Revocable Encryption, Programs, and More: The Case of Multi-Copy Security

Prabhanjan Ananth
University of California, Santa Barbara, CA, USA

Saachi Mutreja
Columbia University, New York, NY, USA

Alexander Poremba
Massachusetts Institute of Technology, Cambridge, MA, USA

Abstract

Fundamental principles of quantum mechanics have inspired many new research directions, particularly in quantum cryptography. One such principle is *quantum no-cloning* which has led to the emerging field of revocable cryptography. Roughly speaking, in a revocable cryptographic primitive, a cryptographic object (such as a ciphertext or program) is represented as a quantum state in such a way that surrendering it effectively translates into losing the capability to use this cryptographic object. All of the revocable cryptographic systems studied so far have a major drawback: the recipient only receives one copy of the quantum state. Worse yet, the schemes become completely insecure if the recipient receives many identical copies of the *same* quantum state – a property that is clearly much more desirable in practice. While multi-copy security has been extensively studied for a number of other quantum cryptographic primitives, it has so far received only little treatment in context of unclonable primitives. Our work, for the first time, shows the feasibility of revocable primitives, such as revocable encryption and revocable programs, which satisfy multi-copy security in oracle models. This suggest that the stronger notion of multi-copy security is within reach in unclonable cryptography more generally, and therefore could lead to a new research direction in the field.

2012 ACM Subject Classification Theory of computation → Cryptographic primitives

Keywords and phrases quantum cryptography, unclonable primitives

Digital Object Identifier 10.4230/LIPIcs.ITC.2025.9

Related Version *Full Version*: https://eprint.iacr.org/2024/1687

Funding *Prabhanjan Ananth*: Supported by the National Science Foundation under the grants FET-2329938 and the Career award (2341004).
Saachi Mutreja: Supported by AFOSR award FA9550-21-1-0040, NSF CAREER award CCF-2144219, and the Sloan Foundation.
Alexander Poremba: Supported by the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Co-design Center for Quantum Advantage (C2QA) under contract number DE-SC0012704.

Acknowledgements The authors would like to thank Henry Yuen and Tal Malkin for many useful discussions.

1 Introduction

Designing mechanisms to provably revoke cryptographic capabilities is an age-old problem [46, 45]. In the public-key infrastructure, certificate authorities have the ability to invalidate public-key certificates [49], especially when the certificates have been compromised. Key rotation policies [29] guarantee that outdated decryption keys become ineffective for future use. The existing approaches to tackle with this problem have their limitations owing to the

6th Conference on Information-Theoretic Cryptography (ITC 2025).
Editor: Niv Gilboa; Article No. 9; pp. 9:1–9:23
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

fact that cryptographic secrets are represented as binary strings and hence, it is infeasible to provably ensure that the malicious attackers have erased information from their devices. In the context of key rotation, a compromised key can still be used to decrypt old ciphertexts. Another issue with using classical information to represent cryptographic keys is that it is difficult to detect compromise: a hacker could steal the classical key from a device without leaving a trace.

Recently, a line of works [47, 11, 5, 13, 28, 41, 8] have leveraged quantum information and proposed new approaches for provable revocation of cryptographic objects, such as ciphertexts, programs and keys. These works studied revocation in the context of many Crypto 101 primitives, including pseudorandom functions, private-key and public-key encryption and digital signatures. In a revocable cryptographic primitive, an object (such as a program or a decryption key, etc.) is associated with a quantum state in such a way that *only with access to the state* the functionality of the original cryptographic object is retained. The common template for defining revocable security is in the form of a cryptographic game: The adversary receives *one copy* of the quantum state that it can use for a limited period of time after which it is supposed to return back the state to the owner. The security guarantee stipulates that after the state is returned, the adversary effectively loses the capability to use the cryptographic object. At this point, it should be clear to the reader the necessity that such cryptographic objects are represented as quantum states: indeed, if they were classical, the adversary could always maintain a secret copy, while pretending to have erased everything from its device. On the other hand, the no-cloning theorem [50, 32] of quantum mechanics suggests that the above security experiment could very well be achieved.

Multi-Copy Security

Let us now zoom in on the part of the security experiment, where the adversary receives *only one copy* of the quantum state. In all of the prior works in the literature so far [5, 13, 28, 41, 8], this limitation persists. One could consider a more general definition, where the adversary receives *k identical* copies of the quantum state and is later asked to return back all of the copies of the state. The security guarantee is similar to before: after returning all of the *k* copies, the adversary should effectively lose all access to the underlying crytptographic object. We term this general security experiment to be *multi-copy security.*

There are a couple of reasons to study multi-copy security for revocable primitives.

- Historical Context: Multi-copy security is not new and has been extensively studied in quantum cryptography, especially in the context of foundational primitives such as pseudorandom states [35, 23, 14, 7, 21, 22] and one-way state generators [43, 42]. Indeed, multi-copy security has been crucial in the design of many cryptographic constructions. The works of [7, 12, 37] used tomography, which inherently requires multiple copies in order to dequantize the communication in some of the quantum cryptographic primitives. Specifically for revocable primitives, a conceptual reason to study multi-copy security is to understand whether having more copies necessarily makes it easier for the adversary to clone quantum states. Investigating multi-copy security for revocable primitives is a starting step towards understanding multi-copy security for more advanced primitives such as public-key quantum money [3, 52]. The question of whether multi-copy security is possible in unclonable cryptography was also recently raised in [40].
- Nested Leasing: Having access to many more copies of the quantum state would also give more power to the user; for example, using a permutation test [36] (a generalized version of SWAP test) where one is given $|\phi\rangle$ and polynomially many copies of $|\psi\rangle$, one can approximately test the overlap between $|\phi\rangle$ and $|\psi\rangle$. This ability allows for nested

leasing of cryptographic objects, such as programs or keys. Suppose a user **A** is leased a large number of, say k, copies of a quantum program $|\psi\rangle$. User **A** could further lease a number, say $k' \ll k$, of copies of $|\psi\rangle$ to user **B**. At a later point in time, when user **B** is asked to return back its copies to user **A**. User **A** can then use its $k - k'$ copies to approximately test whether the returned copies are correct. If the test succeeds, user **A** then is in a position to return back all of its k copies to the true owner[1]. Such a nested leasing approach could be especially useful in organizations with hierarchical structure.

The notion of multi-copy security we consider in this work is closely related to *collusion-resistant security*, considered in the works of [39, 27]. The crucial difference is that in the prior works, the adversary receives *i.i.d* copies of the quantum key whereas in our case, the adversary receives *identical* copies of the quantum key. In the nested leasing application discussed above, it was crucial that the user received many *identical* copies of the same state.

Multi-copy security using commonly studied unclonable states: Challenges

The first step towards addressing multi-copy security is to identify quantum states that are unclonable. We discuss the commonly studied unclonable quantum states below:

- BB84 STATES: these states are of the form $H^\theta |x\rangle$, where $\theta \in \{0,1\}^n$ and $x \in \{0,1\}^n$. These states have been influential in the design of private-key quantum money [48] and in the design of encryption schemes with unclonable ciphertexts [26, 24]. Given many copies of $H^\theta |x\rangle$, one can learn x and θ and hence, recover a complete description of $H^\theta |x\rangle$.
- SUBSPACE AND COSET STATES: these states are of the form $(\sqrt{|A|})^{-1} \cdot \sum_{\mathbf{x} \in A} |\mathbf{x}\rangle$, where $A \subseteq \mathbb{F}_2^n$ is a sparse subspace of $\mathbb{F}_2^n$, for some $n \in \mathbb{N}$. These states have been crucial in the design of public-key quantum money [3, 52], among other primitives. Again given many copies, one can learn the basis of the subspace and hence a complete description of the subspace state. Another related class of unclonable states are coset states which are superpositions over a coset (rather than a subspace) and moreover, each term in the superposition has a phase that depends on a dual coset. Coset states have been influential in constructions of quantum copy-protection [30]. Similar to subspace states, coset states are also learnable.
- SIS-BASED STATES: these states are of the form $\sum_{\mathbf{x} \in \mathbb{Z}_q^m, \mathbf{A}\mathbf{x}=\mathbf{y}} \alpha_{\mathbf{x}} |\mathbf{x}\rangle$, where $q, m \in \mathbb{N}$, $|\alpha_{\mathbf{x}}|^2$ is a discrete Gaussian distribution such that most of the weight is on low norm vectors $\mathbf{x}$ and finally, $\mathbf{A} \in \mathbb{Z}_q^{n \times m}, \mathbf{y} \in \mathbb{Z}_q^n$. They were useful in designing traditional and advanced encryption systems with unclonable quantum keys [44, 13, 41, 8]. Given many copies of this state, one can recover a short basis of the kernel of $\mathbf{A}$ which can then be used to recover the above state.

In other words, all the above types of states are learnable and hence, they cannot be the basis of any unclonable cryptographic scheme satisfying multi-copy security. This suggests that we need to look for new unclonable quantum states that are unlearnable even given many copies. In the past, discovering new unclonable quantum states has led to pushing the frontier of unclonable quantum cryptographic primitives and we believe our endeavour could reap similar results.

[1] A drawback of this approach is that there is some room for user **B** to cheat with noticeable probability in this approach without user **A** noticing, which means that the owner would not always be to pinpoint whether user **A** or user **B** cheated. Still, this approach offers a non-trivial solution to this challenging problem.

2 Our Results

We now give an overview of our results.

Our Approach: Quantum Pseudorandomness Meets Unclonable Cryptography

We use *subset states* to tackle multi-copy security. Subset states have been recently studied in the context of quantum pseudorandomness [33, 34, 2]. A subset state is associated with an unstructured and random subset $S \subset \{0,1\}^n$ of the form $|S\rangle = (\sqrt{|S|})^{-1}\sum_{x \in S}|x\rangle$. Several recent works [33, 34] showed that random subset states (of non-trivial size) are approximate state k-designs for any polynomial k as a function of $n \in \mathbb{N}$, which make random subset states[2] a natural candidate for multi-copy security – particularly since Haar states are unlearnable given polynomially many identical copies. At first sight, it would seem as though that the fact that random subset states are close to Haar states should be discourage us from using them for unclonable cryptography, especially since Haar states have virtually no structure. Indeed, the structure of BB84 states, subspace states and others has been crucially exploited in various applications. Our work shows that subset states, in some sense, have the minimal amount of structure to enable a number of interesting cryptographic primitives in the context of multi-copy revocable cryptography. To the best of our knowledge, these applications also mark the first use case of subset states in the context of cryptography. Our main technical contribution is of *information-theoretic* nature: we prove a query lower bound for *forging* subset elements; concretely, we show that any quantum algorithm that receives k copies of a random subset state $|S\rangle$ cannot produce $k+1$ many subset elements in S unless it makes a large amount of queries to a membership oracle for S. We believe that this result could be of independent interest.

