $\mathsf{C}$ to $\mathcal{C}'$. Note that, although $H$ is a total random oracle, we will later reprogram $H$ at the input $(s, s')$. Thus, $H$ will only serve as $H_{-s,s'}$. Since $\mathcal{A}'$ does not know $(s, s')$, it is hard for $\mathcal{A}'$ to only sample $H_{-s,s'}$.

3. Define two projectors $\Pi_0^B, \Pi_1^B$ over register $\mathsf{B}$ as what we have described at the beginning of the proof, with the random oracle $H^0_{s,s'}$ and $H^1_{s,s'}$ is defined as:

$$H^0_{s,s'}(z,z') = \begin{cases} r & \text{if } z = s, z' = s' \\ H(z,z') & \text{otherwise} \end{cases},$$

and

$$H^1_{s,s'}(z,z') = \begin{cases} r \oplus \Delta & \text{if } z = s, z' = s' \\ H(z,z') & \text{otherwise} \end{cases}.$$

Given $P_{A+s}, P_{A^\perp+s'}$ and the description of $A$, one can efficiently implement point functions that check the canonical vectors $s$ and $s'$; thus, additionally given $H$, $H^0_{s,s'}$ and $H^1_{s,s'}$ can also be efficiently simulated. Therefore, $\mathcal{B}'$ can implement both $\Pi_0^B, \Pi_1^B$ efficiently.
$\mathcal{B}'$ gets $\mathsf{B}$, it applies the efficient approximate threshold measurement $\mathsf{SATI}^{\epsilon,\delta}_{(P,Q),\gamma}$ in Theorem 9 with $P = (\Pi_0^B + \Pi_1^B)/2$, $Q = I - P$, $\gamma = 3/4p$, $\epsilon = 1/4p$ and $\delta = 2^{-\lambda}$.
If the outcome is 1, $\mathcal{B}'$ then runs $\mathcal{B}$ on the leftover state with $H_0$ or $H_1$ picked uniformly at random. It measures and outputs a random query $\mathcal{B}$ makes to the random oracle.
4. Similarly define $\Pi_0^C, \Pi_1^C$ as above on register $\mathsf{C}$. $\mathcal{C}'$ gets $\mathsf{C}$, it applies the efficient approximated threshold measurement $\mathsf{SATI}^{\epsilon,\delta}_{(P,Q),\gamma}$ with $P = (\Pi_0^C + \Pi_1^C)/2$, $Q = I - P$, $\gamma = 3/4p$, $\epsilon = 1/2p$, and $\delta = 2^{-\lambda}$.
When the outcome is 1, $\mathcal{C}'$ runs $\mathcal{C}$ on the leftover state with $H_0$ or $H_1$ picked uniformly at random. It measures and outputs a random query to the random oracle.

By Theorem 9 bullet (1), conditioned on $W \geq 1/q$, both $\mathcal{B}'$ and $\mathcal{C}'$ will get outcome 1 with probability $1/q - 2\delta = O(1/q)$. When both outcomes are 1, by bullet (2) of Theorem 9, the leftover state is $4\delta$-close to the the following state:

$$\sum_{\substack{i:|\lambda_i - 1/2| > 1/4p \\ j:|\mu_j - 1/2| > 1/4p}} \beta_{i,j} \left|\phi_i\right\rangle_{\mathsf{B}} \otimes \left|\psi_j\right\rangle_{\mathsf{C}}.$$

Observe that when $\mathcal{B}$ does not query $(s, s')$, it will succeed with probability exactly $1/2$. Therefore, by Theorem 5, the query weight of $\mathcal{B}$ on $(s, s')$ is at least $1/4p^2T - \mathsf{negl}(\lambda)$, where $T$ is an upper-bound on the number of queries made by $\mathcal{B}$. Arguing similarly for $\mathcal{C}$, we conclude that the adversary $(\mathcal{A}', \mathcal{B}', \mathcal{C}')$ wins with probability at least $O(\eta/(qp^4T^2))$, which is non-negligible.

