Publicly-Verifiable Deletion via Target-Collapsing Functions

James Bartusek[*] UC Berkeley

Dakshita Khurana[†] UIUC

Alexander Poremba[‡] Caltech

Abstract

We build quantum cryptosystems that support publicly-verifiable deletion from standard cryptographic assumptions. We introduce target-collapsing as a weakening of collapsing for hash functions, analogous to how second preimage resistance weakens collision resistance; that is, target-collapsing requires indistinguishability between superpositions and mixtures of preimages of an honestly sampled image.

We show that target-collapsing hashes enable publicly-verifiable deletion (PVD), proving conjectures from [Poremba, ITCS'23] and demonstrating that the Dual-Regev encryption (and corresponding fully homomorphic encryption) schemes support PVD under the LWE assumption. We further build on this framework to obtain a variety of primitives supporting publicly-verifiable deletion from weak cryptographic assumptions, including:

- Commitments with PVD assuming the existence of injective one-way functions, or more generally, *almost-regular* one-way functions. Along the way, we demonstrate that (variants of) target-collapsing hashes can be built from almost-regular one-way functions.
- Public-key encryption with PVD assuming trapdoored variants of injective (or almost-regular) one-way functions. We also demonstrate that the encryption scheme of [Hhan, Morimae, and Yamakawa, Eurocrypt'23] based on pseudorandom group actions has PVD.
- X with PVD for $X \in \{$attribute-based encryption, quantum fully-homomorphic encryption, witness encryption, time-revocable encryption$\}$, assuming X and trapdoored variants of injective (or almost-regular) one-way functions.

[*]bartusek.james@gmail.com

[†]dakshita@illinois.edu

[‡]aporemba@caltech.edu

Contents

1 Introduction

Recent research has explored the exciting possibility of combining quantum information with computational hardness to enable classically infeasible cryptographic tasks. Beginning with proposals such as unforgeable money [Wie83], this list has recently grown to include the possibility of provably deleting cryptographic information encoded into quantum states [Unr15, BI20, HMNY21, HMNY22a, HMNY22b, Por23, BK22, BGG+23, AKN+23, APV23].

In this work, we further investigate the task of provable deletion of information via destructive measurements. We focus on building primitives that satisfy *publicly-verifiable deletion* (PVD). This deletion property allows any participant in possession of a quantum encoding to publish a publicly-verifiable classical certificate proving that they deleted[1] the underlying plaintext. This is in contrast to the weaker *privately-verifiable deletion* property, where deletion can be verified only by parties that hold a secret verification key, and this key must remain hidden from the party holding the ciphertext. Public verification is more desirable due to its stronger security guarantee: secret verification keys do not need to be stored in hidden locations, and security continues to hold even when the verification key is leaked. Furthermore, clients can outsource verification of deletion by publishing the verification key itself.

Our approach to building publicly verifiable deletion departs from templates used in prior works on deletion. While most prior works, building on [Unr15, BI20], rely on the combination of a quantum information-theoretic tool such as Wiesner encodings/BB84 states [Wie83, BB84] and a cryptographic object such as an encryption scheme, our work enables publicly-verifiable deletion by directly using simple cryptographic properties of many-to-one hash functions.

The Template, in a Nutshell. When illustrating our approach to publicly-verifiable deletion, it will help to first consider enabling this for a simple cryptographic primitive: a commitment scheme. That is, we consider building a statistically binding non-interactive quantum bit commitment scheme where each commitment is accompanied by a classical, *public* verification key vk. A receiver holding the commitment may generate a classical proof that they deleted the committed bit b, and this proof can be publicly verified against vk. We would like to guarantee that as long as verification accepts, the receiver has information-theoretically removed b from their view and will be unable to recover it given unbounded resources, despite previously having the bit b determined by their view.

To allow verification to be a public operation, it is natural to imagine the certificate or proof of deletion to be a hard-to-find solution to a public puzzle. For instance, the public verification key could be an image y of a (one-way) function, and the certificate of deletion a valid pre-image $f^{-1}(y)$ of this key. Now, the commitment itself must encode the committed bit b in such a way that the ability to generate $f^{-1}(y)$ given the commitment implies information-theoretic deletion of b. This can be enabled by encoding b in the *phase* of a state supported on multiple pre-images of y.

Namely, given an appropriate *two-to-one* function f, a commitment[2] to a bit b can be

$$\mathsf{Com}(b) = \Big(y, |0, x_0\rangle_{\mathsf{A}} + (-1)^b |1, x_1\rangle_{\mathsf{A}}\Big)$$

[1] In this work, we focus on *information-theoretic* deletion of computationally hidden secrets, where the guarantee is that after deletion, even an unbounded adversary cannot recover the plaintext that was previously determined by their view [BK22].

[2] Technically, it is only an appropriate purification of the scheme described here that will satisfy binding; we ignore this detail for the purposes of this overview.

where $(0, x_0), (1, x_1)$ are the two pre-images of (a randomly sampled) image y.

Given an image y and a state on register A, a valid certificate of deletion of the underlying bit could be any pre-image of y, which for a well-formed commitment will be obtained by measuring the A register in the computational basis. It is easy to see that an immediate *honest* measurement of the A register implies information-theoretic erasure of the phase b. But a malicious adversary holding the commitment may decide to perform arbitrary operations on this state in an attempt to find a pre-image y without erasing b.

In this work, we analyze (minimal) requirements on the cryptographic hardness of f in the template above, so that the ability to computationally find any preimage of y given the commitment necessarily implies *information-theoretic* erasure of b. A useful starting point, inspired by recent conjectures in [Por23], is the *collapsing* property of hash functions. This property was first introduced in [Unr16b] as a quantum strengthening of collision-resistance.

Collapsing Functions. The notion of *collapsing* considers an experiment where a computationally bounded adversary prepares an arbitrary superposition of preimages of f on a register A, after which the challenger tosses a random coin c. If $c = 0$, the challenger measures register A, otherwise it measures a register containing the hash y of the value on register A, thus leaving A holding a superposition of preimages of y. The register A is returned to the adversary, and we say that f is collapsing if the adversary cannot guess c with better than negligible advantage. Constructions of collapsing hash functions are known based on LWE [Unr16a], low-noise LPN [Zha22], and more generally on special types of collision-resistant hashes. They have played a key role in the design of post-quantum protocols, especially in settings where proofs of security of these protocols rely on *rewinding* an adversary.

It is easy to see that

$$\mathsf{Com}(b) = \Big(y, |0, x_0\rangle + (-1)^b |1, x_1\rangle\Big)$$

computationally hides the bit b as long as the function f used to build the commitment above is *collapsing*. Indeed, collapsing implies that the superposition $|0, x_0\rangle + (-1)^b |1, x_1\rangle$ is computationally indistinguishable from the result of measurement in the computational basis, and the latter perfectly erases the phase b. However, PVD requires something stronger: we must show that any adversary that generates a valid pre-image of y given the superposition $|0, x_0\rangle + (-1)^b |1, x_1\rangle$, must have *information-theoretically* deleted b from its view, despite b being information-theoretically present in the adversary's view before generating the certificate. We show via a careful proof that this is indeed the case for collapsing f. Proving this turns out to be non-trivial. Indeed, a similar construction in [Por23] based on the Ajtai hash function [Ajt96] relied on an unproven conjecture, which we prove in this work by developing new techniques.

In addition, we show how f in the template above can be replaced with functions that satisfy weaker properties than collapsing, yielding PVD from regular variants of one-way functions. We discuss these results below.

1.1 Our Results

We introduce new properties of (hash) functions, namely target-collapsing, generalized target-collision-resistance. We will show that hash functions satisfying these properties (1) can be based on (regular) variants of one-way functions and (2) imply publicly-verifiable deletion in many settings. Our results also use an intermediate notion, a variant of target-collapsing that satisfies certified everlasting security. Before discussing our results, we motivate and discuss these new definitions informally below.

1.1.1 Definitions

Target-Collapsing and Generalized Target-Collision-Resistant Functions. Towards better understanding the computational assumptions required for PVD, we observe that in the deletion experiment for the commitment above, the superposition $|x_0\rangle + (-1)^b |x_1\rangle$ is prepared by an *honest committer*. This indicates that the collapsing requirement, where security is required to hold even for an adversarial choice of superposition over preimages, may be overkill.

Inspired by this, we consider a natural weakening called *target-collapsing*, where *the challenger (as opposed to the adversary)* prepares a superposition of preimages of a random image y of f on register A. After this, the challenger tosses a random coin c. If $c = 0$, it does nothing to A, otherwise it measures A in the computational basis. The register A is returned to the adversary, and we say that a hash function is target-collapsing if a computationally bounded adversary cannot guess c with better than negligible advantage.

As highlighted above, this definition weakens collapsing to allow the challenger (instead of the adversary) to prepare the preimage register. The weakening turns out to be significant because we show that target-collapsing functions are realizable from relatively weak cryptographic assumptions – namely variants of one-way functions – which are unlikely to imply (standard) collapsing or collision-resistant hash functions due to known black-box separations [Sim98].

To enable these instantiations from weaker assumptions, we first further generalize target-collapsing so that when $c = 1$, the challenger applies a *binary-outcome measurement* M to A (as opposed to performing a computational basis measurement resulting in a singleton preimage). Thus, a template commitment with PVD from generalized target-collapsing hashes has the form:

$$\mathsf{Com}(b) = \left(y, \sum_{x: f(x)=y, M(x)=0} |x\rangle + (-1)^b \sum_{x: f(x)=y, M(x)=1} |x\rangle \right).$$

We show that this commitment satisfies PVD as long as f is target-collapsing w.r.t. the measurement M, and satisfies an additional property of "generalized" target-collision-resistance (TCR), that we discuss next.

Generalized target-collision-resistance is a quantum generalization of the (standard) cryptographic property of second pre-image resistance/target-collision-resistance. Very roughly, this considers an experiment where the challenger first prepares a superposition of preimages of a random image y of f on register A. After this, the challenger applies a measurement (e.g., a binary-outcome measurement) M on A to obtain outcome μ and sends A to the adversary. We require that no polynomially-bounded adversary given register A can output *any* preimage x' of y such that $M(x') \neq M(\mu)$ (except with negligible probability)[3].

Certified Everlasting Target-Collapsing. In order to show PVD, instead of directly relying on target-collapsing (which only considers computationally bounded adversaries), we introduce a stronger notion that we call *certified everlasting* target-collapsing. This considers the following experiment: as before, the challenger prepares a superposition of preimages of a random image y

[3] We remark that this notion can also be seen as a generalization of "conversion hardness" defined in [HMY23].

of f on register A. After this, the challenger tosses a random coin c. If $c = 0$, it does nothing to A, otherwise it applies measurement M to A. The register A is returned to the adversary, after which the adversary is required to return a pre-image of y as its "deletion certificate". While such a certificate can be obtained via an honest measurement of the register A, the *certified everlasting target-collapsing* property requires that the following *everlasting* security guarantee hold. As long as the adversary is computationally bounded at the time of generating a valid deletion certificate, verification of this certificate implies that the bit c is *information-theoretically* erased from the adversary's view, and cannot be recovered even given unbounded resources. That is, if the adversary indeed returns a valid pre-image, they will never be able to guess whether or not the challenger applied measurement M.

1.1.2 New Constructions and Theorems

Main Theorem. Now, we are ready to state the main theorem of our paper. In a nutshell, this says that any (hash) function f that satisfies both target-collapsing and (generalized) target-collision resistance also satisfies *certified everlasting* target-collapsing.

Theorem 1.1. *(Informal). If f satisfies target-collapsing and generalized target-collision-resistance with respect to measurement M, then f satisfies* certified everlasting target-collapsing *with respect to the measurement M.*

We also extend recent results from the collapsing literature [DS22, Zha22, CX22] to show that for the case of binary-outcome (in fact, polynomial-outcome) measurements M, generalized TCR with respect to M actually implies target-collapsing with respect to M. Thus, we obtain the following corollary.

Corollary 1.2. *(Informal). If f satisfies generalized target-collision-resistance with respect to a* binary-outcome *measurement M, then f satisfies* certified everlasting target-collapsing *with respect to the measurement M.*

Resolving the Strong Gaussian Collapsing Conjecture [Por23]. We now apply the main theorem and its corollary to build various cryptographic primitives with PVD. First, we immediately **prove** the following "strong Gaussian-collapsing"[4] conjecture from [Por23], which essentially conjectures that the Ajtai hash function (based on the hardness of SIS) satisfies a certain form of key-leakage security after deletion. This follows from our main theorem because the Ajtai hash function is known to be collapsing [LZ19, Por23] and collision-resistant (which implies that it is target-collapsing and target-collision-resistant when preimages are sampled from the Gaussian distribution).

Conjecture 1 (Strong Gaussian-Collapsing Conjecture, [Por23])**.** *There exist $n, m, q \in \mathbb{N}$ with $m \geq 2$ and $\sigma > 0$ such that, for every efficient quantum algorithm $\mathcal{A}$,*

$$\left|\Pr\left[\mathsf{StrongGaussCollapseExp}_{\mathcal{A},n,m,q,\sigma}(0) = 1\right] - \Pr\left[\mathsf{StrongGaussCollapseExp}_{\mathcal{A},n,m,q,\sigma}(1) = 1\right]\right| \leq \mathrm{negl}(\lambda)$$

with respect to the experiment defined in Figure 1.

$\underline{\mathsf{StrongGaussCollapseExp}_{\mathcal{A},n,m,q,\sigma}(b)}$:

1. The challenger samples $\bar{\mathbf{A}} \xleftarrow{\$} \mathbb{Z}_q^{n\times(m-1)}$ and prepares the Gaussian state

$$|\psi\rangle_{XY} = \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \rho_\sigma(\mathbf{x})\,|\mathbf{x}\rangle_X \otimes |\mathbf{A}\cdot\mathbf{x} \pmod q\rangle_Y\,,$$

   where $\mathbf{A} = [\bar{\mathbf{A}} \,\|\, \bar{\mathbf{A}}\cdot\bar{\mathbf{x}} \pmod q] \in \mathbb{Z}_q^{n\times m}$ is a matrix with $\bar{\mathbf{x}} \xleftarrow{\$} \{0,1\}^{m-1}$.

2. The challenger measures Y in the computational basis, resulting in

$$|\psi_{\mathbf{y}}\rangle_{XY} = \sum_{\substack{\mathbf{x}\in\mathbb{Z}_q^m:\\ \mathbf{A}\mathbf{x}=\mathbf{y} \pmod q}} \rho_\sigma(\mathbf{x})\,|\mathbf{x}\rangle_X \otimes |\mathbf{y}\rangle_Y\,.$$

3. If $b=0$, the challenger does nothing. Else, if $b=1$, the challenger measures system X in the computational basis. The challenger then sends system X to $\mathcal{A}$, together with the matrix $\mathbf{A}\in\mathbb{Z}_q^{n\times m}$ and the string $\mathbf{y}\in\mathbb{Z}_q^n$.

4. $\mathcal{A}$ sends a classical witness $\mathbf{w}\in\mathbb{Z}_q^m$ to the challenger.