Multi-Copy Revocable Encryption. We first study revocable encryption [47, 5, 13] with multi-copy security. A revocable encryption scheme is a regular encryption scheme but where the ciphertexts are associated with quantum states. Additionally, a revocable encryption scheme comes with the following security notion called *multi-copy revocable security*: informally, it states that any adversary that successfully returns k valid copies of a quantum ciphertext which it was given by a challenger, where k is an arbitrary polynomial, necessarily loses the ability to decrypt the ciphertexts in the future – even if the secret key is revealed. In more detail, the security game is formulated as follows:

- The adversary selects a pair of messages (m_0, m_1) and sends them to the challenger.
- The challenger randomly selects one of the two messages, say m_b, and encrypts it k times using a secret ket sk, and sends the ciphertext copies $|\psi_b\rangle^{\otimes k}$ to the adversary $\mathcal{A}$.
- At a later point in time, $\mathcal{A}$ returns back all the copies of $|\psi_b\rangle$, which are then verified by the challenger.
- After successfully returning back the states, $\mathcal{A}$ receives the secret key sk in the clear. Finally, $\mathcal{A}$ outputs a guess b'.

The scheme is said to be secure if the probability that $b' = b$ is close to $1/2$.

Prior works [47, 5, 13, 28, 8] only studied variants of the above security game in the setting where the adversary receives only one copy of the quantum ciphertext. In fact, their schemes are easily seen to not satisfy multi-copy security. We show the following.

[2] Strictly speaking, we use *pseudorandom* subset states which can be generated efficiently via pseudorandom permutations.

▶ **Theorem 1.** *If post-quantum one-way functions exist, then there exists an encryption scheme with (an oracular notion of) multi-copy revocable security.*

Some remarks are in order. Firstly, our security proof does not fully achieve the standard notion of revocable security guarantee we stated above; rather, we consider a slightly different variant of the experiment, where in the second part of the game (instead of revealing the secret key in the clear) we allow the adversary to query an oracle that is powerful enough to enable decryption during the first phase of the game. While this constitutes a weaker notion of security, it nevertheless results in a meaningful notion of revocable security: once the adversary has successfully returned all of the copies of the ciphertext, it can no longer decrypt the ciphertext in the future – even if it gets access to an oracle that would have previously allowed it to do so. Second, our construction of multi-copy revocable encryption makes use of quantum-secure pseudorandom permutations (QPRPs), which can be constructed from post-quantum one-way functions [51]. In the security experiment which underlies our construction, the aforementioned oracle for decryption (i.e., that which is handed to the adversary after revocation has taken place) is in the form of an ideal oracle for the permutation itself. Once again, the rationale behind our notion of oracular security is that an attacker who receives a QPRP key in the clear would most certainly use it to evaluate the QPRP, and hence it is reasonable to consider a model in which the attacker receives an oracle for the permutation instead.[3] A key advantage of oracular security is that we can directly invoke the security of the QPRP and use a perfectly random permutation instead. [4] We remark that this model loosely resembles the random permutation model behind the international hash function standard SHA-3 [19, 20], except that the adversary only receives oracle access to the permutation during the second part of the revocable security experiment. While our construction only achieves an oracular notion of revocable security, it is nevertheless the very first construction of revocable encryption which satisfies multi-copy security *in any model.*

Multi-Copy Revocable Programs

Our previous discussion on revocable encryption illustrates that encryption and decryption functionalities can be protected even if many copies of the quantum ciphertext are made available to the recipient. We generalize this result further and study whether arbitrary functionalities can be protected. We define and study revocable programs with multi-copy security. In this notion, there is a functionality preserving compiler that takes a program and converts it into a quantum state. The security guarantee is defined similar to revocable encryption:

- The challenger compiles a program P, sampled from a distribution $\mathcal{D}$ on a set of programs $\mathcal{P}$, into a state $|\psi_P\rangle$. It then sends k copies of the state $|\psi_P\rangle$ to the adversary $\mathcal{A}$.
- At a later point in time, $\mathcal{A}$ returns back all of the copies of $|\psi_P\rangle$.
- After returning back the state, $\mathcal{A}$ is given x, where x is sampled from the input distribution of P. It then outputs a guess y.

The scheme is said to be secure if the probability that $y = P(x)$ is roughly close to the trivial success probability. Here, the trivial success probability is defined as the optimal probability of guessing $P(x)$ given just x (and the knowledge of $\mathcal{D}$ and the input distribution).

[3] Note, however, that this does not capture all possible attacks; for example, the adversary could use its knowledge of the QPRP key to break the scheme in other meaningful ways.

[4] This switch is generally not possible in the standard notion of revocable security in which the QPRP key is required to revealed in the clear. Here, QPRP security does not apply.

Prior works propose revocable programs for specific functionalities in the plain model [30] or for general functionalities in oracle models [4]. However, these works guarantee security only if the adversary receives one copy of the state. And as before, these constructions provably do not satisfy multi-copy security. We show the following.

▶ **Theorem 2.** *There exist revocable programs which satisfy (an oracular notion of) multi-copy security in a classical oracle model.*

Unlike Theorem 1, the above theorem relies upon structured and ideal classical oracles.

Finally, for the special case of point functions, we show that we can again only rely upon pseudorandom permutations together with the (standard) quantum random oracle model. We show the following.

▶ **Theorem 3.** *There exist revocable multi-bit point functions which satisfy (an oracular notion of) multi-copy security in quantum random oracle model.*

Our results and techniques opens the door for building more advanced unclonable primitives that preserve their security even if the adversary receives many copies of the unclonable quantum state.

Are Results in Oracle Models Interesting?

It is natural for a reader to be skeptical of our results given that they are based in the oracle models. However, we would like to emphasize that achieving results in the oracle models still requires non-trivial amount of effort. As history suggests, constructions in the oracle models have eventually been adopted to constructions in the plain model. A classic example is the construction of public-key quantum money, which was first proposed in the oracle models by Aaronson and Christiano [3] and later, being instantiated in the plain model by Zhandry [52]. In a similar vein, our techniques could be useful for future works on achieving multi-copy security in the plain model.

Applications to Sponge Hashing

As a complementary contribution, we show that the techniques we developed in this paper are more broadly applicable and extend to other cryptographic settings as well. Here, we single out the so-called *sponge construction* used in SHA-3 [19, 20].

We study a simple query problem: Suppose that an adversary receives as input a hash table for a set of random input keys, where each hash is computed using a *salted* (one-round) sponge hash function. How many quantum queries are necessary to find a new *valid* element in the range of the hash function? Our contribution is a space-time trade-off which precisely characterizes the hardness of finding hash table elements in the presence of oracles that depend non-trivially on the sponge hash function.

2.1 Related work

We now discuss related notions which are relevant to this work.

Copy-Protection

This notion was first introduced by Aaronson [1]. Informally speaking, a copy-protection scheme is a compiler that transforms programs into quantum states in such a way that using the resulting states, one can run the original program. Yet, the security guarantee stipulates that any adversary given one copy of the state cannot produce a bipartite state wherein both parts compute the original program. Copy-protection schemes have since been constructed for various classes of programs and under various different models, for example as in [1, 4, 31, 9, 10, 39, 27]. We remark, however, that all of the aforementioned works are completely insecure if multiple identical copies of the program are made available. The notion of multi-copy security we consider in this work is closely related to *collusion-resistant security*, considered in the works of [39, 27]. The crucial difference is that in the prior works, the adversary receives *i.i.d* copies of the quantum key whereas in our case, the adversary receives *identical* copies of the quantum key.

Secure Software Leasing

Another primitive relevant to revocable cryptography is secure software leasing [11]. The notion of secure software leasing states that any program can be compiled into a functionally equivalent program, represented as a quantum state, in such a way that once the compiled program is returned, the (honest) evaluation algorithm on the residual state cannot compute the original functionality. Secure leasing has been constructed for various functionalities [11, 31, 25, 38]. Similar to copy-protection, none of the aforementioned works consider multi-copy security.

Encryption Schemes with Revocable Ciphertexts

Unruh [47] proposed a (private-key) quantum timed-release encryption scheme that is *revocable*, i.e. it allows a user to *return* the ciphertext of a quantum timed-release encryption scheme, thereby losing all access to the data. Broadbent and Islam [24] introduced the notion of *certified deletion*, which is incomparable with the related notion of unclonable encryption. This has led to the development of other certified deletion protocols, for example as in Ref. [44, 15, 17, 16, 18]. However, the notion of multi-copy security, such as in our work, has not been studied.

3 Preliminaries

Let $\lambda \in \mathbb{N}$ denote the security parameter throughout this work. We assume that the reader is familiar with the fundamental cryptographic concepts.

For $N \in \mathbb{N}$, we use $[N] = \{1, 2, \ldots, N\}$ to denote the set of integers up to N. The symmetric group on $[N]$ is denoted by S_N. In slight abuse of notation, we oftentimes identify elements $x \in [N]$ with bit strings $x \in \{0,1\}^n$ via their binary representation whenever $N = 2^n$ and $n \in \mathbb{N}$. Similarly, we identify permutations $\pi \in S_N$ with permutations $\pi : \{0,1\}^n \to \{0,1\}^n$ over bit strings of length n. For a bit string $x \in \{0,1\}^n$, we frequently use the notation $(x||*)$, where $*$ serves as a placeholder to denote the set $\{(x||y) \,:\, y \in \{0,1\}^m\}$, where $m \in \mathbb{N}$ is another integer which is typically clear in context.

We write $\mathsf{negl}(\cdot)$ to denote any *negligible* function, which is a function f such that, for every constant $c \in \mathbb{N}$, there exists an integer N such that for all $n > N$, $f(n) < n^{-c}$.

▶ **Lemma 4** (One-Way-to-Hiding Lemma, [6]). *Let $\mathcal{X}, \mathcal{Y}$ be arbitrary sets and let $\mathcal{S} \subseteq \mathcal{X}$ be a (possibly random) subset. Let $G, H : \mathcal{X} \to \mathcal{Y}$ be arbitrary (possibly random) functions such that $H(x) = G(x)$, for all $x \notin \mathcal{S}$. Let z be a classical bit string or a (possibly mixed) quantum state (Note that G, H, S, z may have arbitrary joint distribution). Let $\mathcal{A}$ be an oracle-aided quantum algorithm that makes at most q quantum queries. Let $\mathcal{B}$ be an algorithm that on input z chooses a random query index $i \leftarrow [q]$, runs $\mathcal{A}^H(z)$, measures $\mathcal{A}$'s i-th query and outputs the measurement outcome. Then, we have*

$$\left|\Pr\left[\mathcal{A}^G(z) = 1\right] - \Pr\left[\mathcal{A}^H(z) = 1\right]\right| \leq 2q\sqrt{\Pr[\mathcal{B}^H(z) \in \mathcal{S}]}.$$

Moreover, for any fixed choice of G, H, S and z (when z is a classical string or a pure state), we get

$$\| \, |\psi_q^H\rangle - |\psi_q^G\rangle \, \| \leq 2q \sqrt{\frac{1}{q} \sum_{i=0}^{q-1} \| \Pi_{\mathcal{S}} \, |\psi_i^H\rangle \, \|^2},$$

where $|\psi_i^H\rangle$ denotes the intermediate state of $\mathcal{A}$ just before the $(i+1)$-st query, where the initial state at $i = 0$ corresponds to z, and $\Pi_{\mathcal{S}}$ is a projector onto $\mathcal{S}$.