## 4 Unclonable Encryption in the QROM

The following is the unclonable encryption scheme for a single bit:

1. $\mathsf{sk} = A$ where $A$ is a random subspace $A \subseteq \mathbb{F}_2^n$ of dimension $n/2$;
2. $\mathsf{Enc}^H(\mathsf{sk}, m)$: it samples $s \leftarrow \mathsf{CS}(A)$ and $s' \leftarrow \mathsf{CS}(A^\perp)$ uniformly at random; it outputs $|A_{s,s'}\rangle$, $c = H(s, s') \oplus m$;
3. $\mathsf{Dec}^H(\mathsf{sk} = A, (|A_{s,s'}\rangle, c))$:
   - It first computes $s$ in superposition. We know that there is a classical algorithm that on any vector in $A + s$ and the description of $A$, outputs the canonical vector of $A + s$ (which is $s$ in this case). See [10] Definition 4.3 for more references.
     We can run this classical algorithm coherently on $|A_{s,s'}\rangle$ to learn $s$.
   - Since the algorithm on any vector in $A + s$ outputs the same vector, the quantum state stays intact. We can run the same algorithms coherently on the Hadamard basis and the description of $A^\perp$ to learn $s'$.
   - Output $c \oplus H(s, s')$.

With Theorem 12, we can show the scheme satisfy the unclonable IND-CPA security.

*Proof.* If we have some adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ for the scheme beyond, we can construct an adversary $(\mathcal{A}', \mathcal{B}', \mathcal{C}')$ for the strengthened MOE game with the same advantage.

- The adversary $\mathcal{A}'$ gets $(m_0, m_1) \leftarrow \mathcal{A}$ and sends $\Delta = m_0 \oplus m_1$ to the challenger.
- After receiving $|A_{s,s'}\rangle$ and $w$ from the challenger, $\mathcal{A}'$ calculates $c = w \oplus m_0$, and sends $(|A_{s,s'}\rangle, c)$ to $\mathcal{A}$. The output registers $\mathsf{B}, \mathsf{C}$ of $\mathcal{A}$ are sent to $\mathcal{B}', \mathcal{C}'$ respectively.
- $\mathcal{B}', \mathcal{C}'$ exactly run the algorithm of $\mathcal{B}, \mathcal{C}$, and output their output respectively.

Thus we have concluded the unclonable IND-CPA security of our game.

*Remark 1.* Notice that compared to the strengthened MOE game, our construction does not provide additional membership checking oracles.

## 5 Copy-Protection for Point Functions in QROM

### 5.1 Copy-Protection Preliminaries

Below we present the definition of a copy-protection scheme.

**Definition 7 (Copy-Protection Scheme).** *Let $\mathcal{F} = \mathcal{F}(\lambda)$ be a class of efficiently computable functions of the form $f : X \to Y$. A copy protection scheme for $\mathcal{F}$ is a pair of QPT algorithms* $(\mathsf{CopyProtect}, \mathsf{Eval})$ *such that:*

- ***Copy Protected State Generation:*** $\mathsf{CopyProtect}(1^\lambda, d_f)$ *takes as input the security parameter $1^\lambda$ and a classical description $d_f$ of a function $f \in \mathcal{F}$ (that efficiently computes $f$). It outputs a mixed state $\rho_f \in \mathcal{D}(\mathcal{H}_Z)$, where $Z$ is the output register.*
- ***Evaluation:*** $\mathsf{Eval}(1^\lambda, \rho, x)$ *takes as input the security parameter $1^\lambda$, a mixed state $\rho \in \mathcal{D}(\mathcal{H}_Z)$, and an input value $x \in X$. It outputs a bipartite state $\rho' \otimes |y\rangle\langle y| \in \mathcal{D}(\mathcal{H}_Z) \otimes \mathcal{D}(\mathcal{H}_Y)$.*

We will sometimes abuse the notation and write $\mathsf{Eval}(1^\lambda, \rho, x)$ to denote the classical output $y \in Y$ when the residual state $\rho'$ is not significant.

**Definition 8 (Correctness).** *A copy-protection scheme* $(\mathsf{CopyProtect}, \mathsf{Eval})$ *for* $\mathcal{F}$ *is* $\delta$***-correct*** *if the following holds: for every* $x \in X$, $f \in \mathcal{F}$,

$$\Pr\left[f(x) \leftarrow \mathsf{Eval}(1^\lambda, \rho_f, x) \ : \ \rho_f \leftarrow \mathsf{CopyProtect}(1^\lambda, d_f)\right] \geq \delta.$$

*If* $\delta \geq 1 - \mathsf{negl}(\lambda)$, *we simply say that the scheme is* ***correct****.*

*Remark 2.* When $\delta$ is negligibly close to 1, the evaluation algorithm $\mathsf{Eval}$ can be implemented so that it does not disturb the state $\rho_f$. This ensures that $\rho_f$ can be reused polynomially many times with arbitrary inputs.