5. The challenger checks if $\mathbf{w}$ satisfies $\mathbf{A}\cdot\mathbf{w} = \mathbf{y} \pmod q$ and $\|\mathbf{w}\| \le \sigma\sqrt{m/2}$. If true, the challenger sends the trapdoor vector $\mathbf{t} = (\bar{\mathbf{x}}, -1) \in \mathbb{Z}^m$ to $\mathcal{A}$, where $\mathbf{A}\cdot\mathbf{t} = \mathbf{0} \pmod q$. Else, the challenger outputs a random bit $b' \leftarrow \{0,1\}$ and the game ends.

6. $\mathcal{A}$ returns a bit b', which is retured as the output of the experiment.

Figure 1: The strong Gaussian-collapsing experiment [Por23].

This conjecture, from [Por23] considers a slightly weaker notion of certified collapsing which resembles the notion of certified deletion first proposed by Broadbent and Islam [BI20]. Here, the adversary is not computationally unbounded once a valid deletion certificate is produced; instead, the challenger simply reveals some additional secret information (in the case of the strong Gaussian-collapsing experiment, the challenger reveals a short trapdoor vector for the Ajtai hash function[5]).

Following results from [Por23], we obtain the following cryptosystems with PVD, for the first time from standard cryptographic assumptions.

[4] Here, "Gaussian" refers to a quantum superposition of Gaussian-weighted vectors, where the distribution assigns probability proportional to $\rho_\sigma(\mathbf{x}) = \exp(-\pi\|\mathbf{x}\|^2/\sigma^2)$ for vectors $\mathbf{x}\in\mathbb{Z}^m$ and parameter $\sigma > 0$.

[5] In the strong Gaussian-collapsing experiment it is crucial that the trapdoor is only revealed after a valid certificate is presented; otherwise, the adversary can easily distinguish the collapsed from the non-collapsed world by applying the Fourier transform and using the trapdoor to distinguish LWE samples from uniformly random vectors [Por23].

Theorem 1.3. *(Informal) Assuming the hardness of* LWE *and* SIS *with appropriate parameters, there exists public-key encryption and (leveled) fully-homomorphic encryption with* PVD.

Next, we ask whether one necessarily needs to rely on concrete, highly structured assumptions such as LWE in order to achieve publicly-verifiable deletion, or whether weaker generic assumptions suffice. We present a more general approach to building primitives with PVD from weaker, generic assumptions.

Commitments with PVD **from Regular One-Way Functions.** We first formulate the notion of a *balanced binary-measurement* TCR hash, which is any function that is TCR with respect to some appropriately balanced binary-outcome measurement. By balanced, we mean that the set of preimages of a random image will have significant weight on preimages that correspond to both measurement outcomes (this will roughly be required to guarantee the binding property of our commitment/correctness properties of our encryption schemes). By roughly following the template described above, we show that such hashes generically imply commitments with PVD. Next, we show that such "balanced" functions can be based on (almost-)regular one-way functions[6] By carefully instantiating this outline, we obtain the following results.

Theorem 1.4. *(Informal). Assuming the existence of almost-regular one-way functions, there exists a balanced binary-outcome TCR hash, and consequently there exist commitments with* PVD.

Public-Key Encryption with PVD **from Regular Trapdoor Functions.** Next, we take this framework to the public-key setting, showing that any balanced binary-outcome TCR hash with an additional "trapdoor" property generically implies a public-key encryption scheme with PVD. The additional property roughly requires the existence of a trapdoor for f that enables recovering the phase term from the quantum commitments discussed above: we call this *trapdoor phase-recoverability*. We show that balanced binary-outcome TCR, with trapdoor phase-recoverability, can be based on injective trapdoor one-way functions or pseudorandom group actions (the latter builds on [HMY23]).

Theorem 1.5. *(Informal). Assuming the existence of injective trapdoor one-way functions or pseudorandom group actions, there exists a balanced binary-outcome TCR hash with trapdoor phase-recoverability, and consequently there exists public-key encryption with* PVD.

We also show that injectivity requirement on the trapdoor function can be further relaxed to a notion of "superposition-invertible" trapdoor regular one-way function for the results above. Informally, this is a regular one-way function, where a trapdoor allows one to obtain a uniform superposition over all preimages of a given image. This is an example of a *generic assumption* that is not known to, and perhaps is unlikely to, imply classical public-key encryption – but does imply PKE with quantum ciphertexts, and in fact even one that supports PVD. The only other assumption in this category is the concrete assumption that pseudorandom group actions exist [HMY23].

Theorem 1.6. *(Informal). Assuming the existence of superposition-invertiable regular trapdoor functions, there exists a balanced binary-outcome TCR hash with trapdoor phase-recoverability and consequently, there exists public-key encryption with* PVD.

[6] This is a generalization of regular one-way functions where preimage sets for different images should be polynomially related in size.

Advanced Encryption with PVD **from Weak Assumptions** Finally, we show that hybrid encryption gives rise to a generic compiler for encryption with PVD, obtaining the following results.

Theorem 1.7. *(Informal). Assuming the existence of injective trapdoor one-way functions or pseudorandom group actions, and $X \in \{$attribute-based encryption, quantum fully-homomorphic encryption, witness encryption, timed-release encryption$\}$, there exists X with* PVD*.*

Prior to this work, while there existed encryption schemes with PVD from non-standard assumptions such as one-shot signatures [HMNY21], conjectured strong collapsing [Por23] or post-quantum indistinguishability obfuscation [BGG+23], no basic or advanced cryptosystems supporting PVD were known from standard assumptions. We provide a more detailed overview of prior work below.

1.2 Prior work

The first notion resembling *certified deletion* was introduced by Unruh [Unr15] who 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. Unruh's scheme uses conjugate coding [Wie83, BB84] and relies on the *monogamy of entanglement* in order to guarantee that revocation necessarily erases information about the plaintext. Broadbent and Islam [BI20] introduced the notion of *certified deletion* and constructed a private-key quantum encryption scheme with the aforementioned feature which is inspired by the quantum key distribution protocol [BB84, TL17]. In contrast with Unruh's [Unr15] notion of revocable quantum ciphertexts which are eventually returned and verified, Broadbent and Islam [BI20] consider certificates which are entirely classical. Moreover, the security definition requires that, once the certificate is successfully verified, the plaintext remains hidden even if the secret key is later revealed. Inspired by the notion of quantum copy-protection [Aar09], Ananth and La Placa [AL21] defined a form of quantum software protection called *secure software leasing* whose anti-piracy notion requires that the encoded program is returned and verified.

Using a hybrid encryption scheme, Hiroka, Morimae, Nishimaki and Yamakawa [HMNY21] extended the scheme in [BI20] to both public-key and attribute-based encryption with privately-verifiable certified deletion via *receiver non-committing* encryption [JL00, CFGN96]. Hiroka, Morimae, Nishimaki and Yamakawa [HMNY22b] considered *certified everlasting zero-knowledge proofs* for QMA via the notion of *everlasting security* which was first formalized by Müller-Quade and Unruh [MU07]. Bartusek and Khurana [BK22] revisited the notion of certified deletion and presented a unified approach for how to generically convert any public-key, attribute-based, fully-homomorphic, timed-release or witness encryption scheme into an equivalent quantum encryption scheme with certified deletion. In particular, they considered a stronger notion called *certified everlasting security* which allows the adversary to be computationally unbounded once a valid deletion certificate is submitted. This is also the definition we consider in this work. In the same spirit, Hiroka, Morimae, Nishimaki and Yamakawa [HMNY22a] gave a *certified everlasting* functional encryption scheme which allows the receiver of the ciphertext to obtain the outcome specific function applied the plaintext, but nothing else. In other very recent work, Ananth, Poremba and Vaikuntanathan [APV23] used Gaussian superpositions to construct (key)-revocable cryptosystems, such as public-key encryption, fully homomorphic encryption and pseudorandom functions assuming the hardness of LWE, and Agarwal et al. [AKN+23] introduced a generic compiler for adding key-revocability to a variety of cryptosystems. In these systems, the cryptographic key consists of a quantum state which can later be *certifiably revoked* via a quantum channel – in contrast with the classical deletion certificates for ciphertexts considered in this work.

Cryptosystems with Publicly Verifiable Deletion. First, in addition to their results in the setting of private verification, [HMNY21] also gave a public-key encryption scheme with certified deletion which is *publicly verifiable* assuming the existence of one-shot signatures (which rely on strong black-box notions of obfucation) and extractable witness encryption. Using *Gaussian superpositions*, Poremba [Por23] proposed *Dual-Regev*-based public-key and fully homomorphic encryption schemes with certified deletion which are publicly verifiable and proven secure assuming the (then unproven) *strong Gaussian-collapsing conjecture* — a strengthening of the collapsing property of the Ajtai hash. Finally, a recent work [BGG+23] relies on post-quantum indistinguishability obfuscation (iO) to obtain both publicly verifiable deletion and publicly verifiable key revocation. This is a strong assumption for which we have candidates, but no constructions based on standard (post-quantum) assumptions at this time.

2 Technical Overview

In this overview, we begin by discussing the key ideas involved in proving our main theorem. We show how to prove publicly verifiable deletion for a toy protocol that relies on stronger assumptions than the ones that we actually rely on in our actual technical sections.

Next, we progressively relax these assumptions to instantiate broader frameworks, including the one from [Por23], obtaining public-key encryption and fully-homomorphic encryption with PVD from LWE/SIS.

Finally, we further generalize this to enable constructions from weak cryptographic assumptions – including commitments with PVD from variants of one-way functions and PKE with PVD from trapdoored variants of the same assumption. We also discuss a hybrid approach that enables a variety of advanced encryption schemes supporting PVD.

2.1 Proving Our Main Theorem

Consider the toy commitment

$$\mathsf{Com}(b) = \Big(y, |0, x_0\rangle + (-1)^b\,|1, x_1\rangle\Big)$$

where $(0, x_0), (1, x_1)$ are preimages of y under a structured two-to-one function f, where every image has a preimage that begins with a 0 and another that begins with a 1. We note that this commitment can be efficiently prepared by first preparing a superposition over all preimages

$$\sum_{b\in\{0,1\}, x\in\{0,1\}^\lambda} |b, x\rangle$$

on a register X, then writing the output of f applied on X to register Y, and finally measuring the contents of register Y to obtain image y. The register X contains $|0, x_0\rangle + |1, x_1\rangle$, which can be converted to $|0, x_0\rangle + (-1)^b\,|1, x_1\rangle$ via (standard) phase kickback.

To show that the commitment satisfies publicly-verifiable deletion, we consider an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ where $\mathcal{A}_1$ is (quantum) polynomial time and $\mathcal{A}_2$ is unbounded, participating in the following experiment.

- The challenger samples $b \leftarrow \{0,1\}$ and runs $\mathsf{Expmt}_0(b)$, described below.
  $\underline{\mathsf{Exmpt}_0(b):}$
  1. Prepare $\left(|0, x_0\rangle + (-1)^b |1, x_1\rangle, y\right)$ on registers A, B and send them to $\mathcal{A}_1$.
  2. $\mathcal{A}_1$ outputs a (classical) deletion certificate γ,[7] and left-over state ρ.
  3. If $f(\gamma) \neq y$, output a uniformly random bit $b' \leftarrow \{0,1\}$, otherwise output $b' = \mathcal{A}_2(\rho)$.
- The advantage of $\mathcal{A}$ is defined to be $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Expmt}_0} = \left|\Pr[b' = b] - \frac{1}{2}\right|$.

We discuss how to prove the following.

Claim 2.1. *(Informal). For every $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ where $\mathcal{A}_1$ is (quantum) computationally bounded,*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Expmt}_0} = \operatorname{negl}(\lambda),$$

as long as f is target collapsing and target collision-resistant w.r.t. a computational basis measurement of the pre-image register.

Overview of the Proof of Claim 2.1. To prove this claim, we must show that b is information-theoretically *removed* from the leftover state of any $\mathcal{A}_1$ that generates a valid pre-image of y, despite the fact that the adversary's view contains b at the beginning of the experiment.

Proof techniques for this type of experiment were recently introduced in [BK22] in the context of *privately verifiable deletion* via BB84 states. Inspired by their method, our first step is to defer the dependence of the experiment on the bit b. In more detail, we will instead imagine sampling the distribution by guessing a uniformly random $c \leftarrow \{0,1\}$, and initializing the adversary with $(|x_0\rangle + (-1)^c |x_1\rangle, y)$. The challenger later obtains input b and aborts the experiment (outputs $\perp$) if $c \neq b$. Since c was a uniformly random guess, the trace distance between the $b = 0$ and $b = 1$ outputs of this modified experiment is at least half the trace distance between the outputs of the original experiment. Moreover, we can further delay the process of obtaining input b, and then abort or not until *after* the adversary outputs a certificate of deletion. That is, we can consider a *purification* where a register C contains a superposition $|0\rangle + |1\rangle$ of two choices for c, and is later measured to determine bit c. This experiment is discussed in detail below.

$\underline{\mathsf{Expmt}_1(b)}$: The experiment proceeds as follows.

1. Prepare the $|+\rangle$ state on an ancilla register C, and a superposition of preimages $|x_0\rangle + |x_1\rangle$ of a random y on register A.
2. Then, controlled on the contents of register C, do the following: if the control bit is 0, do nothing, and otherwise flip the phase on x_1 (via phase kickback), changing the contents of A to $|x_0\rangle - |x_1\rangle$. This means that the overall state is

   $$\frac{1}{\sqrt{2}} \sum_{c \in \{0,1\}} |c\rangle_{\mathsf{C}} \otimes |0, x_0\rangle_{\mathsf{A}} + (-1)^c |1, x_1\rangle_{\mathsf{A}}$$

   Send A to $\mathcal{A}_1$.

[7] If the $\mathcal{A}_1$ outputs a quantum state as their certificate, the state is measured in the computational basis to obtain a classical certificate γ.

3. Obtain from $\mathcal{A}_1$ a purported certificate of deletion γ.

4. If $f(\gamma) \neq y$, abort, and otherwise measure register C to obtain output c, and abort if $c \neq b$. In the case of abort, output a uniformly random bit $b' \leftarrow \{0,1\}$.

5. If no aborts occurred, output $b' = \mathcal{A}_2(\rho)$.

We note that the event $c = b$ occurs with probability exactly $\frac{1}{2}$, and since measurements on separate subsystems commute, we have that

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Expmt}_1} \geq \frac{1}{2}\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Expmt}_0}. \tag{1}$$

where $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Expmt}_1} = \left|\Pr[\mathsf{Expmt}_1(b) = b] - \frac{1}{2}\right|$ for $b \leftarrow \{0,1\}$.

Once the dependence of the experiment on b has been deferred, as above, we can consider another experiment (described below) where the challenger measures the contents of register A *before* sending it to $\mathcal{A}_1$. Intuitively, performing this measurement *removes* information about b from $\mathcal{A}_1$'s view in a manner that is computationally undetectable by $\mathcal{A}_1$ (due to the target-collapsing property of f).

$\underline{\mathsf{Expmt}_2(b)}$: The experiment proceeds as follows.