Pseudorandom Permutations

A quantum-secure pseudorandom permutation is a a bijective function family which can be constructed from quantum-secure one-way functions [51].

▶ **Definition 5** (QPRP). *Let $\lambda \in \mathbb{N}$ denote the security parameter. Let $P : \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^n$ be a function, where $n(\lambda) = \mathrm{poly}(\lambda)$ is an integer, such that each function $P_k(x) = P(k,x)$ in the corresponding family $\{P_k\}_{k \in \{0,1\}^\lambda}$ is bijective. We say P is a (strong) quantum-secure pseudorandom permutation (or QPRP) if, for every QPT $\mathcal{A}$ with access to both the function and its inverse, it holds that*

$$\left| \Pr_{k \sim \{0,1\}^\lambda} \left[\mathcal{A}^{P_k, P_k^{-1}}(1^\lambda) = 1 \right] - \Pr_{\varphi \sim \mathcal{P}_n} \left[\mathcal{A}^{\varphi, \varphi^{-1}}(1^\lambda) = 1 \right] \right| \leq \mathsf{negl}(\lambda),$$

where $\mathcal{P}_n$ denotes the set of permutations over n-bit strings.

Subset States

We consider the following notations.

- We denote the set of distinct k-tuples over a set S by $\mathrm{dist}(S, k)$.
- Suppose S is a set. We denote $|S\rangle = \frac{1}{\sqrt{|S|}} \sum_{x \in S} |x\rangle$.
- Suppose $X = \{x_1, \ldots, x_t\} \subseteq \{0,1\}^n$. We denote $|\boldsymbol{\sigma}_X\rangle = \frac{1}{t!} \sum_{\sigma \in S_t} |x_{\sigma(1)}, \ldots, x_{\sigma(t)}\rangle$, where S_t denotes the symmetric group on $[t]$.

We use the following lemma which follows from Propositions 3.3 and 3.4 in [34].

▶ **Lemma 6** ([34]). *Let $n, k \in \mathbb{N}$. Let $T \subseteq \{0,1\}^n$ be a subset of size $|T| = t$. Then, it holds that*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\substack{S \subseteq T \\ |S| = s}} \left[|S\rangle\langle S|^{\otimes k} \right], \mathop{\mathbb{E}}_{\substack{X \subseteq T \\ |X| = k}} \left[|\boldsymbol{\sigma}_X\rangle\langle \boldsymbol{\sigma}_X| \right] \right) \leq O\left(\frac{k}{\sqrt{s}} + \frac{sk}{t} \right).$$

4 $k \mapsto k+1$ Unforgeability of Subset States

We now prove the following theorem. Roughly speaking, our theorem says that any quantum algorithm which receives k copies of a random subset state $|S\rangle$ (and a membership oracle for S) cannot find $k+1$ distinct elements in S with high probability unless it makes a large number of queries.

▶ **Theorem 7** ($k \mapsto k+1$ Unforgeability of Subset States)**.** *Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Then, for any q-query quantum oracle algorithm $\mathcal{A}$, and any $1 \leq k < s < t \leq 2^n$, it holds that*

$$\Pr_{\substack{S \subseteq \{0,1\}^n \\ |S|=s}}\left[(x_1,\dots,x_{k+1}) \in \mathrm{dist}(S,k+1) \,:\, (x_1,\dots,x_{k+1}) \leftarrow \mathcal{A}^{\mathcal{O}_S}(|S\rangle^{\otimes k})\right]$$
$$\leq O\left(q \cdot \sqrt{\frac{t-s}{2^n}} + q \cdot \sqrt{\frac{t-k}{2^n}} + \frac{k}{\sqrt{s}} + \frac{sk}{t}\right) + \mathsf{negl}(n).$$

In particular, we can let $k = \mathrm{poly}(n)$, $q = \mathrm{poly}(n)$ and $s(n) = n^{\omega(1)}$ be superpolynomial. Then, for any $t(n) = n^{\omega(1)}$ with $s(n)/t(n) = 1/n^{\omega(1)}$ and $t(n)/2^n = 1/n^{\omega(1)}$, the probability is at most $\mathsf{negl}(n)$.

Proof. Using Lemma 8, we can prove Theorem 7 as follows: Let's assume for contradiction that there exists a q query quantum oracle algorithm $\mathcal{A}$, and a $1 \leq k < s < t \leq 2^n$, such that

$$\Pr_{\substack{S \subseteq \{0,1\}^n \\ |S|=s}}\left[(x_1,\dots,x_{k+1}) \in \mathrm{dist}(S,k+1) \,:\, (x_1,\dots,x_{k+1}) \leftarrow \mathcal{A}^{\mathcal{O}_S}(|S\rangle^{\otimes k})\right]$$
$$= O\left(q \cdot \sqrt{\frac{t-s}{2^n}} + q \cdot \sqrt{\frac{t-k}{2^n}} + \frac{k}{\sqrt{s}} + \frac{sk}{t}\right) + \delta(n).$$

where $\delta(.)$ is some non negligible function. Then, from Lemma 8, this implies that,

$$\Pr_{X \subseteq \{0,1\}^n, |X|=k}\left[(x_1,\dots,x_{k+1}) \in \mathrm{dist}(X,k+1) \,:\, (x_1,\dots,x_{k+1}) \leftarrow \mathcal{A}^{\mathcal{O}_X}(|\boldsymbol{\sigma}_X\rangle)\right]$$
$$\geq \delta(n)$$

However, the probability that $\mathcal{A}$ can succeed in this experiment is 0. This is because, X only contains k elements, and therefore, $\mathcal{A}$ can never produce $k+1$ distinct elements from X. This must imply that $\delta(n)$ is negligible. ◀

Technical Lemma

We need to show the following lemma which made use of in Theorem 7.

▶ **Lemma 8.** *Let $n, k, t \in \mathbb{N}$ be integers such that $1 \leq k < s < t \leq 2^n$. Then, for any q-query quantum oracle algorithm $\mathcal{D}$ which outputs a single bit, it holds that*

$$\left| \Pr_{\substack{S \subseteq \{0,1\}^n \\ |S|=s}}\left[\mathcal{D}^{\mathcal{O}_S}\left(|S\rangle^{\otimes k}\right) = 1\right] - \Pr_{\substack{X \subseteq \{0,1\}^n \\ |X|=k}}\left[\mathcal{D}^{\mathcal{O}_X}\left(|\boldsymbol{\sigma}_X\rangle\right) = 1\right] \right|$$
$$\leq O\left(q \cdot \sqrt{\frac{t-s}{2^n}} + q \cdot \sqrt{\frac{t-k}{2^n}} + \frac{k}{\sqrt{s}} + \frac{sk}{t}\right).$$

Proof. Consider the following hybrid distributions.

$\mathbf{H}_1$**.** Output $\mathcal{D}^{\mathcal{O}_S}(|S\rangle^{\otimes k})$, where $S \subseteq \{0,1\}^n$ is a random subset of size $|S| = s$.

$\mathbf{H}_2$**.** Output $\mathcal{D}^{\mathcal{O}_S}(|S\rangle^{\otimes k})$, where the subset S is sampled as follows: first, sample a random subset $T \subseteq \{0,1\}^n$ of size $|T| = t$, and then let $S \subseteq T$ be a random subset of size $|S| = s$.

Let $p(\mathbf{H}_i)$ be the probability that $\mathbf{H}_i$ outputs 1, for some i. We now show the following.

▷ Claim 9. $p(\mathbf{H}_2) = p(\mathbf{H}_1)$.

Proof. The distribution of sampling $S \subseteq \{0,1\}^n$ of size $|S| = s$ is identical to the distribution of first sampling a superset $T \subseteq \{0,1\}^n$ of size $|T| = t$, and letting $S \subseteq T$ be a random subset of size $|S| = s$. ◁

$\mathbf{H}_3$. Output $\mathcal{D}^{\mathcal{O}_T}(|S\rangle^{\otimes k})$, where the subset S is sampled as follows: first, sample a random subset $T \subseteq \{0,1\}^n$ of size $|T| = t$, and then let $S \subseteq T$ be a random subset of size $|S| = s$.

▷ Claim 10.

$$|p(\mathbf{H}_3) - p(\mathbf{H}_2)| \leq O\left(q \cdot \sqrt{\frac{t-s}{2^n}}\right).$$

Proof. We can model the quantum oracle algorithm $\mathcal{D}^{\mathcal{O}_S}$ on input $|S\rangle^{\otimes t}$ as a sequence of oracle queries and unitary computations followed by a measurement. Thus, the final output state just before the measurement can be written as

$$\left|\Psi_q^S\right\rangle = U_q \mathcal{O}_S U_{q-1} \dots U_1 \mathcal{O}_S U_0 \left|\psi_0\right\rangle |S\rangle^{\otimes k} ,$$

where $U_0, U_1, \dots, U_q$ are unitaries (possibly acting on additional workspace registers, which we omit above), and where $|\psi_0\rangle$ is some fixed initial state which is independent of S.

In the next step of the proof, we will use the "subset flooding" technique to drown S in a random superset. Let $T \subseteq \{0,1\}^n$ be a random superset of S of size $t > s$. We now consider the state

$$\left|\Psi_q^T\right\rangle = U_q \mathcal{O}_T U_{q-1} \dots U_1 \mathcal{O}_T U_0 \left|\psi_0\right\rangle |S\rangle^{\otimes k} .$$

We now claim that the states $\left|\Psi_q^S\right\rangle$ and $\left|\Psi_q^T\right\rangle$ are sufficiently close. From the definition of $\mathcal{O}_T$ and $\mathcal{O}_S$, we have that $\mathcal{O}_T(x) \neq \mathcal{O}_S(x)$ iff $x \in T \backslash S \subset \{0,1\}^n$. By the O2H Lemma (Lemma 4),

$$\begin{aligned}
\underset{\substack{T \subseteq \{0,1\}^n, |T|=t \\ S \subseteq T, |S|=s}}{\mathbb{E}} \left\| \left|\Psi_q^S\right\rangle - \left|\Psi_q^T\right\rangle \right\| &\leq 2q \underset{\substack{T \subseteq \{0,1\}^n, |T|=t \\ S \subseteq T, |S|=s}}{\mathbb{E}} \sqrt{\frac{1}{q} \sum_{i=0}^{q-1} \left\| \Pi_{T \backslash S} \left|\Psi_i^S\right\rangle \right\|^2} \\
&\leq 2q \sqrt{\frac{1}{q} \sum_{i=0}^{q-1} \underset{\substack{T \subseteq \{0,1\}^n, |T|=t \\ S \subseteq T, |S|=s}}{\mathbb{E}} \left\| \Pi_{T \backslash S} \left|\Psi_i^S\right\rangle \right\|^2} \quad \text{(Jensen's inequality)} \\
&= O\left(q \cdot \sqrt{\frac{t-s}{2^n}}\right).
\end{aligned}$$

Therefore, the probability (over the choice of S and T) that $\mathcal{D}^{\mathcal{O}_S}(|S\rangle^{\otimes k})$ succeeds is at most the probability that $\mathcal{D}^{\mathcal{O}_T}(|S\rangle^{\otimes k})$ succeeds – up to an additive loss of $O(q \cdot \sqrt{\frac{t-s}{2^n}})$. ◁

$\mathbf{H}_4$. Output $\mathcal{D}^{\mathcal{O}_T}(|\boldsymbol{\sigma}_X\rangle)$, where the subset X is sampled as follows: first, sample a random subset $T \subseteq \{0,1\}^n$ of size $|T| = t$, and then let $X \subseteq T$ be a random subset of size $|X| = k$.