We define security via a piracy experiment.

**Definition 9 (Piracy Experiment).** *A* ***piracy experiment*** *is a security game defined by a copy-protection scheme* $(\mathsf{CopyProtect}, \mathsf{Eval})$ *for a class of functions* $\mathcal{F}$ *of the form* $f : X \to Y$, *a distribution* $\mathcal{D}_\mathcal{F}$ *over* $\mathcal{F}$, *and a class of distributions* $\mathfrak{D}_X = \{\mathfrak{D}_X(f)\}_{f\in\mathcal{F}}$ *over* $X \times X$. *It is the following game between a challenger and an adversary, which is a triplet of algorithms* $(\mathcal{A}, \mathcal{B}, \mathcal{C})$*:*

- ***Setup Phase:*** *The challenger samples a function* $f \leftarrow \mathcal{D}_\mathcal{F}$ *and sends* $\rho_f \leftarrow \mathsf{CopyProtect}(1^\lambda, d_f)$ *to* $\mathcal{A}$.
- ***Splitting Phase:*** $\mathcal{A}$ *applies a CPTP map to split* $\rho_f$ *into a bipartite state* $\rho_{\mathsf{BC}}$*; it sends the* $\mathsf{B}$ *register to* $\mathcal{B}$ *and the* $\mathsf{C}$ *register to* $\mathcal{C}$. *No communication is allowed between* $\mathcal{B}$ *and* $\mathcal{C}$ *after this phase.*
- ***Challenge Phase:*** *The challenger samples* $(x_B, x_C) \leftarrow \mathfrak{D}_X(f)$ *and sends* $x_B, x_C$ *to* $\mathcal{B}, \mathcal{C}$, *respectively.*
- ***Output Phase:*** $\mathcal{B}$ *and* $\mathcal{C}$ *output* $y_B \in Y$ *and* $y_C \in Y$, *respectively, and send to the challenger. The challenger outputs 1 if* $y_B = f(x_B)$ *and* $y_C = f(x_C)$, *indicating that the adversary has succeeded, and 0 otherwise.*

*The bit output by the challenger is denoted by* $\mathsf{PirExp}^{\mathsf{CopyProtect},\mathsf{Eval}}_{\mathcal{D}_\mathcal{F},\mathfrak{D}_X}(1^\lambda, (\mathcal{A}, \mathcal{B}, \mathcal{C}))$.

As noted by [11], the adversary can always succeed in this game with probability negligibly close to

$$p^{\mathsf{triv}}(\mathcal{D}_\mathcal{F}, \mathfrak{D}_X) := \max_{E\in\{B,C\}} \mathop{\mathbb{E}}_{\substack{f\leftarrow\mathcal{D}_\mathcal{F}\\(x_B,x_C)\leftarrow\mathfrak{D}_X(f)}} \max_{y\in Y} \Pr\left[y \mid x_E\right]$$

by sending $\rho_f$ to $\mathcal{B}$ and have $\mathcal{C}$ guess the most likely output $y$ given input $x_C$ (or vice versa). In other words, $p^{\mathsf{triv}}$ is the success probability of optimal guessing strategy for one party $E \in \{B, C\}$ given only the test input $x_E$.

Bounding the success probability of the adversary is bounded by $p^{\mathsf{triv}}$ captures the intuition that $\rho_f$ is no more helpful for simultaneous evaluation than a black-box program that could only be given to one party.

**Definition 10 (Copy-Protection Security).** *Let* $(\mathsf{CopyProtect}, \mathsf{Eval})$ *be a copy-protection scheme for a class* $\mathcal{F}$ *of functions* $f : X \to Y$*. Let* $\mathcal{D}_{\mathcal{F}}$ *be a distribution over* $\mathcal{F}$ *and* $\mathfrak{D}_X = \{\mathfrak{D}_X(f)\}_{f\in\mathcal{F}}$ *a class of distributions over* $X$*. Then,* $(\mathsf{CopyProtect}, \mathsf{Eval})$ *is called* $(\mathcal{D}_{\mathcal{F}}, \mathfrak{D}_X)$-***secure*** *if there exists a negligible function* $\mathsf{negl}$ *such that any QPT adversary* $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ *satisfies*

$$\Pr\left[b = 1 \ : \ b \leftarrow \mathsf{PirExp}^{\mathsf{CopyProtect},\mathsf{Eval}}_{\mathcal{D}_{\mathcal{F}},\mathfrak{D}_X}\left(1^\lambda, (\mathcal{A}, \mathcal{B}, \mathcal{C})\right)\right] \leq p^{\mathsf{triv}}(\mathcal{D}_{\mathcal{F}}, \mathfrak{D}_X) + \mathsf{negl}(\lambda).$$