- Prepare the $|+\rangle$ state on an ancilla register C, and a superposition of preimages $|x_0\rangle + |x_1\rangle$ of a random y on register A. *Next, measure register* A *in the computational basis.*

  Then, controlled on the contents of register C, do the following: if the control bit is 0, do nothing, and otherwise flip the phase on x_1. This means that the overall state is a uniform mixture of the states

  $$\frac{1}{\sqrt{2}} \sum_{c \in \{0,1\}} |c\rangle_{\mathsf{C}} \otimes |0, x_0\rangle_{\mathsf{A}} \text{ and } \frac{1}{\sqrt{2}} \sum_{c \in \{0,1\}} (-1)^c |c\rangle_{\mathsf{C}} \otimes |1, x_1\rangle_{\mathsf{A}}$$

  Finally, send A to $\mathcal{A}_1$.

- Obtain from $\mathcal{A}_1$ a purported certificate of deletion γ.

- If $f(\gamma) \neq y$, abort, otherwise measure register C to obtain output c, and abort if $c \neq b$. In the case of abort, output a uniformly random bit $b' \leftarrow \{0,1\}$.

- If no aborts occurred, output $b' = \mathcal{A}_2(\rho)$.

As described above, the target-collapsing property of f implies that $\mathcal{A}_1$ cannot (computationally) distinguish the register A obtained in $\mathsf{Expmt}_2(b)$ from the one obtained in $\mathsf{Expmt}_1(b)$. However, this is not immediately helpful: information about which experiment $\mathcal{A}_1$ participated in could potentially be encoded into $\mathcal{A}_1$'s left-over state ρ, so that it remains computationally hidden from $\mathcal{A}_1$ but can be extracted by (unbounded) $\mathcal{A}_2$. And it is after all the output of $\mathcal{A}_2$ that determines the advantage of $\mathcal{A}$. Because of $\mathcal{A}_2$ being unbounded and the experiments only being *computationally* indistinguishable, even if we could show that $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Expmt}_2} = \mathrm{negl}(\lambda)$, it is unclear how to use this to show our desired claim, i.e., $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Expmt}_0} = \mathrm{negl}(\lambda)$. It may appear that the proof is stuck.

To overcome this issue, we will aim to identify an *efficiently computable predicate* of the challenger's system, which will *imply* the following (inefficient) property: when $\mathcal{A}_1$ outputs a valid deletion certificate, even an unbounded $\mathcal{A}_2$ cannot determine whether it participated in $\mathsf{Expmt}_1(b)$ or $\mathsf{Expmt}_2(b)$, i.e., $\mathcal{A}_1$'s left-over state is information-theoretically independent of b.

Identifying an Efficiently Computable Predicate. Observe that in $\mathsf{Expmt}_2(b)$, the ancilla register C is *unentangled* with the rest of the experiment. In fact, the ancilla register is exactly $|+\rangle$ when we give the adversary $|0, x_0\rangle$ on register A, and $|-\rangle$ when we give the adversary $|1, x_1\rangle$ on register A. Moreover, in $\mathsf{Expmt}_2(b)$, the target-collision-resistance of f implies that the computationally-bounded $\mathcal{A}_1$ given x_0 cannot output x_1 as their deletion certificate (and vice-versa).

This, along with the fact that the certificate *must* be a pre-image of y means that the following guarantee holds (except with negligible probability) in $\mathsf{Expmt}_2(b)$:

When the adversary outputs a valid certificate γ, a projection of the pre-image register onto $|+\rangle$ succeeds if $\gamma = (0, x_0)$ and a projection of the pre-image register onto $|-\rangle$ succeeds if $\gamma = (1, x_1)$.

At this point, we can rely on the target-collapsing property of f to prove the following claim: the *efficient projection* described above also succeeds except with negligible probability in $\mathsf{Expmt}_1(b)$, when the adversary generates a valid deletion certificate. If this claim is not true, then since the experiments (including $\mathcal{A}_1$) run in quantum polynomial time until the point that the deletion certificate is generated, and the projection is efficient, one can build a reduction that contradicts target-collapsing of f. This reduction obtains a challenge (which is either a superposition when the challenger did not measure, or a mixture if the challenger did measure) on register A, prepares ancilla C as in $\mathsf{Expmt}_1(b)$, then follows steps 2, 3 identically to $\mathsf{Expmt}_1(b)$. Next, given a deletion certificate (β, x_β), the reduction projects C onto $|0\rangle + (-1)^\beta |1\rangle$, outputting 1 if the projection succeeds and 0 otherwise.

Introducing an Alternative Experiment. Having established that the projection above must succeed in $\mathsf{Expmt}_1(b)$ except with negligible probability, we can now consider an alternative experiment $\mathsf{Expmt}_{\mathsf{alt}}(b)$. This is identical to $\mathsf{Expmt}_1(b)$, except that the challenger *additionally* projects register C onto $|0\rangle + (-1)^\beta |1\rangle$ when the adversary generates a valid certificate (β, x_β). We established above that the projection is successful in $\mathsf{Expmt}_1(b)$ except with negligible probability, and this implies that

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Expmt}_{\mathsf{alt}}} \geq \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Expmt}_1} - \mathrm{negl}(\lambda) \tag{2}$$

where as before, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Expmt}_{\mathsf{alt}}} = \left| \Pr[\mathsf{Expmt}_{\mathsf{alt}}(b) = b] - \frac{1}{2} \right|$ for $b \leftarrow \{0,1\}$.

Crucially, in $\mathsf{Expmt}_{\mathsf{alt}}(b)$, the bit c is determined by a measurement on register C which is *unentangled* with the system and in either the $|+\rangle$ or $|-\rangle$ state (due to the projective measurement that we just applied). Thus, measuring C in the computational basis results in a uniformly random and independent c. By definition of the experiment (abort when $b \neq c$, continue otherwise) – this implies that the bit b is set in a way that is uniformly random and independent of the adversary's view, and thus

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Expmt}_{\mathsf{alt}}} = 0 \tag{3}$$

Now, equations (1, 2, 3) together yield the desired claim, that is, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{Expmt}_0} = \mathrm{negl}(\lambda)$.

This completes a simplified overview of our key ideas, assuming the existence of a perfectly 2-to-1 function f where every image y has preimages $((0, x_0), (1, x_1))$, and where f satisfies both target-collapsing and target-collision-resistance. Unfortunately, we do not know how to build functions satisfying these clean properties from simple generic assumptions. Instead, we will generalize the template above, where the first generalization will no longer require f be 2-to-1.

Generalizing the Template. First, note that we can replace $|0, x_0\rangle$ and $|1, x_1\rangle$ with superpositions over two disjoint sets of preimages of y separated via an efficient binary-outcome measurement, namely

$$\mathsf{Com}(b) = \sum_{x:f(x)=y,M(x)=0} |x\rangle + (-1)^b \sum_{x:f(x)=y,M(x)=1} |x\rangle$$

We can even consider measurements M that have arbitrarily many outcomes. Proof ideas described above also generalize almost immediately to show that for any M, Com satisfies PVD as long as f is target-collapsing and target-collision resistant w.r.t. M. In fact, we can generalize this even further (see our main results in Section 4.2, 4.3) to consider arbitrary (as opposed to uniform) distributions over pre-images, as well as to account for any auxiliary information that may be sampled together with the description of the hash function.

Certified Everlasting Target-Collapsing. As discussed in the results section, our actual technical proofs proceed in two parts. (1) Show that for any M, a function f that is target-collapsing and target-collision resistant w.r.t. M is also *certified everlasting* target-collapsing w.r.t. M, and (2) show that f being *certified everlasting* target-collapsing implies that Com satisfies publicly verifiable deletion.

Recall that *certified* everlasting target collapsing requires that an adversary that outputs a valid deletion certificate information-theoretically loses the bit b determining whether they received a superposition or a mixture of preimages. Our proof of certified everlasting target-collapsing follows analogously to the proof sketched above. In short, we defer measurement of a bit b which decides whether the adversary is given a superposition or a mixture, and then rely on target-collapsing and target-collision-resistance to argue that an efficient projection on the challenger's state (almost) always succeeds when the adversary outputs a valid certificate. We finally show that success of this projection implies that the adversary's state is information-theoretically independent of b.

The certified everlasting target-collapsing property almost immediately implies certified deletion security of Com via a hybrid argument:

- In Hyb_0, the adversary obtains register A containing

$$\mathsf{Com}(0) = \sum_{x:f(x)=y,M(x)=0} |x\rangle + \sum_{x:f(x)=y,M(x)=1} |x\rangle$$

- In Hyb_1, the measurement M is applied to A before sending it to the adversary.

- In Hyb_2, the adversary obtains register A containing

$$\mathsf{Com}(1) = \sum_{x:f(x)=y,M(x)=0} |x\rangle - \sum_{x:f(x)=y,M(x)=1} |x\rangle$$

The certified everlasting hiding property of f guarantees that all hybrids are statistically close when the adversary outputs a valid deletion certificate. Moreover, these experiments abort and output a random bit when the adversary does not output a valid certificate, and it is easy to show (by computational indistinguishability) that the probability of generating a valid certificate remains negligibly close between experiments.

TCR Implies Target-Collapsing for Polynomial-Outcome Measurements We also show that when M has polynomially many possible outcomes, then TCR implies target-collapsing w.r.t. M. This follows from techniques that were recently developed in the literature on collapsing versus collision resistant hash functions [DS22, Zha22, CX22]. In a nutshell, these works showed that any distinguisher that distinguishes mixtures from superpositions over preimages for an *adversarially chosen* image y, can be used to swap between pre-images, and therefore find a collision for y. We observe that their technique is agnostic to whether the image y is chosen randomly (in the targeted setting) or adversarially. Furthermore, it also extends to swapping superpositions over sets of pre-images to superpositions over other sets. These allow us to prove (Section 4.4) that TCR w.r.t. any polynomial-outcome measurement M implies target-collapsing w.r.t. M.

2.2 Publicly-Verifiable Deletion via Gaussian Superpositions

In Section 5, we revisit the *Dual-Regev* public-key and (leveled) fully homomorphic encryption schemes with publicly-verifiable deletion which were proposed by Poremba [Por23] and were conjectured to be secure under the *strong Gaussian-collapsing property*. By applying our main theorem to the Ajtai hash function, we obtain a proof of the conjecture, which allows us to show the certified everlasting security of the aforementioned schemes assuming the hardness of the LWE assumption.

The constructions introduced in [Por23] exploit the the duality between LWE and SIS [SSTX09], and rely on the fact that one encode Dual-Regev ciphertexts via Gaussian superpositions. Below, we give a high-level sketch of the basic public-key construction.

- To generate a pair of keys $(\mathsf{sk}, \mathsf{pk})$, sample a random $\mathbf{A} \in \mathbb{Z}_q^{n \times (m+1)}$ together with a particular short trapdoor vector $\mathbf{t} \in \mathbb{Z}^{m+1}$ such that $\mathbf{A} \cdot \mathbf{t} = \mathbf{0} \pmod q$. Let $\mathsf{pk} = \mathbf{A}$ and $\mathsf{sk} = \mathbf{t}$.
- To encrypt $b \in \{0,1\}$ using $\mathsf{pk} = \mathbf{A}$, generate the following for a random $\mathbf{y} \in \mathbb{Z}_q^n$:

$$\mathsf{vk} \leftarrow (\mathbf{A}, \mathbf{y}), \qquad |\mathsf{CT}\rangle \leftarrow \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \sum_{\mathbf{e} \in \mathbb{Z}_q^{m+1}} \rho_{q/\sigma}(\mathbf{e})\, \omega_q^{-\langle \mathbf{s}, \mathbf{y} \rangle}\, |\mathbf{s}^\intercal \mathbf{A} + \mathbf{e}^\intercal + b \cdot (0, \dots, 0, \lfloor \frac{q}{2} \rfloor)\rangle\,,$$

  where vk is a public verification key and $|\mathsf{CT}\rangle$ is the quantum ciphertext for $\sigma > 0$.
- To decrypt $|\mathsf{CT}\rangle$ using sk, measure in the computational basis to obtain $\mathbf{c} \in \mathbb{Z}_q^{m+1}$, and output 0, if $\mathbf{c}^\intercal \cdot \mathsf{sk} \in \mathbb{Z}_q$ is closer to 0 than to $\lfloor \frac{q}{2} \rfloor$, and output 1, otherwise. Here $\mathsf{sk} = \mathbf{t}$ is chosen such that $\mathbf{c}^\intercal \cdot \mathsf{sk}$ yields an approximation of $b \cdot \lfloor \frac{q}{2} \rfloor$ from which we can recover b.

To delete the ciphertext $|\mathsf{CT}\rangle$, perform a measurement in the Fourier basis. Poremba [Por23] showed that the Fourier transform of $|\mathsf{CT}\rangle$ results in the *dual* quantum state given by

$$|\widehat{\mathsf{CT}}\rangle = \sum_{\substack{\mathbf{x} \in \mathbb{Z}_q^{m+1}: \\ \mathbf{A}\mathbf{x} = \mathbf{y} \pmod q}} \rho_\sigma(\mathbf{x})\, \omega_q^{\langle \mathbf{x}, b \cdot (0, \dots, 0, \lfloor \frac{q}{2} \rfloor)\rangle}\, |\mathbf{x}\rangle\,.$$

In other words, a Fourier basis measurement of $|\mathsf{CT}\rangle$ will necessarily erase all information about the plaintext $b \in \{0,1\}$ and results in a *short* vector $\pi \in \mathbb{Z}_q^{m+1}$ such that $\mathbf{A} \cdot \pi = \mathbf{y} \pmod{q}$. To publicly verify a deletion certificate, simply check whether a certificate π is a solution to the (inhomogenous) SIS problem specified by $\mathsf{vk} = (\mathbf{A}, \mathbf{y})$. Due to the hardness of the SIS problem, it is computationally difficult to produce a valid deletion certificate from $(\mathbf{A}, \mathbf{y})$ alone.

Our approach to proving certified everlasting security of the Dual-Regev public-key and fully-homomorphic encryption schemes with publicly-verifiable deletion in [Por23] is as follows. First, we observe that the Ajtai hash function is both target-collapsing and target-collision-resistant with respect to the discrete Gaussian distribution. Here, the former follows from LWE as a simple consequence of the *Gaussian-collapsing property* previously shown by Poremba [LZ19, Por23], whereas the latter follows immediately from the quantum hardness of SIS. Thus, our main theorem implies that the Ajtai hash function is certified-everlasting target-collapsing (see Theorem 5.5). Finally, as a simple corollary of our theorem, we obtain a proof of the *strong Gaussian-collapsing conjecture* in [Por23], which we state in Corollary 5.6. We also note that the aforementioned conjecture considers a weaker notion of certified collapsing which resembles the notion of certified deletion first proposed by Broadbent and Islam [BI20]. Here, the adversary is not computationally unbounded once a valid deletion certificate is produced; instead, the challenger simply reveals additional secret information (in the case of the strong Gaussian-collapsing experiment, this is a short trapdoor vector for the Ajtai hash function). Our notion of certified everlasting target-collapsing is significantly stronger; in particular, it implies the weaker collapsing scenario considered by Poremba [Por23]. This follows from the fact that the security reduction can simply brute-force search for a short trapdoor solution for the Ajtai hash once it enters the phase in which it is allowed to be computationally unbounded. We exploit this fact in the proof of Corollary 5.6.