▷ Claim 11.

$$|p(\mathbf{H}_4) - p(\mathbf{H}_3)| \leq O\left(\frac{k}{\sqrt{s}} + \frac{sk}{t}\right).$$

Proof. Here, we make use of Lemma 6 which says that, for any superset $T \subseteq \{0,1\}^n$ of size $|T| = t$,

$$\mathsf{TD}\left(\underset{\substack{S \subseteq T \\ |S|=s}}{\mathbb{E}} \left[|S\rangle\langle S|^{\otimes k} \right], \underset{\substack{X \subseteq T \\ |X|=k}}{\mathbb{E}} \left[|\boldsymbol{\sigma}_X\rangle\langle\boldsymbol{\sigma}_X| \right] \right) \leq O\left(\frac{k}{\sqrt{s}} + \frac{sk}{t}\right).$$ ◁

$\mathbf{H}_5$. Output $\mathcal{D}^{\mathcal{O}_X}(|\boldsymbol{\sigma}_X\rangle)$, where the subset X is sampled as follows: first, sample a random subset $T \subseteq \{0,1\}^n$ of size $|T| = t$, and then let $X \subseteq T$ be a random subset of size $|X| = k$.

▷ Claim 12.

$$|p(\mathbf{H}_5) - p(\mathbf{H}_4)| \leq O\left(q \cdot \sqrt{\frac{t-k}{2^n}}\right).$$

Proof. Suppose that $X \subseteq T$ is a random subset of size $|X| = k$, and let $|\boldsymbol{\sigma}_X\rangle = \frac{1}{k!}\sum_{\sigma \in S_k} |x_{\sigma(1)}, \ldots, x_{\sigma(k)}\rangle$, where S_k denotes the symmetric group on $[k]$. Consider the state

$$|\Phi_q^T\rangle = U_q \mathcal{O}_T U_{q-1} \ldots U_1 \mathcal{O}_T U_0 |\psi_0\rangle |\boldsymbol{\sigma}_X\rangle.$$

prepared by $\mathcal{D}^{\mathcal{O}_T}(|\boldsymbol{\sigma}_X\rangle)$ just before the measurement. Similarly, we let

$$|\Phi_q^X\rangle = U_q \mathcal{O}_X U_{q-1} \ldots U_1 \mathcal{O}_X U_0 |\psi_0\rangle |\boldsymbol{\sigma}_X\rangle.$$

be the state prepared by $\mathcal{A}^{\mathcal{O}_X}(|\boldsymbol{\sigma}_X\rangle)$. Using Lemma 4 as before, we get that

$$\begin{aligned}
\mathop{\mathbb{E}}_{\substack{T \subseteq \{0,1\}^n, |T|=t \\ X \subseteq T, |X|=k}} \left\| |\Phi_q^T\rangle - |\Phi_q^X\rangle \right\| &\leq 2q \mathop{\mathbb{E}}_{\substack{T \subseteq \{0,1\}^n, |T|=t \\ X \subseteq T, |X|=k}} \sqrt{\frac{1}{q}\sum_{i=0}^{q-1} \left\| \Pi_{T \setminus X} |\Phi_i^X\rangle \right\|^2} \\
&\leq 2q \sqrt{\frac{1}{q}\sum_{i=0}^{q-1} \mathop{\mathbb{E}}_{\substack{T \subseteq \{0,1\}^n, |T|=t \\ X \subseteq T, |X|=k}} \left\| \Pi_{T \setminus X} |\Phi_i^X\rangle \right\|^2} \qquad \text{(Jensen's inequality)} \\
&\leq O\left(q \cdot \sqrt{\frac{t-k}{2^n}}\right).
\end{aligned}$$

Therefore, the probability (over the choice of X and T) that $\mathcal{D}^{\mathcal{O}_T}(|\boldsymbol{\sigma}_X\rangle)$ succeeds is at most the probability that $\mathcal{D}^{\mathcal{O}_X}(|\boldsymbol{\sigma}_X\rangle)$ succeeds (up to an additive error of $\frac{q}{\sqrt{t-k}}$). ◁

Therefore, by applying the triangle inequality, we get that

$$|p(\mathbf{H}_1) - p(\mathbf{H}_5)| \leq O\left(q \cdot \sqrt{\frac{t-s}{2^n}} + q \cdot \sqrt{\frac{t-k}{2^n}} + \frac{k}{\sqrt{s}} + \frac{sk}{t}\right).$$

This proves the claim. ◀

5 Multi-Copy Revocable Encryption: Definition

In this section we formally define and construct multi-copy secure revocable encryption schemes. These are regular encryption scheme but where the ciphertexts are associated with quantum states. Moreover, the security property guarantees that any adversary that successfully returns k valid copies of a quantum ciphertext (which it received from a trusted party), where k is an arbitrary polynomial, necessarily loses the ability to decrypt the ciphertexts in the future – even if the secret key is revealed.

Our definition of revocable encryption is as follows:

▶ **Definition 13** (Revocable Encryption). *Let $\lambda \in \mathbb{N}$ denote the security parameter. A revocable encryption scheme $\Sigma = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Revoke})$ with plaintext space $\mathcal{M}$ consists of the following QPT algorithms:*

- $\mathsf{KeyGen}(1^\lambda)$*: on input the security parameter 1^λ, output a secret key* sk*.*
- $\mathsf{Enc}(\mathsf{sk}, m)$*: on input the secret key* sk *and a message $m \in \mathcal{M}$, output a (pure) ciphertext state $|\psi\rangle$ and a (private) verification key* vk*.*
- $\mathsf{Dec}(\mathsf{sk}, \rho)$*: on input the secret key* sk *and a quantum state ρ, output a message m'.*
- $\mathsf{Revoke}(\mathsf{sk}, \mathsf{vk}, \sigma)$*: on input the secret key* sk*, a verification key* vk *and a state σ, output $\top$ or $\bot$.*

In addition, we require that Σ satisfies the following two properties:

Correctness of decryption: *for all plaintexts $m \in \mathcal{M}$, it holds that*

$$\mathsf{Pr}\left[m \leftarrow \mathsf{Dec}(\mathsf{sk}, |\psi\rangle) \;:\; \substack{\mathsf{sk} \leftarrow \mathsf{KeyGen}(1^\lambda) \\ (|\psi\rangle, \mathsf{vk}) \leftarrow \mathsf{Enc}(\mathsf{sk}, m)}\right] \geq 1 - \mathsf{negl}(\lambda).$$

Correctness of revocation: *for all plaintexts $m \in \mathcal{M}$, it holds that*

$$\mathsf{Pr}\left[\top \leftarrow \mathsf{Revoke}(\mathsf{sk}, \mathsf{vk}, |\psi\rangle) \;:\; \substack{\mathsf{sk} \leftarrow \mathsf{KeyGen}(1^\lambda) \\ (|\psi\rangle, \mathsf{vk}) \leftarrow \mathsf{Enc}(\mathsf{sk}, m)}\right] \geq 1 - \mathsf{negl}(\lambda).$$

There are two properties we require the above scheme to satisfy.
Firstly, we require the above scheme to be correct. That is, we require the following to hold for all $m \in \{0,1\}^\ell$,

$$\mathsf{Pr}\left[m \leftarrow \mathsf{Dec}(\mathsf{sk}, |\psi\rangle) \;:\; \substack{\mathsf{sk} \leftarrow \mathsf{KeyGen}(1^\lambda) \\ |\psi\rangle \leftarrow \mathsf{Enc}(\mathsf{sk}, m)}\right] \geq 1 - \epsilon(\lambda),$$

for some negligible function $\epsilon(\cdot)$.

Multi-Copy Revocable Security

We use the following notion of security.

▶ **Definition 14** (Multi-Copy Revocable Security). *Let $\lambda \in \mathbb{N}$ denote the security parameter and let $\Sigma = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Revoke})$ be a revocable encryption scheme with plaintext space $\mathcal{M}$. Consider the following experiment between a QPT adversary $\mathcal{A}$ and a challenger.*

$\mathsf{RevokeExpt}_{\lambda,\Sigma,\mathcal{A}}(b)$*:*

1. *$\mathcal{A}$ submits two messages $m_0, m_1 \in \mathcal{M}$ and a polynomial $k = k(\lambda)$ to the challenger.*
2. *The challenger samples a key $\mathsf{sk} \leftarrow \mathsf{KeyGen}(1^\lambda)$ and produces $|\psi_b\rangle \leftarrow \mathsf{Enc}(\mathsf{sk}, m_b)$. Afterwards, the challenger sends the quantum state $|\psi_b\rangle^{\otimes k}$ to $\mathcal{A}$.*
3. *$\mathcal{A}$ returns a quantum state ρ.*
4. *The challenger performs the measurement $\left\{|\psi_b\rangle\langle\psi_b|^{\otimes k}, \; \mathbb{I} - |\psi_b\rangle\langle\psi_b|^{\otimes k}\right\}$ on the returned state ρ. If the measurement succeeds, the game continues; otherwise, the challenger aborts.*
5. *The challenger sends the secret key sk to $\mathcal{A}$.*
6. *$\mathcal{A}$ outputs a bit b'.*

We say that the revocable encryption scheme $\Sigma = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Revoke})$ has multi-copy revocable security, if the following holds for all $\mu \in \{0,1,\bot\}$:

$$\left|\mathsf{Pr}\left[\mu \leftarrow \mathsf{RevokeExpt}_{\lambda,\Sigma,\mathcal{A}}(0)\right] - \mathsf{Pr}\left[\mu \leftarrow \mathsf{RevokeExpt}_{\lambda,\Sigma,\mathcal{A}}(1)\right]\right| \leq \mathsf{negl}(\lambda)\,,$$

▶ Remark 15. In this work, we will work with a weaker variant of this security game, one where the post revocation adversary is given access to an oracle that depends on the key sk instead. The reason for this will become clear from context.