*Copy Protection for Point Functions* A *point function* $f_y : \{0,1\}^m \to \{0,1\}$ is of the form

$$f_y(x) = \begin{cases} 1, & x = y \\ 0, & x \neq y \end{cases}.$$

When dealing with point functions, the classical description of $f_y$ will simply be $y$, and accordingly the distribution $\mathcal{D}_{\mathcal{F}}$ over point functions will be represented by a distribution $\mathcal{D} = \mathcal{D}_\lambda$ over $\{0,1\}^m$. Since copy protection is trivially impossible for a learnable distribution $\mathcal{D}$, we are going to restrict our attention to unlearnable distributions.

**Definition 11.** *A distribution* $\mathcal{D}_\lambda$ *over* $\{0,1\}^m$*, with* $m = \mathsf{poly}(\lambda)$*, is called unlearnable if for any query-bounded adversary* $\mathcal{A}^{f_y(\cdot)}$ *with oracle access to* $f_y(\cdot)$*, we have*

$$\Pr\left[y' = y : \substack{y\leftarrow\mathcal{D}_\lambda \\ y'\leftarrow\mathcal{A}^{f_y(\cdot)}(1^\lambda)}\right] \leq \mathsf{negl}(\lambda).$$

**Definition 12 (Copy-Protection Security for Point Functions).** *Let* $m = \mathsf{poly}(\lambda)$ *and* $\mathcal{F}$ *be the class of point functions* $f_y : \{0,1\}^m \to \{0,1\}$*. Let* $\mathfrak{D}_X = \{\mathfrak{D}_X(f)\}_{f\in\mathcal{F}}$ *be a class of input distributions over* $\{0,1\}^m \times \{0,1\}^m$*. A copy protection scheme* $(\mathsf{CopyProtect}, \mathsf{Eval})$ *for* $\mathcal{F}$ *is called* $\mathfrak{D}_X$-***secure*** *if there exists a negligible function* $\mathsf{negl}$ *such that* $(\mathsf{CopyProtect}, \mathsf{Eval})$ *is* $(\mathcal{D}_\lambda, \mathfrak{D}_X)$-***secure*** *for all unlearnable distributions* $\mathcal{D}_\lambda$ *over* $\{0,1\}^m$*.*

### 5.2 Construction

In this section, we design copy-protection for a class of point functions. We set $n = 2\lambda$ and $d = \lambda$ throughout the section. Our construction will use two hash functions: (a) $G : \{0,1\}^\lambda \to \{0,1\}^{n\cdot d}$ and (b) $H : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \{0,1\}^{4n+\lambda}$. In the security proof, we will treat $G$ and $H$ as random oracles. We will use $\mathbb{F}_2^n$ and $\{0,1\}^n$ interchangeably.

We denote the set of all $d$-dimensional subspaces of $\mathbb{F}_2^n$ by $\mathcal{S}_d$.

We describe the copy-protection scheme $(\mathsf{CopyProtect}, \mathsf{Eval})$ for a class of point functions $\mathcal{F} = \{f_y(\cdot)\}_{y\in\{0,1\}^\lambda}$ as follows:

- $\mathsf{CopyProtect}\left(1^\lambda, y\right)$: it takes as input $\lambda$ in unary notation, $y \in \{0,1\}^\lambda$ and does the following:

1. Compute $\mathbf{v} = G(y)$. Parse $\mathbf{v}$ as a concatenation of $d$ vectors $v_1, \ldots, v_d$, where each $v_i$ has dimension $n$. Abort if the vectors $\{v_1, \ldots, v_d\}$ are not linearly independent.
2. Let $A = \mathrm{Span}\,(v_1, \ldots, v_d)$.
3. Sample $s \leftarrow \mathsf{CS}(A)$ and $s' \leftarrow \mathsf{CS}(A^{\perp})$ uniformly at random.
4. Output the copy-protected state $\sigma = |A_{s,s'}\rangle\langle A_{s,s'}|_{\mathbf{X}} \otimes |H(s,s')\rangle\langle H(s,s')|_{\mathbf{Y}}$.