2.3 Weakening Assumptions for Publicly-Verifiable Deletion

Next, we look for instantiations of the above template from *generic* cryptographic assumptions, as opposed to structured specific assumptions such as LWE. Here, all of our instantiations only require us to consider functions that are target-collision-resistant and target-collapsing w.r.t. binary-outcome measurements (and as discussed above, TCR implies certified-everlasting target-collapsing in this setting). In addition, for the case of commitments, in order for the commitment to satisfy binding[8], we require that there is a measurement that can distinguish

$$\sum_{x: f(x)=y, M(x)=0} |x\rangle + \sum_{x: f(x)=y, M(x)=1} |x\rangle$$

from

$$\sum_{x: f(x)=y, M(x)=0} |x\rangle - \sum_{x: f(x)=y, M(x)=1} |x\rangle$$

with probability δ for any constant $0 < \delta \leq 1$. For the case of public-key encryption, we similarly require that a trapdoor be able to recover the phase with constant probability. We then resort to

[8] We actually prove that a purification of the template commitment described above satisfies honest-binding [Yan22]. Namely, the committer generates the state above but leaves registers containing the image y (and the key, if f is a keyed function) unmeasured, and holds on to these registers for the opening phase. It can later either open the commitment by sending these registers to a receiver, or request deletion, by measuring them and publishing y (and any keys for the function).

standard amplification techniques to boost correctness error from constant to (negligibly close to) 0. We note that this amplification would also work if the phase was recoverable with inverse-polynomial δ (as opposed to constant); however, we focus on constant δ because of simplicity, and because it suffices for our instantiations.

In the template above, we observe that a measurement can find the phase with inverse polynomial probability whenever the sets

$$\sum_{x:f(x)=y,M(x)=0} |x\rangle \text{ and } \sum_{x:f(x)=y,M(x)=1} |x\rangle$$

are somewhat "balanced", i.e. for a random image y, for sets $S_0 = \{x : f(x) = y, M(x) = 0\}$ and $S_1 = \{x : f(x) = y, M(x) = 1\}$, we have that $\frac{|S_0|}{|S_1|}$ is a fixed constant. We show in Section 6.1 and Section 6.2 that commitments and PKE with PVD can be obtained from appropriate variants of TCR functions following this template.

Now, our goal is to build such TCR functions from generic assumptions. A natural idea would be to start with any one-way function f and compose it with a random two-to-one hash h defined on its range[9]. Then, any output y of the composed function $(h \circ f)$ is associated with two elements $\{z_0, z_1\} = h^{-1}(y)$ in the range of f, and the binary-outcome measurement would measure one of z_0 or z_1. Recalling that we eventually want to prove target-collision-resistance, the hope would be that just given a superposition over the preimages of, say, z_0, the one-wayness of f would imply the difficulty of finding a preimage of z_1[10]. This could give the type of TCR property we need.

Technical Bottlenecks, and a Resolution. Unfortunately, there are two issues with the approach proposed above. First, f may be extremely unbalanced, so that the relative sizes of the sets of preimages of two random points y_1, y_2, i.e. $|\{x : f(x) = y_1\}|$ and $|\{x : f(x) = y_2\}|$ in its image may have very different sizes, that are not polynomially related with each other. There may even be many points in the co-domain/range that have *zero* preimages (for a general OWF, we cannot guarantee that its image is equal to its range). A second related issue is that the above sketched reduction to one-wayness may not work. Let's say we choose h to be a two-to-one function defined by a random shift Δ, i.e. $h(x) = h(x \oplus \Delta)$. Then we are essentially asking that it be hard to invert a random *range* element of f, as opposed to $f(x)$ for a random *domain* element x, which is the standard one-wayness assumption.

We don't know how to make this approach work from arbitrary one-way functions, which we leave as an open question. Instead, we appeal to a result of [HHK+09], who in the classical context of building statistically hiding commitments, show the following result. By appropriately combining an (almost)-*regular*[11] one-way function with universal hash functions, it *is* possible to obtain a function f with exactly the required properties: sufficiently balanced, and one-way over its *range*. The former property means that an overwhelming fraction of range elements have

[9]The *co-domain* of a function $f : \{0,1\}^n \to \{0,1\}^m$ is $\{0,1\}^m$, and we will also refer to this as the *range* of the function in this paper. The *image* is the set of all actual output values of f, i.e. the set $\{y : \exists x \text{ such that } f(x) = y\}$. The co-domain/range may in general be a superset of the image of a function.

[10]More concretely, a purported reduction to one-wayness when given challenge image z_1, can sample a random image z_0 with its preimages, then find h s.t. $h(z_0) = h(z_1)$, thereby using a TCR adversary to find a preimage of the given challenge z_1.

[11]An almost regular one-way function generalizes regular one-way functions to require only that for any two images y_1, y_2 of the function, the sizes of preimage sets of y_1, y_2 are polynomially related. In particular, injective functions, and (standard) regular functions also satisfy almost-regularity.

similar-sized preimage sets, while the latter property says that an element y sampled randomly from the range of the function cannot be inverted except with negligible probability. This resolves both the difficulties above.

Given such a balanced function f, we apply a random two-to-one hash h defined by a shift Δ to the range of this f. We prove in Section 6.4 that this implies the flavor of target-collision-restistant hash that we need to construct commitments with PVD.

Public-Key Encryption with PVD**.** Next, we note that the construction above *also* yields a public-key encryption scheme, as long as there is a trapdoor that allows recovery of the phase b given the state

$$y, \sum_{x:f(x)=y,M(x)=0} |x\rangle + (-1)^b \sum_{x:f(x)=y,M(x)=1} |x\rangle$$

We call this property "trapdoor phase-recoverability". We show that this property is achievable from generic assumptions, even those that are not known to imply classical PKE.

- Specifically, trapdoor phase-recoverability is implied by a trapdoored variant of (almost) regular one-way functions, for which a trapdoor to the function allows recovery of a uniform superposition over all preimages of any given image y. This then allows efficient projection onto $\sum_{x:f(x)=y,M(x)=0} |x\rangle + (-1)^b \sum_{x:f(x)=y,M(x)=1} |x\rangle$ for any efficient M. We also note that this property is satisfied by any (standard) trapdoored injective function. But it is also satisfied by functions such as the Ajtai function that are not necessarily injective. Indeed, it is unclear how to build classical public-key encryption, or even PKE with classical ciphertexts, given a general trapdoor phase-recoverable function. Nevertheless, we formalize the above ideas in Section 6.2 and Section 6.4 to build PKE schemes with quantum ciphertexts, that also support PVD.

- Additionally, we show in Section 6.5 that a recent public-key encryption scheme of [HMY23] from pseudorandom group actions also satisfies trapdoor phase-recoverability: in fact, the decryption algorithm in [HMY23] relies on recovering the phase from a similar superposition, given a trapdoor.

Hybrid Encryption with PVD. Finally, we observe that we can use any encryption scheme Enc to encrypt the trapdoor td associated with the above construction, and security will still hold. That is, if Enc is semantically-secure, then our techniques extend to show that a ciphertext of the form

$$y, \sum_{x:f(x)=y,M(x)=0} |x\rangle + (-1)^b \sum_{x:f(x)=y,M(x)=1} |x\rangle, \mathsf{Enc}(\mathsf{td})$$

where td is the trapdoor for f, still supports publicly-verifiable deletion of the bit b. Thus, our approach can be seen as a way to *upgrade* cryptographic schemes Enc with special properties to satisfy PVD. In particular, we prove in Section 6.3 that instantiating Enc appropriately with attribute-based encryption, fully-homomorphic encryption, witness encryption, or timed-release encryption gives us the same scheme supporting PVD.

2.4 Discussion and Directions for Future Work

Our work demonstrates a strong relationship between weak security properties of (trapdoored) one-way functions and publicly-verifiable deletion. In particular, previous work [Por23] conjectured that collapsing functions, which are a quantum strengthening of collision-resistant hashes, lead to cryptosystems with publicly-verifiable deletion. Besides proving this conjecture, we also show that collapsing/collision-resistance, which are considered stronger assumptions than one-wayness, are actually not necessary for PVD.

Indeed, weakenings that we call target-collapsing and generalized-target-collision-resistance, can be obtained from (regular) variants of one-way functions, and do suffice for publicly-verifiable deletion. Analogously to their classical counterparts, we believe that these primitives will be of independent interest. Indeed, a natural question that this work leaves open is whether variants of these primitives that suffice for publicly-verifiable deletion can be based on *one-way functions* without the regularity constraint. It is also interesting to further understand relationships and implications between target-collision-resistance and target-collapsing, including when these properties may or may not imply each other. It may also be useful to understand if these weaker properties can suffice in place of stronger properties such as collapsing and collision-resistance in other contexts, including the design of post-quantum protocols.

Finally, note that we rely on trapdoored variants of these primitives to build public-key encryption schemes. Here too, in addition to obtaining PKE with PVD from any injective trapdoor one-way function (TDF), it becomes possible to relax assumptions to only require (almost)-regularity and trapdoor phase-recoverability – properties that can plausibly be achieved from weaker concrete assumptions than injective TDFs. These are new examples of complexity assumptions that yield public-key encryption with quantum ciphertexts, but may be too weak to obtain PKE with classical ciphertexts. It is an interesting question to further investigate the weakest complexity assumptions that may imply public-key encryption, with or without PVD.

Acknowledgements

D.K. was supported in part by NSF CAREER CNS-2238718, NSF CNS-2247727 and DARPA SIEVE. This material is based upon work supported by the Defense Advanced Research Projects Agency through Award HR00112020024.

A.P. is partially supported by AFOSR YIP (award number FA9550-16-1-0495), the Institute for Quantum Information and Matter (an NSF Physics Frontiers Center; NSF Grant PHY-1733907) and by a grant from the Simons Foundation (828076, TV).

3 Preliminaries

In this section, we review basic concepts from quantum computing and cryptography.

3.1 Quantum Computing

We refer to [NC11, Wil13] for a comprehensive background on quantum computation.

A finite-dimensional complex Hilbert space is denoted by $\mathcal{H}$, and we use subscripts to distinguish between different systems (or registers); for example, we let $\mathcal{H}_{\mathsf{A}}$ be the Hilbert space corresponding to a system A. The tensor product of two Hilbert spaces $\mathcal{H}_{\mathsf{A}}$ and $\mathcal{H}_{\mathsf{B}}$ is another Hilbert space denoted by $\mathcal{H}_{\mathsf{AB}} = \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$. We let $\mathcal{L}(\mathcal{H})$ denote the set of linear operators over $\mathcal{H}$. A quantum system over the 2-dimensional Hilbert space $\mathcal{H} = \mathbb{C}^2$ is called a *qubit*. For $n \in \mathbb{N}$, we refer to quantum registers over the Hilbert space $\mathcal{H} = \left(\mathbb{C}^2\right)^{\otimes n}$ as n-qubit states. We use the word *quantum state* to refer to both pure states (unit vectors $|\psi\rangle \in \mathcal{H}$) and density matrices $\rho \in \mathcal{D}(\mathcal{H})$, where we use the notation $\mathcal{D}(\mathcal{H})$ to refer to the space of positive semidefinite linear operators of unit trace acting on $\mathcal{H}$. Occasionally, we consider *subnormalized states*, i.e. states in the space of positive semidefinite operators over $\mathcal{H}$ with trace norm not exceeding 1.

The *trace distance* of two density matrices $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ is given by

$$\mathsf{TD}(\rho, \sigma) = \frac{1}{2} \operatorname{Tr}\left[\sqrt{(\rho - \sigma)^\dagger (\rho - \sigma)}\right].$$

A quantum channel $\Phi : \mathcal{L}(\mathcal{H}_{\mathsf{A}}) \to \mathcal{L}(\mathcal{H}_{\mathsf{B}})$ is a linear map between linear operators over the Hilbert spaces $\mathcal{H}_{\mathsf{A}}$ and $\mathcal{H}_{\mathsf{B}}$. We say that a channel Φ is *completely positive* if, for a reference system R of arbitrary size, the induced map $I_R \otimes \Phi$ is positive, and we call it *trace-preserving* if $\operatorname{Tr}[\Phi(X)] = \operatorname{Tr}[X]$, for all $X \in \mathcal{L}(\mathcal{H})$. A quantum channel that is both completely positive and trace-preserving is called a quantum CPTP channel.

A polynomial-time *uniform* quantum algorithm (or QPT algorithm) is a polynomial-time family of quantum circuits given by $\mathcal{C} = \{C_\lambda\}_{\lambda \in \mathbb{N}}$, where each circuit $C \in \mathcal{C}$ is described by a sequence of unitary gates and measurements; moreover, for each $\lambda \in \mathbb{N}$, there exists a deterministic polynomial-time Turing machine that, on input 1^λ, outputs a circuit description of C_λ. Similarly, we also define (classical) probabilistic polynomial-time (PPT) algorithms. A quantum algorithm may, in general, receive (mixed) quantum states as inputs and produce (mixed) quantum states as outputs. Occasionally, we restrict QPT algorithms implicitly; for example, if we write $\Pr\left[\mathcal{A}(1^\lambda) = 1\right]$ for a QPT algorithm $\mathcal{A}$, it is implicit that $\mathcal{A}$ is a QPT algorithm that outputs a single classical bit.

Quantum Fourier transform. Let $q \geq 2$ be a modulus and $n \in \mathbb{N}$ and let $\omega_q = e^{\frac{2\pi i}{q}} \in \mathbb{C}$ denote the primitive q-th root of unity. The m-qudit *q-ary quantum Fourier transform* over the ring $\mathbb{Z}_q^m$ is defined by the operation,

$$\mathsf{FT}_q : \quad |\mathbf{x}\rangle \quad \mapsto \quad \sqrt{q^{-m}} \sum_{\mathbf{y} \in \mathbb{Z}_q^m} \omega_q^{\langle \mathbf{x}, \mathbf{y} \rangle} |\mathbf{y}\rangle, \qquad \forall \mathbf{x} \in \mathbb{Z}_q^m.$$

The q-ary quantum Fourier transform is *unitary* and can be efficiently implemented on a quantum computer for any integer modulus $q \geq 2$ [HH00].

Pauli Twirling. We use the following unitary operators:

- Pauli-Z operator:

$$\mathsf{Z}^z = \sum_{x \in \{0,1\}} (-1)^{x \cdot z} |x\rangle\langle x|, \quad \text{for } z \in \{0, 1\}.$$

- Multi-qubit Pauli-Z operator:

$$\mathsf{Z}^z = \mathsf{Z}^{z_1} \otimes \cdots \otimes \mathsf{Z}^{z_m}, \quad \text{for } z \in \{0, 1\}^m.$$

- Controlled-Z operator:

$$\mathsf{CZ}^z = \sum_{c\in\{0,1\}} |c\rangle\langle c| \otimes \mathsf{Z}^{c\cdot z}, \quad \text{for } z \in \{0,1\}^m.$$

Here, we use the notation $\mathsf{Z}^0 = I$ and $\mathsf{Z}^1 = \mathsf{Z}$, as well as $c \cdot z = (c\cdot z_1, \dots, c \cdot z_m)$ for $z \in \{0,1\}^m$.

We use the following well-known property of the Pauli-Z dephasing channel which says that, on average, a random Pauli-Z twirl induces a measurement in the computational basis.