▶ Remark 16 (Search variant). Occasionally, we also consider the search variant of multi-copy revocable encryption. Here, the experiment is similar, except that in Step 1, the adversary only submits k to the challenger. Then, in Step 2, the challenger chooses a message m uniformly at random from the plaintext space, encrypts it k times and sends all of the copies to the adversary. Finally, the adversary is said to win the game if it guesses m correctly.

6 Construction of Multi-Copy Secure Revocable Encryption

In this section, we instantiate our revocable encryption scheme using quantum-secure pseudorandom permutations (QPRPs), and we prove security in an oracular model: this means that, rather than revealing the QPRP key in the final part of the revocable security experiment, we instead allow the adversary to query an oracle for a the permutation instead.

▶ **Construction 17.** *Let $\lambda \in \mathbb{N}$ be the security parameter. Let $n, m \in \mathbb{N}$ be polymomial in λ. Let $\Phi = \{\Phi_\lambda\}_{\lambda\in\mathbb{N}}$ be an ensemble of permutations $\Phi_\lambda = \{\varphi_\kappa : \{0,1\}^{n+m} \to \{0,1\}^{n+m}\}_{\kappa\in\mathcal{K}_\lambda}$, for some set $\mathcal{K}_\lambda$. Consider the scheme $\Sigma^\Phi = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Revoke})$ which consists of the following QPT algorithms:*

- $\mathsf{KeyGen}(1^\lambda)$*: sample a uniformly random key $\kappa \in \mathcal{K}_\lambda$ and let $\mathsf{sk} = \kappa$.*
- $\mathsf{Enc}(\mathsf{sk}, \mu)$*: on input the secret key $\mathsf{sk} = \kappa$ and message $\mu \in \{0,1\}^m$, sample $y \sim \{0,1\}^m$ and prepare the subset state given by*

  $$|S_y\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\varphi_\kappa(x||y)\rangle .$$

  Output the ciphertext state $(|S_y\rangle^{\otimes k}, y \oplus \mu)$ and (private) verification key $\mathsf{vk} = y$.
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$*: on input the decryption key κ and ciphertext state $(|S_y\rangle, z) \leftarrow \mathsf{ct}$, do the following:*
  - *Coherently compute φ_κ^{-1} on $|S_y\rangle$ and store the answer in a separate output register.*
  - *Measure the output register to get $x'||y' \in \{0,1\}^{n+m}$.*
  - *Output $y' \oplus z$.*
- $\mathsf{Revoke}(\mathsf{sk}, \mathsf{vk}, \rho)$*: on input sk, a state ρ and verification key vk, it parses $\kappa \leftarrow \mathsf{sk}$, $y \leftarrow \mathsf{vk}$ and applies the measurement $\{|S_y\rangle\langle S_y|, \mathbb{I} - |S_y\rangle\langle S_y|\}$ to ρ; it outputs $\top$ if it succeeds, and $\bot$ otherwise.*

Proof of Multi-Copy Revocable Security

▶ **Theorem 18.** *Construction 17, when instantiated with a QPRP $\Phi = \{\Phi_\lambda\}_{\lambda\in\mathbb{N}}$, satisfies (an oracular notion of) multi-copy revocable security.*

Proof. Because we are working in the oracular model of revocable security, we can invoke QPRP security and assume that Σ in Construction 17 is instantiated with a perfectly random permutation φ rather than a QPRP permutation φ_κ.

Suppose that our construction does not achieve multi-copy revocable security. Then, there exists an adversary $\mathcal{A}$ such that

$$\left|\Pr\left[\mu \leftarrow \mathsf{RevokeExpt}_{\lambda,\Sigma,\mathcal{A}}(0)\right] - \Pr\left[\mu \leftarrow \mathsf{RevokeExpt}_{\lambda,\Sigma,\mathcal{A}}(1)\right]\right| = \epsilon(\lambda),$$

for some non-negligible function $\epsilon(\cdot)$. For convenience, we model $\mathcal{A}$ as a pair of quantum algorithms $(\mathcal{A}_0, \mathcal{A}_1)$, where $\mathcal{A}_0$ corresponds to the pre-revocation adversary, and $\mathcal{A}_1$ corresponds to the post-revocation adversary. We consider the following sequence of hybrid distributions.

$\mathbf{H}_1^b$. This corresponds to $\mathsf{RevokeExpt}^{\mathcal{A}}(1^\lambda, b)$.

1. $\mathcal{A}_0$ submits two m-bit messages (μ_0, μ_1) and a polynomial $k = k(\lambda)$ to the challenger.
2. The challenger samples $y \sim \{0,1\}^m$ and produces a quantum state

$$|S_y\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |\varphi(x||y)\rangle .$$

   The challenger then sends $|S_y\rangle^{\otimes k}$ and $y \oplus \mu_b$ to $\mathcal{A}_0$.
3. $\mathcal{A}_0$ prepares a bipartite state on registers R and AUX, and sends R to the challenger and AUX to $\mathcal{A}_1$.
4. The challenger performs the projective measurement $\left\{|S_y\rangle\langle S_y|^{\otimes k}, \, \mathbb{I} - |S_y\rangle\langle S_y|^{\otimes k}\right\}$ on R. If the measurement succeeds, the challenger outputs $\perp$. Otherwise, the challenger continues.
5. The challenger grants $\mathcal{A}_1$ quantum oracle access to φ^{-1}.
6. $\mathcal{A}_1$ outputs a bit b'.

$\mathbf{H}_2^b$. This is the same experiment as in $\mathbf{H}_1^b$, except that we change how $|S_y\rangle^{\otimes k}$ is generated before revocation:

- The challenger samples a random subset $S \subseteq \{0,1\}^{n+m}$ of size $|S| = 2^n$.
- The challenger samples a random $y \sim \{0,1\}^m$.
- The challenger sends $|S\rangle^{\otimes k}$ and $y \oplus \mu_b$ to $\mathcal{A}_0$.

Later, the challenger samples a random permutation $\pi : \{0,1\}^{n+m} \to \{0,1\}^{n+m}$ subject to the constraint that $\pi(s) = *||y$, for all $s \in S$. In other words, $\pi(S) = T_y$, where

$$T_y := \left\{x \in \{0,1\}^{n+m} \, : \, x = (*||y)\right\}$$

and $|S| = |T_y| = 2^n$. After revocation, $\mathcal{A}_1$ receives oracle access to π.

▷ Claim 19. $\mathbf{H}_1^b$ and $\mathbf{H}_2^b$ are identically distributed.

Proof. This follows immediately. We just changed the order in which we sample things. ◁

$\mathbf{H}_3^b$. This is the same experiment as in $\mathbf{H}_2^b$, except that we change the second part of the experiment: after the challenger sends $|S\rangle^{\otimes k}$ and $y \oplus \mu_b$ to $\mathcal{A}_0$, he does the following:

- The challenger samples a random function $g : S \to T_y$. [5]
- The challenger samples a random permutation $\omega : (\{0,1\}^{n+m} \setminus S) \to (\{0,1\}^{n+m} \setminus T_y)$.

After revocation, $\mathcal{A}_1$ receives oracle access to $f : \{0,1\}^{n+m} \to \{0,1\}^{n+m}$, where

$$f(x) = \begin{cases} g(x), & \text{if } x \in S \\ \omega(x), & \text{if } x \notin S. \end{cases}$$

[5] Note that we have $g(S) \subseteq T_y$ in general.

▷ Claim 20. $\mathbf{H}_2^b$ and $\mathbf{H}_3^b$ are $O(q^3/2^n)$-close whenever $\mathcal{A}$ makes q queries.

Proof. Here, we apply Zhandry's result which says that random functions are indistinguishable from random permutations. Consider the following algorithm $\mathcal{B}$ which receives oracle access to O, which is either a random function $F : \{0,1\}^n \to \{0,1\}^n$ or a random permutation $P : \{0,1\}^n \to \{0,1\}^n$:

1. $\mathcal{B}$ samples a random subset $S \subseteq \{0,1\}^{n+m}$ of size $|S| = 2^n$ and a random $y \sim \{0,1\}^m$.
2. $\mathcal{B}$ sends $|S_y\rangle^{\otimes k}$ and $y \oplus \mu_b$ to $\mathcal{A}_0$.
3. When $\mathcal{A}_0$ replies with a bipartite state on registers R and AUX, $\mathcal{B}$ performs the projective measurement $\left\{|S\rangle\!\langle S|^{\otimes k}, \ \mathbb{I} - |S\rangle\!\langle S|^{\otimes k}\right\}$ on R. If it succeeds, $\mathcal{B}$ outputs $\perp$. Otherwise, $\mathcal{B}$ continues.
4. $\mathcal{B}$ runs the post-revocation adversary $\mathcal{A}_1$ on input AUX. Whenever $\mathcal{A}_1$ makes a query, $\mathcal{B}$ answers using the function

$$f(x) = \begin{cases} (\tau \circ O \circ \sigma)(x), & \text{if } x \in S \\ \omega(x), & \text{if } x \notin S \end{cases}$$

   where we let
   - σ be some canonical mapping from S (with $|S| = 2^n$) onto $\{0,1\}^n$, i.e., σ is a a function which assigns each element of $S \subseteq \{0,1\}^{n+m}$ a unique bit string in $\{0,1\}^n$.
   - τ be the function which maps each $x \in \{0,1\}^n$ to $(x||y) \in \{0,1\}^{n+m}$.

Note that whenever O is a random permutation, the view of $\mathcal{A}$ is precisely $\mathbf{H}_3^b$; whereas, if O is a random function, the view of $\mathcal{A}$ is precisely $\mathbf{H}_4^b$. Therefore, the claim follows from Zhandry's result on indistinguishability of random pemrutations from random functions (see full version for formal statement). ◁

$\mathbf{H}_4^b$. This is the same experiment as in $\mathbf{H}_3^b$, except that we change the second part of the experiment once again: after the challenger sends $|S_y\rangle^{\otimes k}$ and $y \oplus \mu_b$ to $\mathcal{A}_0$, he does the following:

- the challenger samples a random function $f : \{0,1\}^{n+m} \to \{0,1\}^{n+m}$ subject to the constraint that $f(s) = *||y$, for all $s \in S$.

After revocation, $\mathcal{A}_1$ receives oracle access to f.

▷ Claim 21. $\mathbf{H}_3^b$ and $\mathbf{H}_4^b$ are $O\big(q^3/(2^{n+m} - 2^n)\big)$-close whenever $\mathcal{A}$ makes q queries.

Proof. The proof again follows since distinguishing $\mathbf{H}_3^b$ and $\mathbf{H}_4^b$ amounts to distinguishing a random function from a random permutation mapping a random permutation $\omega : (\{0,1\}^{n+m} \setminus S) \to (\{0,1\}^{n+m} \setminus T_y)$. Since the domain and co-domain are of equal size $2^{n+m} - 2^n$, the advantage is at most $O\big(q^3/(2^{n+m} - 2^n)\big)$. ◁

$\mathbf{H}_5^b$. This is the same experiment as in $\mathbf{H}_4^b$, but now we change what $\mathcal{A}_0$ receives in the pre-revocation phase:

- The challenger samples a random subset $S \subseteq \{0,1\}^{n+m}$ of size $|S| = 2^n$.
- The challenger samples a random $y \sim \{0,1\}^m$.
- The challenger sends $(|S_y\rangle^{\otimes k}, y)$ to $\mathcal{A}_0$.