– $\mathsf{Eval}(\sigma, x)$: on input the copy-protected state $\sigma \in \mathcal{D}(\mathcal{H}_{\mathbf{X}} \otimes \mathcal{H}_{\mathbf{Y}})$, input $x \in \{0,1\}^{\lambda}$, it does the following:

1. Measure the register $\mathbf{Y}$ of $\sigma$ to obtain the value $\theta$. Call the resulting state $\sigma'$.
2. Compute $\mathbf{v} = G(x)$. Parse $\mathbf{v}$ as a concatenation of $d$ vectors $v_1, \ldots, v_d$, where each $v_i$ has dimension $n$. Abort if the vectors $\{v_1, \ldots, v_d\}$ are not linearly independent.
3. Let $A = \mathrm{Span}\,(v_1, \ldots, v_d)$.
4. Apply $U_A$ coherently on $\sigma' \otimes |0^{2n}\rangle\langle 0^{2n}|_{\mathbf{Z}} \otimes |0^{\mathsf{poly}(\lambda)}\rangle\langle 0^{\mathsf{poly}(\lambda)}|_{\mathbf{anc}}$ to obtain the state $\sigma''$, where $U_A$ is a unitary that computes $(s, s')$ given $|A_{s,s'}\rangle$.
5. Query $H$ on the register $\mathbf{Z}$ and store the answer in a new register $\mathbf{out}$.
6. Measure the register $\mathbf{out}$ in the computational basis. Denote the post-measurement state by $\sigma_{\mathbf{out}}$ and the measurement outcome by $\theta'$.
7. If $\theta = \theta'$, output $\sigma_{\mathbf{out}} \otimes |1\rangle\langle 1|$. Otherwise, output $\sigma_{\mathbf{out}} \otimes |0\rangle\langle 0|$.

We first discuss at a high level why this construction works. Regarding correctness, we argue that Eval on input $x \neq y$ computes a random subspace $A'$, such that $|A'_{s,s'}\rangle$ is nearly orthogonal to $|A_{s,s'}\rangle$. As a result, Eval recovers $(s, s')$ incorrectly. Since as a sufficiently expanding hash function $H$ is injective with high probability, Eval fails.

As for security, first we show that it is hard for $\mathcal{A}$ to query the oracles $G, H$ on inputs $y, (s, s')$. Next, we argue that $\mathcal{B}$ and $\mathcal{C}$ cannot both recover $(s, s')$, otherwise they break the MOE game in Theorem 11.

We give the formal statements below. Detailed proofs can be found in the full version.

**Lemma 7.** $(\mathsf{CopyProtect}, \mathsf{Eval})$ *satisfies correctness.*

**Lemma 8.** $(\mathsf{CopyProtect}, \mathsf{Eval})$ *is a $\mathfrak{D}_X$-secure copy-protection scheme for point functions with input length $\lambda$, where $\mathfrak{D}_X(y) = \mathfrak{D}_y^B \times \mathfrak{D}_y^C$ is a product distribution.*

*Remark 3.* In our security proof, the adversary can run in unbounded time as long as it is query-bounded.

*Remark 4.* Using techniques from the proof of Theorem 12, our scheme can also be shown to be secure for the case when $\mathfrak{D}_X(y)$ samples correlated test inputs, i.e. the case when either $x_B = x_C = y$ or $x_B, x_C$ are both random.

## References


[1] Scott Aaronson. "Quantum copy-protection and quantum money". In: *2009 24th Annual IEEE Conference on Computational Complexity*. IEEE. 2009, pp. 229–242 (cit. on pp. 2, 12).

[2] Scott Aaronson and Paul Christiano. "Quantum money from hidden subspaces". In: *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*. 2012, pp. 41–60 (cit. on p. 2).

[3] Scott Aaronson, Jiahui Liu, Qipeng Liu, Mark Zhandry, and Ruizhe Zhang. "New approaches for quantum copy-protection". In: *Annual International Cryptology Conference*. Springer. 2021, pp. 526–555 (cit. on pp. 2, 12, 16).

[4] Ryan Amos, Marios Georgiou, Aggelos Kiayias, and Mark Zhandry. "One-shot signatures and applications to hybrid quantum/classical authentication". In: *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*. 2020, pp. 255–268 (cit. on p. 2).

[5] Prabhanjan Ananth and Fatih Kaleoglu. "Unclonable Encryption, Revisited". In: *Theory of Cryptography Conference*. Springer. 2021, pp. 299–329 (cit. on pp. 2, 3, 5, 6, 12, 17).