Lemma 3.1 (Pauli-Z Twirl)**.** *The Pauli-*Z *dephasing channel applied to an m-qubit state ρ satsifies*

$$\mathcal{Z}(\rho) \stackrel{\text{def}}{=} 2^{-m} \sum_{z\in\{0,1\}^m} \mathsf{Z}^z \rho\, (\mathsf{Z}^z)^\dagger = \sum_{x\in\{0,1\}^m} \mathrm{Tr}[|x\rangle\langle x|\,\rho]\; |x\rangle\langle x|\,.$$

3.2 Cryptography

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

The Short Integer Solution problem. The (inhomogenous) SIS problem was introduced by Ajtai [Ajt96] in his seminal work on average-case lattice problems. The problem is defined as follows.

Definition 3.2 (Inhomogenous SIS problem,[Ajt96])**.** *Let $n, m \in \mathbb{N}$ be integers, let $q \geq 2$ be a modulus and let $\beta > 0$ be a parameter. The Inhomogenous Short Integer Solution problem* (ISIS) *problem is to find a short solution $\mathbf{x} \in \mathbb{Z}^m$ with $\|\mathbf{x}\| \leq \beta$ such that $\mathbf{A}\cdot\mathbf{x} = \mathbf{y} \pmod q$ given as input a tuple $(\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}, \mathbf{y} \xleftarrow{\$} \mathbb{Z}_q^n)$. The Short Integer Solution* (SIS) *problem is a homogenous variant of the* ISIS *problem with input $(\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}, \mathbf{0} \in \mathbb{Z}_q^n)$.*

Micciancio and Regev [MR07] showed that the SIS problem is, on the average, as hard as approximating worst-case lattice problems to within small factors. Subsequently, Gentry, Peikert and Vaikuntanathan [GPV08] gave an improved reduction showing that, for parameters $m = \mathrm{poly}(n)$, $\beta = \mathrm{poly}(n)$ and prime $q \geq \beta \cdot \omega(\sqrt{n \log q})$, the average-case $\mathsf{SIS}_{n,q,\beta}^m$ problem is as hard as approximating the shortest independent vector problem (SIVP) problem in the worst case to within a factor $\gamma = \beta \cdot \tilde{O}(\sqrt{n})$. We assume that $\mathsf{SIS}_{n,q,\beta}^m$, for $m = \Omega(n \log q)$, $\beta = 2^{o(n)}$ and $q = 2^{o(n)}$, is hard against polynomial-time quantum adversaries.

The Learning with Errors problem. The *Learning with Errors* problem serves as the primary basis of hardness of post-quantum cryptosystems and was introduced by Regev [Reg05]. The problem is defined as follows.

Definition 3.3 (Learning with Errors problem, [Reg05])**.** *Let $n, m \in \mathbb{N}$ be integers, let $q \geq 2$ be a modulus and let $\alpha \in (0,1)$ be a noise ratio parameter. The (decisional) Learning with Errors* ($\mathsf{LWE}_{n,q,\alpha q}^m$) *problem is to distinguish between the following samples*

$$(\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}, \mathbf{s}^\intercal \mathbf{A} + \mathbf{e}^\intercal \pmod q) \quad \textit{and} \quad (\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}, \mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^m),$$

where $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$ is a uniformly random vector and where $\mathbf{e} \sim D_{\mathbb{Z}^m,\sigma}$ is a discrete Gaussian error vector, where $D_{\mathbb{Z}^m,\sigma}$ assigns probability proportional to $\rho_\sigma(\mathbf{x}) = \exp\left(-\pi\|\mathbf{x}\|^2/\sigma^2\right)$ to each $\mathbf{x} \in \mathbb{Z}^m$, for $\sigma = \alpha q > 0$.

We rely on the quantum $\mathsf{LWE}^m_{n,q,\alpha q}$ *assumption which states that the samples above are computationally indistinguishable for any* QPT *algorithm.*

It was shown in [Reg05, PRS17] that the $\mathsf{LWE}^m_{n,q,\alpha q}$ problem with parameter $\alpha q \geq 2\sqrt{n}$ is at least as hard as approximating the shortest independent vector problem (SIVP) to within a factor of $\gamma = \widetilde{O}(n/\alpha)$ in worst case lattices of dimension n. In this work we assume the subexponential hardness of $\mathsf{LWE}^m_{n,q,\alpha q}$ which relies on the worst case hardness of approximating short vector problems in lattices to within a subexponential factor. We assume that $\mathsf{LWE}^m_{n,q,\alpha q}$, for $m = \Omega(n \log q)$, $q = 2^{o(n)}$, $\alpha = 1/2^{o(n)}$, is hard against polynomial-time quantum adversaries.

4 Main Theorem: Certified Everlasting Target-Collapsing

4.1 Definitions

In this section, we present our definitions of target-collapsing and (generalized) target-collision-resistance. We parameterize our definitions by a distribution $\mathcal{D}$ over preimages and a measurement function $\mathcal{M}$. Note that when $\mathcal{M}$ is the identity function, the notion of $(\mathcal{D}, \mathcal{M})$-target-collapsing corresponds to a notion where the entire preimage register is measured in the computational basis. In this case we drop parameterization by $\mathcal{M}$ and just say $\mathcal{D}$-target-collapsing. Also, when $\mathcal{D}$ is the uniform distribution, we drop parameterization by $\mathcal{D}$ and just say $\mathcal{M}$-target-collapsing.

Definition 4.1 (($\mathcal{D}, \mathcal{M}$)-Target-Collapsing Hash Function)**.** *Let $\lambda \in \mathbb{N}$ be the security parameter. A hash function family given by $\mathcal{H} = \{H_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}\}_{\lambda \in \mathbb{N}}$ is $(\mathcal{D}, \mathcal{M})$-target-collapsing for some distribution $\mathcal{D} = \{D_\lambda\}_{\lambda \in \mathbb{N}}$ over $\{\{0,1\}^{m(\lambda)}\}_{\lambda \in \mathbb{N}}$ and family of functions $\mathcal{M} = \{\{M[h] : \{0,1\}^{m(\lambda)} \to \{0,1\}^{k(\lambda)}\}_{h \in H_\lambda}\}_{\lambda \in \mathbb{N}}$ if, for every QPT adversary $\mathcal{A} = \{\mathcal{A}_\lambda\}_{\lambda \in \mathbb{N}}$,*

$$|\Pr\left[\mathsf{TargetCollapseExp}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\lambda}(0) = 1\right] - \Pr\left[\mathsf{TargetCollapseExp}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\lambda}(1) = 1\right]| \leq \mathrm{negl}(\lambda).$$

Here, the experiment $\mathsf{TargetCollapseExp}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\lambda}(b)$ *is defined as follows:*

1. *The challenger prepares the state*
$$\sum_{x \in \{0,1\}^{m(\lambda)}} \sqrt{D_\lambda(x)}\,|x\rangle$$
on register X, and samples a random hash function $h \xleftarrow{\$} H_\lambda$. Then, it coherently computes h on X (into a fresh $n(\lambda)$-qubit register Y) and measures system Y in the computational basis, which results in an outcome $y \in \{0,1\}^{n(\lambda)}$.

2. *If $b = 0$, the challenger does nothing. Else, if $b = 1$, the challenger coherently computes $M[h]$ on X (into a fresh $k(\lambda)$-qubit register V) and measures system V in the computational basis. Finally, the challenger sends the outcome state in system X to $\mathcal{A}_\lambda$, together with the string $y \in \{0,1\}^{n(\lambda)}$ and a description of the hash function h.*

3. *$\mathcal{A}_\lambda$ returns a bit b', which we define as the output of the experiment.*

We also define an analogous notion of $(\mathcal{D}, \mathcal{M})$-target-collision-resistance, as follows. Similarly to above, we drop the parameterization by $\mathcal{M}$ in the case that it is the identity function, and we drop the parameterization by $\mathcal{D}$ in the case that it is the uniform distribution. Notice that target-collision-resistance (without parameterization) then coincides with the classical notion where a uniformly random input is sampled, and the adversary must find a collision with respect to this input (this is also sometimes called second-preimage resistance, or weak collision-resistance).

Definition 4.2 (($\mathcal{D}, \mathcal{M}$)-Target-Collision-Resistant Hash Function)**.** *A hash function family* $\mathcal{H} = \{H_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}\}_{\lambda \in \mathbb{N}}$ *is* $(\mathcal{D}, \mathcal{M})$*-target-collision-resistant for some distribution* $\mathcal{D} = \{D_\lambda\}_{\lambda \in \mathbb{N}}$ *over* $\{\{0,1\}^{m(\lambda)}\}_{\lambda \in \mathbb{N}}$ *and family of functions* $\mathcal{M} = \{\{M[h] : \{0,1\}^{m(\lambda)} \to \{0,1\}^{k(\lambda)}\}_{h \in H_\lambda}\}_{\lambda \in \mathbb{N}}$ *if, for every QPT adversary* $\mathcal{A} = \{\mathcal{A}_\lambda\}_{\lambda \in \mathbb{N}}$*,*

$$|\Pr\big[\mathsf{TargetCollRes}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\lambda} = 1\big]| \leq \mathrm{negl}(\lambda).$$

Here, the experiment $\mathsf{TargetCollRes}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\lambda}$ *is defined as follows:*

1. *The challenger prepares the state*
$$\sum_{x \in \{0,1\}^{m(\lambda)}} \sqrt{D_\lambda(x)}\, |x\rangle$$
on register X, and samples a random hash function $h \xleftarrow{\$} H_\lambda$. Next, it coherently computes h on X (into a fresh $n(\lambda)$-qubit system Y) and measures system Y in the computational basis, which results in an outcome $y \in \{0,1\}^{n(\lambda)}$. Next, it coherently computes $M[h]$ on X (into a fresh $k(\lambda)$-qubit register V) and measures system V in the computational basis, which results in an outcome v. Finally, its sends the outcome state in system X to $\mathcal{A}_\lambda$, together with the string $y \in \{0,1\}^{n(\lambda)}$ and a description of the hash function h.

2. *$\mathcal{A}_\lambda$ responds with a string $x \in \{0,1\}^{m(\lambda)}$.*

3. *The experiment outputs 1 if $h(x) = y$ and $M[h](x) \neq v$.*

Finally, we define the notion of a *certified everlasting* target-collapsing hash.

Definition 4.3. *A hash function family $\mathcal{H} = \{H_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}\}_{\lambda \in \mathbb{N}}$ is certified everlasting $(\mathcal{D}, \mathcal{M})$-target-collapsing for some distribution $\mathcal{D} = \{D_\lambda\}_{\lambda \in \mathbb{N}}$ over $\{\{0,1\}^{m(\lambda)}\}_{\lambda \in \mathbb{N}}$ and family of functions $\mathcal{M} = \{\{M[h] : \{0,1\}^{m(\lambda)} \to \{0,1\}^{k(\lambda)}\}_{h \in H_\lambda}\}_{\lambda \in \mathbb{N}}$ if for every two-part adversary $\mathcal{A} = \{\mathcal{A}_{0,\lambda}, \mathcal{A}_{1,\lambda}\}_{\lambda \in \mathbb{N}}$, where $\{\mathcal{A}_{0,\lambda}\}_{\lambda \in \mathbb{N}}$ is QPT and $\{\mathcal{A}_{1,\lambda}\}_{\lambda \in \mathbb{N}}$ is unbounded, it holds that*

$$|\Pr\left[\mathsf{EvTargetCollapseExp}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\lambda}(0) = 1\right] - \Pr\left[\mathsf{EvTargetCollapseExp}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\lambda}(1) = 1\right]| \leq \mathrm{negl}(\lambda).$$

Here, the experiment $\mathsf{EvTargetCollapseExp}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\lambda}(b)$ *is defined as follows:*

1. *The challenger prepares the state*
$$\sum_{x \in \{0,1\}^{m(\lambda)}} \sqrt{D_\lambda(x)}\, |x\rangle$$
on register X, and samples a random hash function $h \xleftarrow{\$} H_\lambda$. Then, it coherently computes h on X (into a fresh $n(\lambda)$-qubit system Y) and measures system Y in the computational basis, which results in an outcome $y \in \{0,1\}^{n(\lambda)}$.

2. *If $b = 0$, the challenger does nothing. Else, if $b = 1$, the challenger coherently computes $M[h]$ on X (into an auxiliary $k(\lambda)$-qubit system V) and measures system V in the computational basis. Finally, the challenger sends the outcome state in system X to $\mathcal{A}_{0,\lambda}$, together with the string $y \in \{0,1\}^{n(\lambda)}$ and a description of the hash function h.*

3. *$\mathcal{A}_{0,\lambda}$ sends a classical certificate $\pi \in \{0,1\}^{m(\lambda)}$ to the challenger and initializes $\mathcal{A}_{1,\lambda}$ with its residual state.*

4. *The challenger checks if $h(\pi) = y$. If true, $\mathcal{A}_{1,\lambda}$ is run until it outputs a bit b'. Otherwise, $b' \leftarrow \{0,1\}$ is sampled uniformly at random. The output of the experiment is b'.*

4.2 Main Theorem

Our main theorem is the following.

Theorem 4.4. *Let $\mathcal{H} = \{H_\lambda\}_{\lambda \in \mathbb{N}}$ be a hash function family that is both $(\mathcal{D}, \mathcal{M})$-target-collapsing and $(\mathcal{D}, \mathcal{M})$-target-collision-resistant, for some distribution $\mathcal{D}$ and efficiently computable family of functions $\mathcal{M}$. Then, $\mathcal{H}$ is certified everlasting $(\mathcal{D}, \mathcal{M})$-target-collapsing.*

Proof. Throughout the proof, we will leave the security parameter implicit, defining $H \coloneqq H_\lambda, D \coloneqq D_\lambda, m \coloneqq m(\lambda), n \coloneqq n(\lambda)$, $k \coloneqq k(\lambda)$, $\mathcal{A}_0 \coloneqq \mathcal{A}_{0,\lambda}$, and $\mathcal{A}_1 \coloneqq \mathcal{A}_{1,\lambda}$. Next, we define

$$|\psi\rangle_X \coloneqq \sum_{x \in \{0,1\}^m} \sqrt{D(x)}\, |x\rangle \,.$$

For $h \in H, y \in \{0,1\}^m$, we define a unit vector

$$|\psi_{h,y}\rangle_X \propto \sum_{x \in \{0,1\}^m : h(x) = y} \sqrt{D(x)}\, |x\rangle \,.$$

Finally, for $h \in H, y \in \{0,1\}^m, v \in \{0,1\}^k$ we define a unit vector

$$|\psi_{h,y,v}\rangle_X \propto \sum_{x \in \{0,1\}^m : h(x) = y, M[h](x) = v} \sqrt{D(x)}\, |x\rangle \,.$$

We consider the following hybrids.

- $\mathsf{Exp}_0(b)$:
  1. The challenger prepares $|\psi\rangle_X$, samples a random hash function $h \xleftarrow{\$} H_\lambda$, coherently computes h on X into a fresh n-qubit register Y, and measures Y in the computational basis to obtain $y \in \{0,1\}^n$ and a left-over state $|\psi_{h,y}\rangle_X$.
  2. If $b = 0$, the challenger does nothing. Else, if $b = 1$, the challenger computes $M[h]$ on X into a fresh k-qubit register V, and measures V in the computational basis. Finally, the challenger sends the left-over state in system X to $\mathcal{A}_0$, together with the string $y \in \{0,1\}^n$ and a classical description of h.
  3. $\mathcal{A}_0$ sends a classical certificate $\pi \in \{0,1\}^m$ to the challenger and initializes $\mathcal{A}_1$ with its residual state.