After revocation, the challenger samples a random function $f : \{0,1\}^{n+m} \to \{0,1\}^{n+m}$ subject to the constraint that $f(s) = *||y \oplus \mu_b$, for all $s \in S$. $\mathcal{A}$ receives oracle access to f.

▷ Claim 22. $\mathbf{H}_4^b$ and $\mathbf{H}_5^b$ are indentical.

Proof. This follows from the fact that we have just re-labeled the variables. ◁

$\mathbf{H}_6^b$. This is the same experiment as in $\mathbf{H}_5^b$, except that we once again change what $\mathcal{A}_0$ receives in the pre-revocation phase:

- The challenger samples a random subset $S \subseteq \{0,1\}^{n+m}$ of size $|S| = 2^n$.
- The challenger samples a random $y \sim \{0,1\}^m$.
- The challenger samples a random $u \sim \{0,1\}^m$.
- The challenger sends $(|S_y\rangle^{\otimes k}, y)$ to $\mathcal{A}_0$.

After revocation, the challenger samples a random function $f : \{0,1\}^{n+m} \to \{0,1\}^{n+m}$ subject to the constraint that $f(s) = *||u$, for all $s \in S$. $\mathcal{A}$ receives oracle access to f.

Note that hybrids $\mathbf{H}_6^0$ and $\mathbf{H}_6^1$ are identically distributed. By assumption, we also know that $\mathcal{A}$ distinguishes $\mathbf{H}_1^0$ and $\mathbf{H}_1^1$ with non-negligible advantage. Therefore, our previous hybrid argument has shown that $\mathcal{A}$ must also distinguish $\mathbf{H}_5^0$ and $\mathbf{H}_6^0$ (respectively, hybrids $\mathbf{H}_5^1$ and $\mathbf{H}_6^1$) with advantage at least $\epsilon'(\lambda)$, for some non negligible function $\epsilon'(\lambda)$. To complete the proof, we show the following claim which yields the desired contradiction to the $k \mapsto k+1$ unforgeability property of subset states from Theorem 7.

▷ Claim 23. Forge in Algorithm 1 is a poly(λ)-query algorithm (which internally runs $\mathcal{A}$) such that

$$\Pr_{\substack{S \subseteq \{0,1\}^{n+m}\\ |S|=2^n}}\left[(x_1,\dots,x_{k+1}) \in \mathrm{dist}(S,k+1) \;:\; (x_1,\dots,x_{k+1}) \leftarrow \mathsf{Forge}^{\mathcal{O}_S}(|S\rangle^{\otimes k})\right] \geq 1/\mathrm{poly}(\lambda).$$

Proof. Since $\mathbf{H}_5^b$ and $\mathbf{H}_6^b$ can be distinguished by the adversary $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ with advantage $\epsilon'(\lambda)$, for some non-negligible function $\epsilon'(\lambda)$, this implies that the post-revocation adversary $\mathcal{A}_1$ is an algorithm for which the following property holds: given as input uniformly random string y and an auxiliary register (conditioned on revocation succeeding), $\mathcal{A}_1$ can distinguish whether it is given an oracle for a function $H : \{0,1\}^{n+m} \to \{0,1\}^{n+m}$ which is random subject to the constraint that $H(s) = *||y \oplus \mu_b$ for all $s \in S$, or whether it is given an oracle for a function $G : \{0,1\}^{n+m} \to \{0,1\}^{n+m}$ which is a random function subject to the constraint that $G(s) = *||u$ for all $s \in S$. Crucially, the two functions differ precisely on inputs belonging to S, and are otherwise identical.

Consider the quantum extractor $\mathsf{Ext}^G(y, \mathsf{AUX})$ which is defined as follows:

1. Sample $i \leftarrow [q]$, where q denotes the total number of queries made by $\mathcal{A}$.
2. Run $\mathcal{A}_1^G(y, \mathsf{AUX})$ just before the $(i-1)$-st query to G.
3. Measure $\mathcal{A}_1$'s i-th query in the computational basis, and output the measurement outcome.

From the O2H Lemma (see full version for the formal statement), we get that

$$\left|\Pr\left[\mathcal{A}_1^H(y,\mathsf{AUX}_{|\top}) = 1 \;:\; \substack{S\subset\{0,1\}^{n+m},|S|=2^n\\ y\sim\{0,1\}^m\\ (\mathsf{R},\mathsf{AUX})\leftarrow\mathcal{A}_0(|S\rangle^{\otimes k},y)\\ H \text{ s.t. } H(s)=*||y\oplus\mu_b,\forall s\in S}\right] - \Pr\left[\mathcal{A}_1^G(y,\mathsf{AUX}_{|\top}) = 1 \;:\; \substack{S\subset\{0,1\}^{n+m},|S|=2^n\\ y\sim\{0,1\}^m,u\sim\{0,1\}^m\\ (\mathsf{R},\mathsf{AUX})\leftarrow\mathcal{A}_0(|S\rangle^{\otimes k},y)\\ G \text{ s.t. } G(s)=*||u,\forall s\in S}\right]\right|$$
$$\leq 2q\sqrt{\Pr\left[\mathsf{Ext}^G(y,\mathsf{AUX}_{|\top}) \in S \;:\; \substack{S\subset\{0,1\}^{n+m},|S|=2^n\\ y\sim\{0,1\}^m,u\sim\{0,1\}^m\\ (\mathsf{R},\mathsf{AUX})\leftarrow\mathcal{A}_0(|S\rangle^{\otimes k},y)\\ G \text{ s.t. } G(s)=*||u,\forall s\in S}\right]},$$

where $\mathsf{AUX}_{|\top}$ corresponds to the register AUX conditioned on the event that the projective measurement

$$\left\{|S\rangle\!\langle S|^{\otimes k},\; \mathbb{I} - |S\rangle\!\langle S|^{\otimes k}\right\}$$

succeeds on register R. Because the distinguishing advantage of the adversary $\mathcal{A}_1$ is non-negligible (conditioned on the event that revocation succeeds on register R) and $q = \mathrm{poly}(\lambda)$, we get

$$\Pr\left[\mathsf{Ext}^G(y, \mathsf{AUX}_{|\top}) \in S \ : \ \substack{S\subset\{0,1\}^{n+m},|S|=2^n \\ y\sim\{0,1\}^m, u\sim\{0,1\}^m \\ (\mathsf{R},\mathsf{AUX})\leftarrow\mathcal{A}_0(|S\rangle^{\otimes k},y) \\ G \text{ s.t. } G(s)=*||u,\forall s\in S}\right] \geq 1/\mathrm{poly}(\lambda).$$

To complete the proof, we now show that $\mathsf{Forge}^{\mathcal{O}_S}(|S\rangle^{\otimes k})$ in Algorithm 1 is a successful algorithm against the $k \to k+1$ unforgeability of subset states.

Algorithm 1 $\mathsf{Forge}^{\mathcal{O}_S}(|S\rangle^{\otimes k})$.

```
Input: $|S\rangle^{\otimes k}$ and a membership oracle $\mathcal{O}_S$, where $S \subset \{0,1\}^{n+m}$ is a subset.
Output: $x_1, \dots x_{k+1} \in \{0,1\}^{n+m}$.
Sample uniformly random strings $y, u \sim \{0,1\}^m$;
Run $(\mathsf{R}, \mathsf{AUX}) \leftarrow \mathcal{A}_0(|S\rangle^{\otimes k}, y)$;
Measure $\mathsf{R}$ in the computational basis to obtain $x_1, \dots, x_k$;
Run the quantum extractor $\mathsf{Ext}^G(y, \mathsf{AUX})$ to obtain an element $x_{k+1}$, where the
  oracle $G$ can be simulated via $\mathcal{O}_S$ as follows: on input $x \in \{0,1\}^{n+m}$, we let
      $G(x) = \begin{cases} g_1(x)||u, & \text{if } \mathcal{O}_S(x) = 1 \\ g_2(x), & \text{otherwise} \end{cases}$
  where $g_1 : \{0,1\}^{n+m} \to \{0,1\}^n$ and $g_2 : \{0,1\}^{n+m} \to \{0,1\}^{n+m}$ are uniformly
  random functions.
Output $(x_1, \dots, x_{k+1})$.
```

Let $\mathsf{Revoke}(S, k, \mathsf{R})$ denote the projective measurement $\{|S\rangle\langle S|^{\otimes k}, \ \mathbb{I} - |S\rangle\langle S|^{\otimes k}\}$ of register R. Using the Simultaneous Distinct Extraction Lemma (Lemma 24), we get that

$$\begin{aligned} &\Pr_{\substack{S\subseteq\{0,1\}^{n+m} \\ |S|=2^n}}\left[(x_1, \dots, x_{t+1}) \in \mathrm{dist}(S, k+1) \ : \ (x_1, \dots, x_{k+1}) \leftarrow \mathsf{Forge}^{\mathcal{O}_S}(|S\rangle^{\otimes k})\right] \\ &\geq \left(1 - O\left(\frac{k^2}{2^n}\right)\right) \cdot \Pr\left[\mathsf{Revoke}(S, k, \mathsf{R}) = \top \ : \ \substack{S\subset\{0,1\}^{n+m},|S|=2^n \\ y\sim\{0,1\}^m \\ (\mathsf{R},\mathsf{AUX})\leftarrow\mathcal{A}_0(|S\rangle^{\otimes k},y)}\right] \\ &\qquad \cdot \Pr\left[\mathsf{Ext}^G(y, \mathsf{AUX}_{|\top}) \in S \ : \ \substack{S\subset\{0,1\}^{n+m},|S|=2^n \\ y\sim\{0,1\}^m, u\sim\{0,1\}^m \\ (\mathsf{R},\mathsf{AUX})\leftarrow\mathcal{A}_0(|S\rangle^{\otimes k},y) \\ G \text{ s.t. } G(s)=*||u,\forall s\in S}\right] \end{aligned}$$

which is at least inverse polynomial in λ. This proves the claim. ◁

Thus, we obtain the desired contradiction to the $k \mapsto k+1$ unforgeability property of subset states from Theorem 7. This completes the proof of multi-copy revocable encryption security. ◀

6.1 Simultaneous Distinct Extraction Lemma

The following lemma allows us to analyze the probability of simultaneously extracting $k+1$ distinct subset elements in some subset $S \subseteq \{0,1\}^n$ in terms of the success probability of revocation (i.e., the projection onto $|S\rangle\langle S|^{\otimes k}$) and the success probability of extracting another subset element from the adversary's state.