[6] Prabhanjan Ananth and Rolando L La Placa. "Secure Software Leasing". In: *Eurocrypt* (2021) (cit. on pp. 2, 3, 13).

[7] Charles H Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. "Strengths and weaknesses of quantum computing". In: *SIAM journal on Computing* 26.5 (1997), pp. 1510–1523 (cit. on pp. 13, 14).

[8] Anne Broadbent, Stacey Jeffery, Sébastien Lord, Supartha Podder, and Aarthi Sundaram. "Secure software leasing without assumptions". In: *Theory of Cryptography Conference*. Springer. 2021, pp. 90–120 (cit. on p. 13).

[9] Anne Broadbent and Sébastien Lord. "Uncloneable Quantum Encryption via Oracles". In: *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*. Ed. by Steven T. Flammia. Vol. 158. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2020, 4:1–4:22. DOI: 10.4230/LIPIcs.TQC.2020.4 (cit. on pp. 2, 4, 6–10, 12, 17).

[10] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. "Hidden cosets and applications to unclonable cryptography". In: *Annual International Cryptology Conference*. Springer. 2021, pp. 556–584 (cit. on pp. 2, 5, 8, 9, 13, 18, 19, 25).

[11] Andrea Coladangelo, Christian Majenz, and Alexander Poremba. *Quantum copy-protection of compute-and-compare programs in the quantum random oracle model*. 2020. arXiv: 2009.13865 [quant-ph] (cit. on pp. 2, 3, 6, 13, 26).

[12] Eric Culf and Thomas Vidick. "A monogamy-of-entanglement game for subspace coset states". In: *arXiv preprint arXiv:2107.13324* (2021) (cit. on pp. 9, 19).

[13] Marios Georgiou and Mark Zhandry. "Unclonable decryption keys". In: *IACR Cryptol. ePrint Arch* 877.2020 (2020), p. 3 (cit. on p. 2).

[14] Daniel Gottesman. "Uncloneable encryption". In: *arXiv preprint quant-ph/0210062* (2002) (cit. on p. 2).
[15] Andrew Lutomirski. "An online attack against Wiesner's quantum money". In: *arXiv preprint arXiv:1010.0256* (2010) (cit. on p. 9).
[16] Christian Majenz, Christian Schaffner, and Mehrdad Tahmasbi. "Limitations on Uncloneable Encryption and Simultaneous One-Way-to-Hiding". In: (Nov. 2021). arXiv: 2103.14510 [quant-ph] (cit. on pp. 4, 6, 8, 12).
[17] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667 (cit. on p. 13).
[18] Roy Radian and Or Sattath. "Semi-quantum money". In: *Journal of Cryptology* 35.2 (2022), pp. 1–70 (cit. on p. 2).
[19] Oded Regev. *Witness-preserving Amplification of QMA*. 2005. URL: https://cims.nyu.edu/~regev/teaching/quantum_fall_2005/ln/qma.pdf (cit. on p. 14).
[20] Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. "A monogamy-of-entanglement game with applications to device-independent quantum cryptography". In: *New Journal of Physics* 15.10 (2013), p. 103002. DOI: 10.1088/1367-2630/15/10/103002 (cit. on p. 7).
[21] Dominique Unruh. "Revocable Quantum Timed-Release Encryption". In: *J. ACM* 62.6 (Dec. 2015). ISSN: 0004-5411. DOI: 10.1145/2817206 (cit. on p. 8).
[22] Thomas Vidick. *Lecture Notes on Interactive proofs with quantum devices*. 2021. URL: http://users.cms.caltech.edu/~vidick/teaching/fsmp/lecture1.pdf (cit. on p. 14).
[23] Thomas Vidick and Tina Zhang. "Classical proofs of quantum knowledge". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2021, pp. 630–660 (cit. on p. 8).
[24] Stephen Wiesner. "Conjugate coding". In: *ACM Sigact News* 15.1 (1983), pp. 78–88 (cit. on pp. 1, 7).
[25] Mark Zhandry. "Quantum lightning never strikes the same state twice. or: quantum money from cryptographic assumptions". In: *Journal of Cryptology* 34.1 (2021), pp. 1–56 (cit. on pp. 2, 5).
[26] Mark Zhandry. "Schrödinger's pirate: How to trace a quantum decoder". In: *Theory of Cryptography Conference*. Springer. 2020, pp. 61–91 (cit. on pp. 11, 16).