4. The challenger checks if $h(\pi) = y$. If true, $\mathcal{A}_1$ is run until it outputs a bit b'. Otherwise, $b' \leftarrow \{0,1\}$ is sampled uniformly at random. The output of the experiment is b'.

- $\mathsf{Exp}_1(b)$:

1. The challenger prepares $|\psi\rangle_X$, samples a random hash function $h \xleftarrow{\$} H_\lambda$, coherently computes h on X into a fresh n-qubit register Y, and measures Y in the computational basis to obtain $y \in \{0,1\}^n$ and a left-over state $|\psi_{h,y}\rangle_X$.
2. The challenger computes $M[h]$ on X into a fresh k-qubit register V to obtain a state

$$\propto \sum_{x \in \{0,1\}^m : h(x)=y} \sqrt{D(x)}\, |x\rangle_X \, |M[h](x)\rangle_V .$$

Then, the challenger samples a random string $z \xleftarrow{\$} \{0,1\}^k$, prepares a $|+\rangle$ state in system C, and applies a controlled-Z^z operation from C to V, which results in a state

$$\begin{aligned} &\propto \sum_{c \in \{0,1\}} |c\rangle_C \otimes \sum_{x \in \{0,1\}^m : h(x)=y} \sqrt{D(x)}\, |x\rangle_X \, \mathsf{Z}^{c \cdot z} \, |M[h](x)\rangle_V \\ &= \sum_{c \in \{0,1\}} |c\rangle_C \otimes \sum_{x \in \{0,1\}^m : h(x)=y} \sqrt{D(x)} (-1)^{c \cdot \langle M[h](x), z\rangle} \, |x\rangle_X \, |M[h](x)\rangle_V . \end{aligned}$$

Finally, the challenger uncomputes the V register by again computing $M[h]$ from X to V, and sends system X to $\mathcal{A}_0$, together with $y \in \{0,1\}^n$ and a classical description of h.
3. $\mathcal{A}_0$ sends a classical certificate $\pi \in \{0,1\}^m$ to the challenger and initializes $\mathcal{A}_1$ with its residual state.
4. The challenger checks if $h(\pi) = y$. Then, the challenger measures system C to obtain $c' \in \{0,1\}$ and checks that $c' = b$. If both checks are true, $\mathcal{A}_1$ is run until it outputs a bit b'. Otherwise, $b' \leftarrow \{0,1\}$ is sampled uniformly at random. The output of the experiment is b'.

- $\mathsf{Exp}_2(b)$:

1. The challenger prepares $|\psi\rangle_X$, samples a random hash function $h \xleftarrow{\$} H_\lambda$, coherently computes h on X into a fresh n-qubit register Y, and measures Y in the computational basis to obtain $y \in \{0,1\}^n$ and a left-over state $|\psi_{h,y}\rangle_X$.
2. The challenger computes $M[h]$ on X into a fresh k-qubit register V. Then, the challenger samples a random string $z \xleftarrow{\$} \{0,1\}^k$, prepares a $|+\rangle$ state in system C, applies a controlled-Z^z operation from C to V, and finally uncomputes the V register by again computing $M[h]$ from X to V. Note that this results in a state

$$\propto \sum_{c \in \{0,1\}} |c\rangle_C \otimes \sum_{x \in \{0,1\}^m : h(x)=y} (-1)^{c \cdot \langle M[h](x), z\rangle} \, |x\rangle_X .$$

Finally, it sends system X to $\mathcal{A}_0$, together with $y \in \{0,1\}^n$ and a classical description of h.

3. $\mathcal{A}_0$ sends a classical certificate $\pi \in \{0,1\}^m$ and initializes $\mathcal{A}_1$ with its residual state.
4. The challenger checks if $h(\pi) = y$. Then, the challenger applies the following projective measurement to system C:

$$\left\{ |\phi_\pi^z\rangle\langle\phi_\pi^z|, I - |\phi_\pi^z\rangle\langle\phi_\pi^z| \right\} \quad \text{where} \quad |\phi_\pi^z\rangle := \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{\langle M[h](\pi), z\rangle} |1\rangle \right),$$

and checks that the first outcome is observed. Finally, the challenger measures system C to obtain $c' \in \{0,1\}$ and checks that $c' = b$. If all three checks are true, $\mathcal{A}_1$ is run until it outputs a bit b'. Otherwise, $b' \leftarrow \{0,1\}$ is sampled uniformly at random. The output of the experiment is b'.

Finally, we also use the following hybrid which is convenient for the sake of the proof.

- $\mathsf{Exp}_3(b)$:

1. The challenger prepares $|\psi\rangle_X$, samples a random hash function $h \xleftarrow{\$} H_\lambda$, coherently computes h on X into a fresh n-qubit register Y, and measures Y in the computational basis to obtain $y \in \{0,1\}^n$ and a left-over state $|\psi_{h,y}\rangle_X$.
2. The challenger computes $M[h]$ on X into a fresh k-qubit register V. Then, the challenger measures V in the computational basis to obtain $v \in \{0,1\}^k$. Next, the challenger samples a random string $z \xleftarrow{\$} \{0,1\}^k$, prepares a $|+\rangle$ state in system C, applies a controlled-Z^z operation from C to V, and finally uncomputes the V register by again computing $M[h]$ from X to V. Note that this results in the state

$$\frac{1}{\sqrt{2}} \left(|0\rangle_C + (-1)^{\langle v,z\rangle} |1\rangle_C \right) \otimes |\psi_{h,y,v}\rangle_X .$$

Finally, the challenger sends system X to $\mathcal{A}_0$, together with $y \in \{0,1\}^n$ and a classical description of h.
3. $\mathcal{A}_0$ sends a classical certificate $\pi \in \{0,1\}^m$ to the challenger and initializes $\mathcal{A}_1$ with its residual state.
4. The challenger checks if $h(\pi) = y$. Then, the challenger applies the following projective measurement to system C:

$$\left\{ |\phi_\pi^z\rangle\langle\phi_\pi^z|, I - |\phi_\pi^z\rangle\langle\phi_\pi^z| \right\} \quad \text{where} \quad |\phi_\pi^z\rangle := \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{\langle M[h](\pi), z\rangle} |1\rangle \right),$$

and checks that the first outcome is observed. Finally, the challenger measures system C to obtain $c' \in \{0,1\}$ and checks that $c' = b$. If all three checks are true, $\mathcal{A}_1$ is run until it outputs a bit b'. Otherwise, $b' \leftarrow \{0,1\}$ is sampled uniformly at random. The output of the experiment is b'.

Before we analyze the probability of distinguishing between the consecutive hybrids, we first show that the following statements hold for the final experiment $\mathsf{Exp}_3(b)$.

Claim 4.5. *The probability that the challenger accepts the deletion certificate π in Step 4 of $\mathsf{Exp}_3(b)$ and $M[h](\pi) \neq v$ is negligible. That is,*

$$\Pr_{h,y,v}\left[h(\pi) = y \;\;\wedge\;\; M[h](\pi) \neq v \;:\; \pi \leftarrow \mathcal{A}_0(h, y, |\psi_{h,y,v}\rangle)\right] \leq \mathrm{negl}(\lambda),$$

where the probability is over the challenger preparing $|\psi\rangle$, sampling h, and measuring y and v as described in $\mathsf{Exp}_3(b)$ to produce the left-over state $|\psi_{h,y,v}\rangle$.

Proof. This follows directly from the assumed $(\mathcal{D}, \mathcal{M})$-target-collision resistance of $\mathcal{H}$, since the above probability is exactly $\Pr\left[\mathsf{TargetCollRes}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\lambda} = 1\right]$. □

Claim 4.6. *The probability that the challenger accepts the deletion certificate π in Step 4 of $\mathsf{Exp}_3(b)$ and the subsequent projective measurement on system C fails (returns the second outcome) is negligible.*

Proof. This follows directly from Claim 4.5, which implies that except with negligible probability, the register C is in the state

$$\frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{\langle v,z\rangle}|1\rangle\right)$$

at the time the challenger applies the projective measurement.

□

For any experiment $\mathsf{Exp}_i(b)$, we define the advantage

$$\mathsf{Adv}(\mathsf{Exp}_i) := |\Pr[\mathsf{Exp}_i(0) = 1] - \Pr[\mathsf{Exp}_i(1) = 1]|.$$

Claim 4.7.

$$\mathsf{Adv}(\mathsf{Exp}_2) = 0.$$

Proof. First note that in the case that the challenger rejects because either the deletion certificate is invalid or their projection fails, the experiment does not involve b, and thus the advantage of the adversary is 0. Second, in the case that the challenger's projection succeeds, the register C is either in the state

$$\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{\langle \pi,z\rangle}|1\rangle) \quad \text{or} \quad \frac{1}{\sqrt{2}}(|0\rangle - (-1)^{\langle \pi,z\rangle}|1\rangle)$$

for some $z \in \{0,1\}^k$, and thereby completely unentangled from the rest of the system. Notice that the challenger's measurement of system C with outcome c' results in a uniformly random bit, which completely masks b. Therefore, the experiment is also independent of b in this case, and thus the adversary's overall advantage in Exp_2 is 0. □

Next, we argue the following.

Claim 4.8.

$$|\mathsf{Adv}(\mathsf{Exp}_2) - \mathsf{Adv}(\mathsf{Exp}_1)| \leq \mathrm{negl}(\lambda).$$

Proof. Recall that Claim 4.6 shows that the projective measurement performed by the challenger in Step 4 of Exp_3 succeeds with overwhelming probability. We now argue that the same is also true in Exp_2. Suppose for the sake of contradiction that there is a non-negligible difference between the success probabilities of the measurement. We now show that this implies the existence of an efficient distinguisher $\mathcal{A}'$ that breaks the $(\mathcal{D}, \mathcal{M})$-target-collapsing property of the hash family $\mathcal{H} = \{H_\lambda\}_{\lambda \in \mathbb{N}}$.

$\mathcal{A}'$ receives (y, h) and a state on register X from its challenger. Next, it computes $M[h]$ on X into a fresh k-qubit register V, samples a random string $z \xleftarrow{\$} \{0,1\}^k$, prepares a $|+\rangle$ state in system C, applies a controlled-Z^z operation from C to V, and then uncomputes register V by again applying $M[h]$ from X to V. Then, it runs $\mathcal{A}$ on (y, h, X), which outputs a certificate π.

Finally, $\mathcal{A}'$ applies the following projective measurement to system C:

$$\left\{ |\phi_\pi^z\rangle\langle\phi_\pi^z|, I - |\phi_\pi^z\rangle\langle\phi_\pi^z| \right\} \quad \text{where} \quad |\phi_\pi^z\rangle := \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{\langle \pi, z \rangle} |1\rangle \right),$$

and outputs 1 if the measurement succeeds and 0 otherwise. If there is a non-negligible difference in success probabilities of this measurement between $\mathsf{Exp}_3(b)$ and $\mathsf{Exp}_2(b)$ (for any $b \in \{0,1\}$), then $\mathcal{A}'$ breaks $(\mathcal{D}, \mathcal{M})$-target-collapsing of $\mathcal{H}$.

Now, recall that $\mathsf{Exp}_2(b)$ is identical to $\mathsf{Exp}_1(b)$, except that the challenger applies an additional a measurement in Step 4. Because the measurement succeeds with overwhelming probability, it follows from Gentle Measurement that the advantage of the adversary must remain the same up to a negligible amount. This proves the claim. □

Claim 4.9.

$$\mathsf{Adv}(\mathsf{Exp}_1) = \mathsf{Adv}(\mathsf{Exp}_0)/2.$$

Proof. First note that in $\mathsf{Exp}_1(b)$, we can imagine measuring register C to obtain c' and aborting if $c' \neq b$ before the challenger sends any information to the adversary. This follows because register C is disjoint from the adversary's registers. Next, by Lemma 3.1, we have the following guarantees about the state on system X given to the adversary in $\mathsf{Exp}_1(b)$.

- In the case $c' = b = 0$, the reduced state on register X is $|\psi_{h,y}\rangle$.
- In the case that $c' = b = 1$, the reduced state on register X is a mixture over $|\psi_{h,y,v}\rangle$ where v is the result of measuring register V in the computational basis.

Thus, this experiment is identical to $\mathsf{Exp}_0(b)$, except that we decide to abort and output a uniformly random bit b' with probability 1/2 at the beginning of the experiment.

□

Putting everything together, we have that $\mathsf{Adv}(\mathsf{Exp}_0) \leq \mathrm{negl}(\lambda)$, which completes the proof.

□

4.3 Auxiliary Information

Next, we generalize the above theorem statement to handle hash functions that are sampled with some auxiliary information. That is, there is an algorithm $(h, \mathsf{aux}) \leftarrow \mathsf{Samp}(1^\lambda)$ that samples the description of a hash function h along with some auxiliary information aux. We will want to allow the adversary to potentially see information about aux (but not necessarily all of it), so we define a family $\mathcal{Z} = \{Z_\lambda(\mathsf{aux})\}_{\lambda \in \mathbb{N}}$ that specifies what information the adversary sees about aux. In the most straightforward case, $\mathcal{Z}$ could be some distribution over classical or quantum states, parameterized by aux. However, we also consider an *interactive* $Z_\lambda(\mathsf{aux})$. That is, Z_λ is the description of an interactive machine that is initialized with aux and interacts with the adversary $\mathcal{A}_\lambda$.