▶ **Lemma 24** (Simultaneous Distinct Extraction). *Let $n, k \in \mathbb{N}$ and let $\rho \in \mathcal{D}(\mathcal{H}_X \otimes \mathcal{H}_Y)$ be an any density matrix, where $\mathcal{H}_X$ is an $n \cdot k$-qubit Hilbert space and where $\mathcal{H}_Y$ is an arbitrary Hilbert space. Let $|S\rangle$ denote a subset state, for some subset $S \subseteq \{0,1\}^n$, and let $\mathcal{E} : \mathcal{L}(\mathcal{H}_Y) \to \mathcal{L}(\mathcal{H}_{X'})$ be any* CPTP *map of the form*

$$\mathcal{E}_{Y \to X'}(\sigma) = \mathrm{Tr}_E\left[V_{Y \to X'E}\, \sigma V^{\dagger}_{Y \to X'E}\right], \quad \forall \sigma \in \mathcal{D}(\mathcal{H}_Y),$$

for some isometry $V_{Y \to X'E}$ and n-qubit Hilbert space $\mathcal{H}_{X'}$. Consider the POVM *element*

$$\Lambda = \sum_{\substack{s_1,\dots,s_{k+1} \in S \\ (s_1,\dots,s_{k+1}) \in \mathrm{dist}(S,k+1)}} |s_1,\dots,s_k\rangle\langle s_1,\dots,s_k|_X \otimes V^{\dagger}_{Y \to X'E}(|s_{k+1}\rangle\langle s_{k+1}|_{X'} \otimes I_E) V_{Y \to X'E}.$$

Let $\rho_X = \mathrm{Tr}_Y[\rho_{XY}]$ denote the reduced state. Then, it holds that

$$\mathrm{Tr}[\Lambda \rho] \geq \left(1 - O\left(\frac{k^2}{|S|}\right)\right) \cdot \mathrm{Tr}\left[|S\rangle\langle S|^{\otimes k} \rho_X\right] \cdot \mathrm{Tr}\left[\, |S\rangle\langle S|\; \mathcal{E}_{Y \to X'}(\sigma)\right],$$

where $\sigma = \mathrm{Tr}\left[(|S\rangle\langle S|^{\otimes k} \otimes I)\rho\right]^{-1} \cdot \mathrm{Tr}_X[(|S\rangle\langle S|^{\otimes k} \otimes I)\rho]$ is a reduced state in system Y.

7 Multi-Copy Revocable Programs: Definition

In this section, we study whether arbitrary functionalities can be revoked. We define and study revocable programs with multi-copy security. In this notion, there is a functionality preserving compiler that takes a program and converts it into a quantum state, which can later be certifiably revoked.

We now give a formal definition of revocable programs.

▶ **Definition 25** (Revocable Program). *Let $\mathcal{P} = \bigcup_{\lambda \in \mathbb{N}} \mathcal{P}_\lambda$ be a class of efficiently computable program families $\mathcal{P}_\lambda = \{P : \mathcal{X}_\lambda \to \mathcal{Y}_\lambda\}$ with domain $\mathcal{X}_\lambda$ and range $\mathcal{Y}_\lambda$. A revocable program compiler for the class $\mathcal{P}$ is a tuple $\Sigma =$ (Compile, Eval, Revoke) consisting of the following QPT algorithms:*

- $\mathsf{Compile}(1^\lambda, P)$*: on input the security parameter 1^λ and a program $P \in \mathcal{P}_\lambda$ with $P : \mathcal{X}_\lambda \to \mathcal{Y}_\lambda$, output a quantum state $|\Psi_P\rangle$ and a (private) verification key* vk.
- $\mathsf{Eval}(|\Psi_P\rangle, x)$*: on input a quantum state $|\Psi_P\rangle$ and input $x \in \mathcal{X}_\lambda$, output $P(x)$.*
- $\mathsf{Revoke}(\mathsf{vk}, \sigma)$*: on input the verification key* vk *and a state σ, output $\top$ or $\bot$.*

In addition, we require that Σ satisfies the following two properties for all $\lambda \in \mathbb{N}$:

Correctness of evaluation: *for all programs $P \in \mathcal{P}_\lambda$ and inputs $x \in \mathcal{X}_\lambda$, it holds that*

$$\Pr\left[P(x) \leftarrow \mathsf{Eval}(|\Psi_P\rangle, x) \;:\; (|\Psi_P\rangle, \mathsf{vk}) \leftarrow \mathsf{Compile}(1^\lambda, P)\right] \geq 1 - \mathsf{negl}(\lambda).$$

Correctness of revocation: *for all programs $P \in \mathcal{P}_\lambda$, it holds that*

$$\Pr\left[\top \leftarrow \mathsf{Revoke}(\mathsf{vk}, (|\Psi_P\rangle) \;:\; (|\Psi_P\rangle, \mathsf{vk}) \leftarrow \mathsf{Compile}(1^\lambda, P)\right] \geq 1 - \mathsf{negl}(\lambda).$$

Multi-Copy Revocable Security

We use the following notion of security.

▶ **Definition 26** (Multi-Copy Revocable Security for Programs)**.** *Let $\mathscr{P} = \bigcup_{\lambda\in\mathbb{N}} \mathcal{P}_\lambda$ be a class of efficiently computable program families $\mathcal{P}_\lambda = \{P : \mathcal{X}_\lambda \to \mathcal{Y}_\lambda\}$ and let $\mathscr{D}_{\mathscr{P}} = \bigcup_{\lambda\in\mathbb{N}} \mathscr{D}_{\mathcal{P}_\lambda}$ be an ensemble of program distributions. Let $\mathscr{D}_{\mathcal{X}} = \bigcup_{\lambda\in\mathbb{N}} \mathscr{D}_{\mathcal{X}_\lambda}$ be an ensemble of challenge distribution families with $\mathcal{D}_{\mathcal{X}_\lambda} = \{\mathcal{D}_{\mathcal{X}_\lambda}(P)\}_{P\in\mathcal{P}_\lambda}$. Consider the following experiment between a QPT adversary $\mathcal{A}$ and a challenger.*

$\underline{\mathsf{RevokeExpt}^{\mathscr{D}_{\mathscr{P}},\mathscr{D}_{\mathcal{X}}}_{\lambda,\Sigma,\mathcal{A}}:}$

1. *$\mathcal{A}$ submits a polynomial $k = k(\lambda)$ to the challenger.*
2. *The challenger samples a program $P \sim \mathcal{D}_{\mathcal{P}_\lambda}$ with domain $\mathcal{X}_\lambda$ and range $\mathcal{Y}_\lambda$, and runs $\mathsf{Compile}(1^\lambda, P)$ to generate a pair $(|\Psi_P\rangle, \mathsf{vk})$. Afterwards, the challenger sends the quantum state $|\Psi_P\rangle^{\otimes}$ to $\mathcal{A}$.*
3. *$\mathcal{A}$ returns a quantum state ρ.*
4. *The challenger performs the measurement $\left\{|\Psi_P\rangle\langle\Psi_P|^{\otimes k}, \mathbb{I} - |\Psi_P\rangle\langle\Psi_P|^{\otimes k}\right\}$ on the returned state ρ. If the measurement succeeds, the game continues; otherwise, the challenger aborts.*
5. *The challenger samples a challenge input $x \sim \mathcal{D}_{\mathcal{X}_\lambda}(P)$ sends x to $\mathcal{A}$.*
6. *The adversary outputs $y \in \mathcal{Y}_\lambda$.*
7. *The challenger outputs 1 if and only if $P(x) = y$.*

We say that a revocable program compiler $\Sigma = (\mathsf{Compile}, \mathsf{Eval}, \mathsf{Revoke})$ has multi-copy revocable security for the ensembles $\mathscr{D}_{\mathscr{P}}$ and $\mathscr{D}_{\mathcal{X}}$, if the following holds for any QPT adversary $\mathcal{A}$:

$$\mathsf{Pr}\left[1 \leftarrow \mathsf{RevokeExpt}^{\mathscr{D}_{\mathscr{P}},\mathscr{D}_{\mathcal{X}}}_{\lambda,\Sigma,\mathcal{A}}\right] \leq p^{\mathscr{D}_{\mathscr{P}},\mathscr{D}_{\mathcal{X}}}_{\mathrm{triv}}(\lambda) + \mathsf{negl}(\lambda)\,,$$

where $p^{\mathscr{D}_{\mathscr{P}},\mathscr{D}_{\mathcal{X}}}_{\mathrm{triv}}(\lambda) = \sup_{\mathcal{A}}\{\mathsf{Pr}\,[P(x) \leftarrow \mathcal{A}(x) \;:\; x \leftarrow \mathcal{D}_{\mathcal{X}_\lambda}(P)]\}$ is the trivial guessing probability.

8 Construction of Multi-Copy Secure Revocable Programs in a Classical Oracle Model

In this section, we give a construction of multi-copy secure revocable programs; specifically, we work with a classical oracle model. Our construction is as follows:

▶ **Construction 27.** *Let $\lambda \in \mathbb{N}$ be the security parameter. Let $n, m \in \mathbb{N}$ be polymomial in λ. Let $\Phi = \{\Phi_\lambda\}_{\lambda\in\mathbb{N}}$ be an ensemble of permutations $\Phi_\lambda = \{\varphi_\kappa : \{0,1\}^{n+m} \to \{0,1\}^{n+m}\}_{\kappa\in\mathcal{K}_\lambda}$, for some set $\mathcal{K}_\lambda$.*

- $\mathsf{Setup}(1^\lambda)$: sample a uniformly random key $\kappa \in \mathcal{K}_\lambda$ and let $\mathsf{vk} = \kappa$.
- $\mathsf{Compile}(1^\lambda, P)$: on input 1^λ and a program $P \in \mathcal{P}_\lambda$ with $P : \mathcal{X}_\lambda \to \mathcal{Y}_\lambda$, do the following:
  - Sample $y \sim \{0,1\}^m$ and prepare the subset state given by

    $$|S_y\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\varphi_\kappa(x||y)\rangle\,.$$

  - Let $|\Psi_P\rangle = |S_y\rangle$ and, for brevity, let $S = \{\varphi_\kappa(x||y) \;:\; x \in \{0,1\}^n\}$ be the corresponding subset.
  - Let $O = O_{P,S}$ denote an a (public) classical oracle, which is defined as follows:

    $$O_{P,S}(x,s) = \begin{cases} P(x), & \text{if } s \in S \\ 0, & \text{otherwise} \end{cases}$$

- $\mathsf{Eval}^{O}(|\Psi_P\rangle, x)$: on input $|\Psi_P\rangle$, $x \in \mathcal{X}_\lambda$, do the following:
  - Coherently evaluate $O_{P,S}$ on input $|x\rangle \otimes |\Psi_P\rangle$, and compute its output into an ancillary register.
  - Measure the ancillary register and then output the measurement outcome.
- $\mathsf{Revoke}(\mathsf{vk}, \rho)$: on input vk, a state ρ and verification key vk, it parses $y \leftarrow \mathsf{vk}$ and applies the measurement $\{|S_y\rangle\langle S_y|, \mathbb{I} - |S_y\rangle\langle S_y|\}$ to ρ; it outputs $\top$ if it succeeds, and $\perp$ otherwise.