Definition 4.10. *A hash function family* $\mathcal{H} = \{H_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}\}_{\lambda\in\mathbb{N}}$ *with an associated sampling algorithm* Samp *is* $(\mathcal{D},\mathcal{M},\mathcal{Z})$*-target-collapsing for some distribution* $\mathcal{D} = \{D_\lambda\}_{\lambda\in\mathbb{N}}$ *over* $\{\{0,1\}^{m(\lambda)}\}_{\lambda\in\mathbb{N}}$*, family of functions* $\mathcal{M} = \{\{M[h] : \{0,1\}^{m(\lambda)} \to \{0,1\}^{k(\lambda)}\}_{h\in H_\lambda}\}_{\lambda\in\mathbb{N}}$*, and family of (static or interactive) distributions* $\mathcal{Z} = \{Z_\lambda(\mathsf{aux})\}_{(\cdot,\mathsf{aux})\in\mathsf{Samp}(1^\lambda),\lambda\in\mathbb{N}}$ *if, for every QPT adversary* $\mathcal{A} = \{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$*,*

$$|\Pr\left[\mathsf{TargetCollapseExp}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\mathcal{Z},\lambda}(0) = 1\right] - \Pr\left[\mathsf{TargetCollapseExp}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\mathcal{Z},\lambda}(1) = 1\right]| \le \mathrm{negl}(\lambda),$$

where the experiment $\mathsf{TargetCollapseExp}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\mathcal{Z},\lambda}(b)$ *is defined as in Definition 4.1 except that* h *is sampled by* $(h,\mathsf{aux}) \leftarrow \mathsf{Samp}(1^\lambda)$*, and the adversary is given (or interacts with)* $Z_\lambda(\mathsf{aux})$ *along with* (X, y, h)*.*

Definition 4.11. *A hash function family* $\mathcal{H} = \{H_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}\}_{\lambda\in\mathbb{N}}$ *with an associated sampling algorithm* Samp *is* $(\mathcal{D},\mathcal{M},\mathcal{Z})$*-target-collision-resistant for some distribution* $\mathcal{D} = \{D_\lambda\}_{\lambda\in\mathbb{N}}$ *over* $\{\{0,1\}^{m(\lambda)}\}_{\lambda\in\mathbb{N}}$*, family of functions* $\mathcal{M} = \{\{M[h] : \{0,1\}^{m(\lambda)} \to \{0,1\}^{k(\lambda)}\}_{h\in H_\lambda}\}_{\lambda\in\mathbb{N}}$*, and family of (static or interactive) distributions* $\mathcal{Z} = \{Z_\lambda(\mathsf{aux})\}_{(\cdot,\mathsf{aux})\in\mathsf{Samp}(1^\lambda),\lambda\in\mathbb{N}}$ *if, for every QPT adversary* $\mathcal{A} = \{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$*,*

$$\Pr\left[\mathsf{TargetCollRes}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\mathcal{Z},\lambda}(0) = 1\right] \le \mathrm{negl}(\lambda),$$

where the experiment $\mathsf{TargetCollRes}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\mathcal{Z},\lambda}(b)$ *is defined as in Definition 4.2 except that* h *is sampled by* $(h,\mathsf{aux}) \leftarrow \mathsf{Samp}(1^\lambda)$*, and the adversary is given (or interacts with)* $Z_\lambda(\mathsf{aux})$ *along with* (X, y, h)*.*

Definition 4.12. *A hash function family* $\mathcal{H} = \{H_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}\}_{\lambda\in\mathbb{N}}$ *with an associated sampling algorithm* Samp *is certified everlasting* $(\mathcal{D},\mathcal{M},\mathcal{Z})$*-target-collapsing for some distribution* $\mathcal{D} = \{D_\lambda\}_{\lambda\in\mathbb{N}}$ *over* $\{\{0,1\}^{m(\lambda)}\}_{\lambda\in\mathbb{N}}$*, family of functions* $\mathcal{M} = \{\{M[h] : \{0,1\}^{m(\lambda)} \to \{0,1\}^{k(\lambda)}\}_{h\in H_\lambda}\}_{\lambda\in\mathbb{N}}$*, and family of (static or interactive) distributions* $\mathcal{Z} = \{Z_\lambda(\mathsf{aux})\}_{(\cdot,\mathsf{aux})\in\mathsf{Samp}(1^\lambda),\lambda\in\mathbb{N}}$ *if, for every two-part adversary* $\mathcal{A} = \{\mathcal{A}_{0,\lambda}, \mathcal{A}_{1,\lambda}\}_{\lambda\in\mathbb{N}}$*, where* $\{\mathcal{A}_{0,\lambda}\}_{\lambda\in\mathbb{N}}$ *is QPT and* $\{\mathcal{A}_{1,\lambda}\}_{\lambda\in\mathbb{N}}$ *is unbounded, it holds that*

$$|\Pr\left[\mathsf{EvTargetCollapseExp}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\mathcal{Z},\lambda}(0) = 1\right] - \Pr\left[\mathsf{EvTargetCollapseExp}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\mathcal{Z},\lambda}(1) = 1\right]| \le \mathrm{negl}(\lambda),$$

where the experiment $\mathsf{EvTargetCollapseExp}_{\mathcal{H},\mathcal{A},\mathcal{D},\mathcal{M},\mathcal{Z},\lambda}(b)$ *is defined as in Definition 4.2 except that* h *is sampled by* $(h,\mathsf{aux}) \leftarrow \mathsf{Samp}(1^\lambda)$*, and the first part of the adversary* $\mathcal{A}_{0,\lambda}$ *is given (or interacts with)* $Z_\lambda(\mathsf{aux})$ *along with* (X, y, h)*.*

Now, the following generalization of Theorem 4.4 follows immediately from the proof of Theorem 4.4, by additionally giving $Z_\lambda(\mathsf{aux})$ to the adversary in each of the experiments.

Theorem 4.13. *Let* $\mathcal{H} = \{H_\lambda\}_{\lambda\in\mathbb{N}}$ *be a hash function family that is both* $(\mathcal{D},\mathcal{M},\mathcal{Z})$*-target-collapsing and* $(\mathcal{D},\mathcal{M},\mathcal{Z})$*-target-collision-resistant, for some distribution* $\mathcal{D}$*, efficiently computable family of functions* $\mathcal{M}$*, and (static or interactive) distribution* $\mathcal{Z}$*. Then,* $\mathcal{H}$ *is certified everlasting* $(\mathcal{D},\mathcal{M},\mathcal{Z})$*-target-collapsing.*

4.4 Target-Collision-Resistance implies Target-Collapsing for Polynomial-Outcome Measurements

In this section, we show that recent techniques from the collapsing hash function / collapsing commitment literature [DS22, Zha22, CX22] imply that when $\mathcal{M}$ is a function with polynomial number of outcomes, then $(\mathcal{D},\mathcal{M},\mathcal{Z})$-target-collision-resistance implies $(\mathcal{D},\mathcal{M},\mathcal{Z})$-target-collapsing. In this paper, we will only need to use this claim for *two-outcome* measurements, but we show it for the more general case of polynomial-outcome measurements.

Lemma 4.14. *Let $\mathcal{H} = \{H_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}\}_{\lambda\in\mathbb{N}}$ be a hash function family that is $(\mathcal{D},\mathcal{M},\mathcal{Z})$-target-collision-resistant for some distribution $\mathcal{D} = \{D_\lambda\}_{\lambda\in\mathbb{N}}$ over $\{\{0,1\}^{m(\lambda)}\}_{\lambda\in\mathbb{N}}$, family of functions $\mathcal{M} = \{\{M[h] : \{0,1\}^{m(\lambda)} \to \{0,1\}^{k(\lambda)}\}_{h\in H_\lambda}\}_{\lambda\in\mathbb{N}}$ for $k(\lambda) = O(\log\lambda)$, and family of (static or interactive) distributions $\mathcal{Z} = \{Z_\lambda(\mathsf{aux})\}_{(\cdot,\mathsf{aux})\in\mathsf{Samp}(1^\lambda),\lambda\in\mathbb{N}}$. Then, $\mathcal{H}$ is $(\mathcal{D},\mathcal{M},\mathcal{Z})$-target-collapsing.*

Proof. We will make use of the following fact [DS22, Claim 3.5].

Fact 4.15. *Let D be a projector, $\{\Pi_i\}_{i\in[N]}$ be pairwise orthogonal projectors, and $|\psi\rangle$ be any state such that $|\psi\rangle \in \mathsf{im}(\sum_{i\in[N]}\Pi_i)$. Then,*

$$\sum_{i\in[N]} \left\| \left(\sum_{j\neq i}\Pi_j\right) D\Pi_i |\psi\rangle \right\|^2 \geq \frac{1}{N}\left(\|D|\psi\rangle\|^2 - \left(\sum_{i\in[N]}\|D\Pi_i|\psi\rangle\|^2\right)\right)^2.$$

Now, suppose there exists an adversary $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$ that breaks the $(\mathcal{D},\mathcal{M},\mathcal{Z})$-target-collapsing of $\mathcal{H}$. Dropping parameterization by λ for convenience, we can write such an adversary as a binary outcome projective measurement $(D, I-D)$ applied to a state received from the challenger. For any $h \in H_\lambda, y \in \{0,1\}^n$, let $|\psi_{h,y}\rangle$ be the normalized state such that

$$|\psi_{h,y}\rangle \propto |h,y\rangle \otimes \sum_{x\in\{0,1\}^m : h(x)=y} \sqrt{D(x)}\,|x\rangle,$$

and for $i \in \{0,1\}^k$, let

$$\Pi_{i,h} := \sum_{x\in\{0,1\}^m : M[h](x)=i} |x\rangle\langle x|.$$

Then, the adversary's advantage in the $(\mathcal{D},\mathcal{M},\mathcal{Z})$-target-collapsing game can be written as

$$\mathop{\mathbb{E}}_{h,y}\left[\|D|\psi_{h,y}\rangle\|^2 - \sum_{i\in\{0,1\}^k}\|D\Pi_{i,h}|\psi_{h,y}\rangle\|^2\right] = \mathsf{non\text{-}negl}(\lambda),$$

where the expectation is over the sampling of $h \leftarrow H_\lambda$ and the challenger's measurement of y.

Thus, by Fact 4.15, it follows that

$$\mathop{\mathbb{E}}_{h,y}\left[\sum_{i\in\{0,1\}^k}\left\|\left(\sum_{j\neq i}\Pi_{j,h}\right) D\Pi_{i,h}|\psi_{h,y}\rangle\right\|^2\right] = \mathsf{non\text{-}negl}(\lambda),$$

since $2^k = 2^{O(\log\lambda)} = \mathrm{poly}(\lambda)$. This completes the proof, as this expression exactly corresponds to the adversary's probability of winning the $(\mathcal{D},\mathcal{M},\mathcal{Z})$-target-collision-resistance game by applying D and then measuring in the computational basis.

□

5 Publicly-Verifiable Deletion from Dual-Regev Encryption

In this section, we recall the constructions of Dual-Regev public-key encryption as well as fully homomorphic encryption with publicly-verifiable deletion introduced by Poremba [Por23]. Using our main result on certified-everlasting target-collapsing hashes in Theorem 4.4, we prove the *strong Gaussian-collapsing conjecture* in [Por23], and then conclude that the aforementioned constructions achieve certified-everlasting security assuming the quantum hardness of LWE and SIS.

First, let us recall the definition of public-key encryption with publicly-verifiable deletion.

5.1 Definition: Encryption with Publicly-Verifiable Deletion

A public-key encryption (PKE) scheme with publicly-verifiable deletion (PVD) has the following syntax.

- $\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$: the key generation algorithm takes as input the security parameter λ and outputs a public key pk and secret key sk.
- $\mathsf{Enc}(\mathsf{pk}, m) \to (\mathsf{vk}, |\mathsf{CT}\rangle)$: the encryption algorithm takes as input the public key pk and a plaintext m, and outputs a (public) verification key vk and a ciphertext $|\mathsf{CT}\rangle$.
- $\mathsf{Dec}(\mathsf{sk}, |\mathsf{CT}\rangle) \to m$: the decryption algorithm takes as input the secret key sk and a ciphertext $|\mathsf{CT}\rangle$ and outputs a plaintext m.
- $\mathsf{Del}(|\mathsf{CT}\rangle) \to \pi$: the deletion algorithm takes as input a ciphertext $|\mathsf{CT}\rangle$ and outputs a deletion certificate π.
- $\mathsf{Vrfy}(\mathsf{vk}, \pi) \to \{\top, \bot\}$: the verify algorithm takes as input a (public) verification key vk and a proof π, and outputs $\top$ or $\bot$.

Definition 5.1 (Correctness of deletion)**.** *A PKE scheme with PVD satisfies* correctness of deletion *if for any m, it holds with $1 - \mathrm{negl}(\lambda)$ probability over $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda), (\mathsf{vk}, |\mathsf{CT}\rangle) \leftarrow \mathsf{Enc}(\mathsf{pk}, m), \pi \leftarrow \mathsf{Del}(|\mathsf{CT}\rangle), \mu \leftarrow \mathsf{Vrfy}(\mathsf{vk}, \pi)$ that $\mu = \top$.*

Definition 5.2 (Certified deletion security)**.** *A PKE scheme with PVD satisfies* certified deletion security *if it satisfies standard semantic security, and moreover, for any QPT adversary $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$, it holds that*

$$\mathsf{TD}\left(\mathsf{EvPKE}_{\mathcal{A},\lambda}(0), \mathsf{EvPKE}_{\mathcal{A},\lambda}(1)\right) = \mathrm{negl}(\lambda),$$

where the experiment $\mathsf{EvPKE}_{\mathcal{A},\lambda}(b)$ is defined as follows.

- *Sample $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$ and $(\mathsf{vk}, |\mathsf{CT}\rangle) \leftarrow \mathsf{Enc}(\mathsf{pk}, b)$.*
- *Run $\mathcal{A}_\lambda(\mathsf{pk}, \mathsf{vk}, |\mathsf{CT}\rangle)$, and parse their output as a deletion certificate π and a left-over quantum state ρ.*
- *If $\mathsf{Vrfy}(\mathsf{vk}, \pi) = \top$, output ρ, and otherwise output $\bot$.*

Before we introduce the Dual-Regev public-key schemes proposed by Poremba [Por23], let us first recall some basic facts about Gaussian superpositions.

5.2 Gaussian Superpositions

Let $m \in \mathbb{N}$. The *Gaussian measure* ρ_σ with parameter $\sigma > 0$ is defined as

$$\rho_\sigma(\mathbf{x}) = \exp\left(-\pi\|\mathbf{x}\|^2/\sigma^2\right), \qquad \forall \mathbf{x} \in \mathbb{R}^m.$$

Given a modulus $q \in \mathbb{N}$ and $\sigma \in (\sqrt{2m}, q/\sqrt{2m})$, the *truncated* discrete Gaussian distribution $D_{\mathbb{Z}_q^m,\sigma}$ over the finite set $\mathbb{Z}^m \cap (-\frac{q}{2}, \frac{q}{2}]^m$ with support $\{\mathbf{x} \in \mathbb{Z}_q^m : \|\mathbf{x}\| \leq \sigma\sqrt{m}\}$ is defined as

$$D_{\mathbb{Z}_q^m,\sigma}(\mathbf{x}) = \frac{\rho_\sigma(\mathbf{x})}{\sum\limits_{\mathbf{z}\in\mathbb{Z}_q^m, \|\mathbf{z}\|\leq\sigma\sqrt{m}} \rho_\sigma(\mathbf{z})}.$$

In this section, we consider Gaussian superposition states over $\mathbb{Z}^m \cap (-\frac{q}{2}, \frac{q}{2}]^m$ of the form

$$|\psi\rangle = \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \rho_\sigma(\mathbf{x})\,|\mathbf{x}\rangle\,.$$

The state $|\psi\rangle$ is not normalized for convenience. A standard tail bound [Ban93, Lemma 1.5 (ii)] implies that (the normalized variant of) $|\psi\rangle$ is within negligible trace distance of a *truncated* discrete Gaussian superposition $|\tilde{\psi}\rangle$ with support $\{\mathbf{x} \in \mathbb{Z}_q^m : \|\mathbf{x}\| \leq \sigma\sqrt{\frac{m}{2}}\}$, where

$$|\tilde{\psi}\rangle = \left(\sum_{\mathbf{z}\in\mathbb{Z}_q^m, \|\mathbf{z}\|\leq\sigma\sqrt{\frac{m}{2}}} \rho_{\frac{\sigma}{\sqrt{2}}}(\mathbf{z})\right)^{-\frac{1}{2}} \sum_{\mathbf{x}\in\mathbb{Z}_q^m : \|\mathbf{x}\|\leq\sigma\sqrt{\frac{m}{2}}} \rho_\sigma(\mathbf{x})\,|\mathbf{x}\rangle\,.$$

Note that a measurement of $|\tilde{\psi}\rangle$ results in a sample from the truncated discrete Gaussian distribution $D_{\mathbb{Z}_q^m,\frac{\sigma}{\sqrt{2}}}$. We remark that Gaussian superpositions with parameter $\sigma = \Omega(\sqrt{m})$ can be efficiently implemented using standard quantum state preparation techniques; for example using *quantum rejection sampling* and the *Grover-Rudolph algorithm* [GR02, Reg05, Bra18, BCM+21].