The above scheme is easily seen to satisfy correctness.

Proof of Multi-Copy Revocable Security

Before we analyze the security of Construction 27, let us first remark that we can instantiate the scheme using a QPRP family $\Phi_\lambda = \{\varphi_\kappa : \{0,1\}^{n+m} \to \{0,1\}^{n+m}\}_{\kappa \in \mathcal{K}_\lambda}$, for some key space $\mathcal{K}_\lambda$. In the security proof, however, we will work with the random permutation model instead. This means that we will consider random permutations throughout the security game.

▶ **Theorem 28.** *Construction 27 satisfies multi-copy revocable security for any pair of distributions $\mathcal{D}_{\mathcal{P}}, \mathcal{D}_{\mathcal{X}}$ in a classical oracle model, where the recipient receives an (ideal classical) oracle for the purpose of evaluation.*

Proof. Please see full version. ◀

9 Construction of Multi-Copy Secure Revocable Point Functions in the QROM

Please see the full version for this section.

10 Applications to Sponge Hashing

Please see the full version for this section.

References

1 Scott Aaronson. Quantum copy-protection and quantum money. In *2009 24th Annual IEEE Conference on Computational Complexity*, pages 229–242. IEEE, 2009. doi:10.1109/CCC.2009.42.

2 Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh Vazirani, Chenyi Zhang, and Zixin Zhou. Quantum Pseudoentanglement. In Venkatesan Guruswami, editor, *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*, volume 287 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 2:1–2:21, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ITCS.2024.2.

3 Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 41–60, 2012. doi:10.1145/2213977.2213983.

4 Scott Aaronson, Jiahui Liu, Qipeng Liu, Mark Zhandry, and Ruizhe Zhang. New approaches for quantum copy-protection. In *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part I 41*, pages 526–555. Springer, 2021. doi:10.1007/978-3-030-84242-0_19.

5 Shweta Agrawal, Fuyuki Kitagawa, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa. Public key encryption with secure key leasing. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 581–610. Springer, 2023. doi:10.1007/978-3-031-30545-0_20.

6 Andris Ambainis, Mike Hamburg, and Dominique Unruh. Quantum security proofs using semi-classical oracles. Cryptology ePrint Archive, Paper 2018/904, 2018. URL: https://eprint.iacr.org/2018/904.

7 Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. Pseudorandom (function-like) quantum state generators: New definitions and applications. In *Theory of Cryptography Conference*, pages 237–265. Springer, 2022. doi:10.1007/978-3-031-22318-1_9.

8 Prabhanjan Ananth, Zihan Hu, and Zikuan Huang. Quantum key-revocable dual-regev encryption, revisited. *Cryptology ePrint Archive*, 2024.

9 Prabhanjan Ananth and Fatih Kaleoglu. A note on copy-protection from random oracles. *arXiv preprint*, 2022. arXiv:2208.12884.

10 Prabhanjan Ananth, Fatih Kaleoglu, and Qipeng Liu. Cloning games: A general framework for unclonable primitives. *arXiv preprint*, 2023. arXiv:2302.01874.

11 Prabhanjan Ananth and Rolando L La Placa. Secure software leasing. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 501–530. Springer, 2021. doi:10.1007/978-3-030-77886-6_17.

12 Prabhanjan Ananth, Yao-Ting Lin, and Henry Yuen. Pseudorandom strings from pseudorandom quantum states. In *ITCS*, 2024.

13 Prabhanjan Ananth, Alexander Poremba, and Vinod Vaikuntanathan. Revocable cryptography from learning with errors. In *Theory of Cryptography Conference*, pages 93–122. Springer, 2023. doi:10.1007/978-3-031-48624-1_4.

14 Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In *Annual International Cryptology Conference*, pages 208–236. Springer, 2022. doi:10.1007/978-3-031-15802-5_8.

15 James Bartusek and Dakshita Khurana. Cryptography with certified deletion. In *Advances in Cryptology – CRYPTO 2023: 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023, Proceedings, Part V*, pages 192–223, Berlin, Heidelberg, 2023. Springer-Verlag. doi:10.1007/978-3-031-38554-4_7.

16 James Bartusek, Dakshita Khurana, Giulio Malavolta, Alexander Poremba, and Michael Walter. Weakening assumptions for publicly-verifiable deletion. Cryptology ePrint Archive, Paper 2023/559, 2023. URL: https://eprint.iacr.org/2023/559.

17 James Bartusek, Dakshita Khurana, and Alexander Poremba. Publicly-verifiable deletion via target-collapsing functions. In *Advances in Cryptology – CRYPTO 2023: 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023, Proceedings, Part V*, pages 99–128, Berlin, Heidelberg, 2023. Springer-Verlag. doi:10.1007/978-3-031-38554-4_4.

18 Amit Behera, Zvika Brakerski, Or Sattath, and Omri Shmueli. Pseudorandomness with proof of destruction and applications. In *Theory of Cryptography Conference*, pages 125–154. Springer, 2023. doi:10.1007/978-3-031-48624-1_5.

19 G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. Cryptographic sponge functions. Submission to NIST (Round 3), 2011. URL: http://sponge.noekeon.org/CSF-0.1.pdf.

20 G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. The keccak sha-3 submission. Submission to NIST (Round 3), 2011. URL: http://keccak.noekeon.org/Keccak-submission-3.pdf.

21 John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. Unitary complexity and the uhlmann transformation problem, 2023. doi:10.48550/arXiv.2306.13073.

22 John Bostanci, Jonas Haferkamp, Dominik Hangleiter, and Alexander Poremba. Efficient quantum pseudorandomness from hamiltonian phase states, 2024. doi:10.48550/arXiv.2410.08073.

23 Zvika Brakerski and Omri Shmueli. (pseudo) random quantum states with binary phase. In *Theory of Cryptography Conference*, pages 229–250. Springer, 2019. doi:10.1007/978-3-030-36030-6_10.

24 Anne Broadbent and Rabib Islam. Quantum encryption with certified deletion. In *Theory of Cryptography: 18th International Conference, TCC 2020, Durham, NC, USA, November 16–19, 2020, Proceedings, Part III 18*, pages 92–122. Springer, 2020. doi:10.1007/978-3-030-64381-2_4.

25 Anne Broadbent, Stacey Jeffery, Sébastien Lord, Supartha Podder, and Aarthi Sundaram. Secure software leasing without assumptions. In *Theory of Cryptography Conference*, pages 90–120. Springer, 2021. doi:10.1007/978-3-030-90459-3_4.

26 Anne Broadbent and Sébastien Lord. Uncloneable quantum encryption via oracles. *arXiv preprint*, 2019. arXiv:1903.00130.

27 Alper Çakan and Vipul Goyal. Unclonable cryptography with unbounded collusions. *Cryptology ePrint Archive*, 2023.

28 Orestis Chardouvelis, Vipul Goyal, Aayush Jain, and Jiahui Liu. Quantum key leasing for pke and fhe with a classical lessor. *arXiv preprint*, 2023. arXiv:2310.14328.

29 Google Cloud. Key rotation, 2024. URL: https://cloud.google.com/kms/docs/key-rotation.

30 Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. In *Advances in Cryptology – CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part I*, pages 556–584, Berlin, Heidelberg, 2021. Springer-Verlag. doi:10.1007/978-3-030-84242-0_20.

31 Andrea Coladangelo, Christian Majenz, and Alexander Poremba. Quantum copy-protection of compute-and-compare programs in the quantum random oracle model. *Quantum*, 8:1330, May 2024. doi:10.22331/q-2024-05-02-1330.

32 DGBJ Dieks. Communication by epr devices. *Physics Letters A*, 92(6):271–272, 1982.

33 Tudor Giurgica-Tiron and Adam Bouland. Pseudorandomness from subset states. *arXiv preprint*, 2023. doi:10.48550/arXiv.2312.09206.

34 Fernando Granha Jeronimo, Nir Magrafta, and Pei Wu. Subset states and pseudorandom states. *arXiv preprint*, 2023. doi:10.48550/arXiv.2312.15285.

35 Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38*, pages 126–152. Springer, 2018. doi:10.1007/978-3-319-96878-0_5.

36 Masaru Kada, Harumichi Nishimura, and Tomoyuki Yamakami. The efficiency of quantum identity testing of multiple states. *Journal of Physics A: Mathematical and Theoretical*, 41(39):395309, 2008.

37 Dakshita Khurana and Kabir Tomer. Commitments from quantum one-wayness. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 968–978, 2024. doi:10.1145/3618260.3649654.

38 Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Secure software leasing from standard assumptions. In *Theory of Cryptography Conference*, pages 31–61. Springer, 2021. doi:10.1007/978-3-030-90459-3_2.

39 Jiahui Liu, Qipeng Liu, Luowen Qian, and Mark Zhandry. Collusion resistant copy-protection for watermarkable functionalities. In *Theory of Cryptography Conference*, pages 294–323. Springer, 2022. doi:10.1007/978-3-031-22318-1_11.

40 Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple constructions of linear-depth t-designs and pseudorandom unitaries, 2024. doi:10.48550/arXiv.2404.12647.

41 Tomoyuki Morimae, Alexander Poremba, and Takashi Yamakawa. Revocable quantum digital signatures. *arXiv preprint*, 2023. arXiv:2312.13561.

42 Tomoyuki Morimae and Takashi Yamakawa. One-wayness in quantum cryptography. *arXiv preprint*, 2022. arXiv:2210.03394.

43 Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In *Annual International Cryptology Conference*, pages 269–295. Springer, 2022. doi:10.1007/978-3-031-15802-5_10.

44 Alexander Poremba. Quantum proofs of deletion for learning with errors. *arXiv preprint*, 2022. arXiv:2203.01610.

45 Ronald L Rivest. Can we eliminate certificate revocation lists? In *Financial Cryptography: Second International Conference, FC'98 Anguilla, British West Indies February 23–25, 1998 Proceedings 2*, pages 178–183. Springer, 1998. doi:10.1007/BFB0055482.

46 Stuart G Stubblebine. Recent-secure authentication: Enforcing revocation in distributed systems. In *Proceedings 1995 IEEE Symposium on Security and Privacy*, pages 224–235. IEEE, 1995. doi:10.1109/SECPRI.1995.398935.

47 Dominique Unruh. Revocable quantum timed-release encryption. Cryptology ePrint Archive, Paper 2013/606, 2013. doi:10.1145/2817206.

48 Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983. doi:10.1145/1008908.1008920.

49 Wikipedia. Certificate revocation, 2024. URL: https://en.wikipedia.org/wiki/Certificate_revocation.

50 William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

51 Mark Zhandry. A note on quantum-secure prps, 2016. arXiv:1611.05564.

52 Mark Zhandry. Quantum lightning never strikes the same state twice. or: quantum money from cryptographic assumptions. *Journal of Cryptology*, 34:1–56, 2021.