Let $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$. We use the following algorithm, denoted by $\mathsf{GenGauss}(\mathbf{A}, \sigma)$ which prepares a partially measured Gaussian superposition of pre-images of a randomly generated image.

1. Prepare a Gaussian superposition in system X with parameter $\sigma > 0$:
$$|\psi\rangle = \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \rho_\sigma(\mathbf{x})\,|\mathbf{x}\rangle \otimes |\mathbf{0}\rangle\,.$$
2. Apply the unitary $U_\mathbf{A} : |\mathbf{x}\rangle\,|\mathbf{0}\rangle \rightarrow |\mathbf{x}\rangle\,|\mathbf{A}\cdot\mathbf{x} \pmod q\rangle$, which results in the state
$$|\psi\rangle = \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \rho_\sigma(\mathbf{x})\,|\mathbf{x}\rangle \otimes |\mathbf{A}\cdot\mathbf{x} \pmod q\rangle\,.$$
3. Measure the second register in the computational basis, which results in $\mathbf{y} \in \mathbb{Z}_q^n$ and a state
$$|\psi_\mathbf{y}\rangle = \sum_{\substack{\mathbf{x}\in\mathbb{Z}_q^m:\\ \mathbf{A}\mathbf{x}=\mathbf{y} \pmod q}} \rho_\sigma(\mathbf{x})\,|\mathbf{x}\rangle\,.$$

Finally, we use the following lemma which characterizes the Fourier transform of a partially measured Gaussian superposition.

Lemma 5.3 ([Por23], Lemma 16). *Let $m \in \mathbb{N}$, $q \geq 2$ be a prime and $\sigma \in (\sqrt{8m}, q/\sqrt{8m})$. Let $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ be a matrix whose columns generate $\mathbb{Z}_q^n$ and let $\mathbf{y} \in \mathbb{Z}_q^n$ be arbitrary. Then, the q-ary quantum Fourier transform of the (normalized variant of the) Gaussian coset state*

$$|\psi_{\mathbf{y}}\rangle = \sum_{\substack{\mathbf{x}\in\mathbb{Z}_q^m \\ \mathbf{A}\mathbf{x}=\mathbf{y} \pmod q}} \rho_\sigma(\mathbf{x})\,|\mathbf{x}\rangle$$

is within negligible (in $m \in \mathbb{N}$) trace distance of the (normalized variant of the) Gaussian state

$$|\hat{\psi}_{\mathbf{y}}\rangle = \sum_{\mathbf{s}\in\mathbb{Z}_q^n} \sum_{\mathbf{e}\in\mathbb{Z}_q^m} \rho_{q/\sigma}(\mathbf{e})\,\omega_q^{-\langle\mathbf{s},\mathbf{y}\rangle}\,|\mathbf{s}^\intercal\mathbf{A} + \mathbf{e}^\intercal \pmod q\rangle\,.$$

5.3 (Strong) Gaussian-Collapsing Property.

We use the following result which says that the Ajtai hash function is target-collapsing with respect to the truncated discrete Gaussian distribution.

Theorem 5.4 (Gaussian-collapsing property, [Por23], Theorem 4). *Let $n \in \mathbb{N}$ and q be a prime with $m \geq 2n\log q$, each parameterized by $\lambda \in \mathbb{N}$. Let $\sigma \in (\sqrt{8m}, q/\sqrt{8m})$. Then, the following samples are computationallyindistinguishable assuming the quantum hardness of decisional $\mathsf{LWE}^m_{n,q,\alpha q}$, for any noise ratio $\alpha \in (0,1)$ with relative noise magnitude $1/\alpha = \sigma\cdot 2^{o(n)}$:*

$$\left(\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m},\ |\psi_{\mathbf{y}}\rangle = \sum_{\substack{\mathbf{x}\in\mathbb{Z}_q^m \\ \mathbf{A}\mathbf{x}=\mathbf{y}}} \rho_\sigma(\mathbf{x})\ |\mathbf{x}\rangle\,,\ \mathbf{y}\in\mathbb{Z}_q^n\right) \approx_c \left(\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m},\ |\mathbf{x}_0\rangle\,,\ \mathbf{A}\cdot\mathbf{x}_0\ \in \mathbb{Z}_q^n\right)$$

where $(|\psi_{\mathbf{y}}\rangle, \mathbf{y}) \leftarrow \mathsf{GenGauss}(\mathbf{A},\sigma)$ and where $\mathbf{x}_0 \sim D_{\mathbb{Z}_q^m,\frac{\sigma}{\sqrt{2}}}$ is a discrete Gaussian error.

Using our main theorem on certified-everlasting target-collapsing hashes in Theorem 4.4, we can now prove a stronger variant of Theorem 5.4. We show the following:

Theorem 5.5. *Let $\lambda \in \mathbb{N}$ be the security parameter, $n(\lambda) \in \mathbb{N}$, $q(\lambda) \in \mathbb{N}$ be a modulus, $m \geq 2n\log q$ and $\sigma \in (\sqrt{2m}, q/\sqrt{2m})$. Then, the Ajtai hash function family $\mathcal{H} = \{H_\lambda\}_{\lambda\in\mathbb{N}}$ with*

$$H_\lambda = \left\{h_{\mathbf{A}} : \{\mathbf{x}\in\mathbb{Z}_q^m : \|\mathbf{x}\| \leq \sigma\sqrt{m/2}\} \to \mathbb{Z}_q^n \text{ s.t. } h_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\cdot\mathbf{x} \pmod q;\ \mathbf{A}\in\mathbb{Z}_q^{n\times m}\right\}.$$

is certified everlasting $D_{\mathbb{Z}_q^m,\frac{\sigma}{\sqrt{2}}}$-target-collapsing assuming the quantum hardness of $\mathsf{SIS}^m_{n,q,\sigma\sqrt{2m}}$ and $\mathsf{LWE}^m_{n,q,\alpha q}$, for any noise ratio $\alpha \in (0,1)$ with relative noise magnitude $1/\alpha = \sigma\cdot 2^{o(n)}$.

Proof. By the Gaussian-collapsing property in Theorem 5.4, it follows that $\mathcal{H}$ is $D_{\mathbb{Z}_q^m,\frac{\sigma}{\sqrt{2}}}$-target-collapsing assuming the quantum hardness of $\mathsf{LWE}^m_{n,q,\alpha q}$, for any noise ratio $\alpha \in (0,1)$ with relative noise magnitude $1/\alpha = \sigma\cdot 2^{o(n)}$. Moreover, from the quantum hardness of $\mathsf{SIS}^m_{n,q,\sigma\sqrt{2m}}$ it follows that $\mathcal{H}$ is $D_{\mathbb{Z}_q^m,\frac{\sigma}{\sqrt{2}}}$-target-collision-resistant. Therefore, the claim follows from Theorem 4.4. $\square$

As a corollary, we immediately recover the so-called strong Gaussian-collapsing property of the Ajtai hash function which was previously stated as a conjecture by Poremba [Por23].

Corollary 5.6 (Strong Gaussian-collapsing property).
Let $\lambda \in \mathbb{N}$ be the security parameter, $n(\lambda) \in \mathbb{N}$, $q(\lambda) \in \mathbb{N}$ be a modulus and $m > 2n \log q$. Let $\sigma = \Omega(\sqrt{m})$ be a parameter. Then, the Ajtai hash function satisfies the strong Gaussian-collapsing property assuming the quantum hardness of $\mathsf{SIS}^m_{n,q,\sigma\sqrt{2m}}$ and $\mathsf{LWE}^m_{n,q,\alpha q}$, for any noise ratio $\alpha \in (0,1)$ with relative noise magnitude $1/\alpha = \sigma \cdot 2^{o(n)}$. In other words, for every QPT adversary $\mathcal{A}$,

$$|\Pr\left[\mathsf{StrongGaussCollapseExp}_{\mathcal{A},n,m,q,\sigma}(0) = 1\right] - \Pr\left[\mathsf{StrongGaussCollapseExp}_{\mathcal{A},n,m,q,\sigma}(1) = 1\right] \leq \mathrm{negl}(\lambda)$$

where $\mathsf{StrongGaussCollapseExp}_{\mathcal{A},n,m,q,\sigma}(b)$ is the experiment from Figure 1.

Proof. To prove the statement, we can simply reduce the certified everlasting $D_{\mathbb{Z}_q^m,\frac{\sigma}{\sqrt{2}}}$-target-collapsing security of the Ajtai hash $\mathbf{A} = [\bar{\mathbf{A}} \,\|\, \bar{\mathbf{A}} \cdot \bar{\mathbf{x}} \pmod q] \in \mathbb{Z}_q^{n\times m}$ with $\bar{\mathbf{x}} \xleftarrow{\$} \{0,1\}^{m-1}$ to the strong Gaussian-collapsing security, and invoke Theorem 5.5. Here we rely on the fact that the distribution of $\mathbf{A}$ is statistically close to uniform by the leftover hash lemma whenever $m > 2n \log q$. Now consider the unbounded reduction that given $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, samples a uniformly random vector $\mathbf{t} = (\mathbf{x}, -1) \in \mathbb{Z}^m$ with $\mathbf{x} \in \{0,1\}^{m-1}$ such that $\bar{\mathbf{A}}\mathbf{x} = \bar{\mathbf{A}}\bar{\mathbf{x}} \pmod q$, and then runs the second part of the strong Gaussian-collapsing adversary on input $\mathbf{t}$ in order to predict the challenger's bit. Note that such vectors $\mathbf{t}$ exist because of how the matrix $\mathbf{A}$ is constructed in the experiment. If the strong Gaussian-collapsing adversary has noticeable advantage, then so does the reduction, which would break the certified everlasting $D_{\mathbb{Z}_q^m,\frac{\sigma}{\sqrt{2}}}$-target-collapsing security of the Ajtai hash. □

5.4 Dual-Regev Public-Key Encryption with Publicly-Verifiable Deletion

We now consider the following Dual-Regev encryption scheme introduced by Poremba [Por23].

Construction 1 (Dual-Regev PKE with Publicly-Verifiable Deletion). *Let $n \in \mathbb{N}$ be the security parameter, $m \in \mathbb{N}$ and q be a prime. Let $\alpha \in (0,1)$ and $\sigma = 1/\alpha$ be parameters. The Dual-Regev PKE scheme $\mathsf{DualPKECD} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Del}, \mathsf{Vrfy})$ with certified deletion is defined as follows:*

$\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$: *sample a random matrix $\bar{\mathbf{A}} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ and a vector $\bar{\mathbf{x}} \xleftarrow{\$} \{0,1\}^m$ and choose $\mathbf{A} = [\bar{\mathbf{A}} \| \bar{\mathbf{A}} \cdot \bar{\mathbf{x}} \pmod q]$. Output $(\mathsf{pk}, \mathsf{sk})$, where $\mathsf{pk} = \mathbf{A} \in \mathbb{Z}_q^{n\times(m+1)}$ and $\mathsf{sk} = (-\bar{\mathbf{x}}, 1) \in \mathbb{Z}_q^{m+1}$.*

$\mathsf{Enc}(\mathsf{pk}, b) \to (\mathsf{vk}, |\mathsf{CT}\rangle)$: *parse the public key as $\mathbf{A} \leftarrow \mathsf{pk}$. To encrypt a single bit $b \in \{0,1\}$, generate the following pair for a random $\mathbf{y} \in \mathbb{Z}_q^n$:*

$$\mathsf{vk} \leftarrow (\mathbf{A}, \mathbf{y}), \quad |\mathsf{CT}\rangle \leftarrow \sum_{\mathbf{s}\in\mathbb{Z}_q^n} \sum_{\mathbf{e}\in\mathbb{Z}_q^{m+1}} \rho_{q/\sigma}(\mathbf{e})\, \omega_q^{-\langle \mathbf{s},\mathbf{y}\rangle} \, |\mathbf{s}^\intercal \mathbf{A} + \mathbf{e}^\intercal + b \cdot (0, \dots, 0, \lfloor \frac{q}{2} \rfloor)\rangle \,,$$

where vk is the public verification key and $|\mathsf{CT}\rangle$ is an $(m+1)$-qudit quantum ciphertext.

$\mathsf{Dec}(\mathsf{sk}, |\mathsf{CT}\rangle) \to \{0,1\}$: *to decrypt, measure $|\mathsf{CT}\rangle$ in the computational basis with outcome $\mathbf{c} \in \mathbb{Z}_q^m$. Compute $\mathbf{c}^\intercal \cdot \mathsf{sk} \in \mathbb{Z}_q$ and output 0, if it is closer to 0 than to $\lfloor \frac{q}{2} \rfloor$, and output 1, otherwise.*

$\mathsf{Del}(|\mathsf{CT}\rangle) \to \pi$: *Measure $|\mathsf{CT}\rangle$ in the Fourier basis and output the measurement outcome $\pi \in \mathbb{Z}_q^{m+1}$.*

$\mathsf{Vrfy}(\mathsf{vk}, \pi) \to \{\top, \bot\}$: *to verify a deletion certificate* $\pi \in \mathbb{Z}_q^{m+1}$, *parse* $(\mathbf{A}, \mathbf{y}) \leftarrow \mathsf{vk}$ *and output* $\top$, *if* $\mathbf{A} \cdot \pi = \mathbf{y} \pmod q$ *and* $\|\pi\| \leq \sqrt{m+1}/\sqrt{2}\alpha$, *and output* $\bot$, *otherwise.*

Let us now illustrate how the deletion procedure takes place. Recall from Lemma 5.3 that the Fourier transform of the ciphertext $|\mathsf{CT}\rangle$ results in the *dual* quantum state

$$|\widehat{\mathsf{CT}}\rangle = \sum_{\substack{\mathbf{x} \in \mathbb{Z}_q^{m+1}: \\ \mathbf{A}\mathbf{x} = \mathbf{y} \pmod q}} \rho_\sigma(\mathbf{x})\, \omega_q^{\langle \mathbf{x}, b \cdot (0,\dots,0,\lfloor \frac{q}{2} \rfloor) \rangle} \, |\mathbf{x}\rangle \,. \tag{4}$$

In other words, a Fourier basis measurement of $|\mathsf{CT}\rangle$ necessarily erases all information about the plaintext $b \in \{0,1\}$ and results in a *short* vector $\pi \in \mathbb{Z}_q^{m+1}$ such that $\mathbf{A} \cdot \pi = \mathbf{y} \pmod q$. Hence, to publicly verify a deletion certificate we can simply check whether it is a solution to the ISIS problem specified by the verification key $\mathsf{vk} = (\mathbf{A}, \mathbf{y})$. Using Theorem 5.5, we obtain the following:

Theorem 5.7. *Let* $n \in \mathbb{N}$ *and let* $q \geq 2$ *be a prime modulus such that* $q = 2^{o(n)}$ *and* $m \geq 2n \log q$. *Let* $\sigma \in (\sqrt{8m}, q/\sqrt{8m})$ *and* $\alpha \in (0,1)$ *be a noise ratio with* $1/\alpha = 2^{o(n)} \cdot \sigma$. *Then, the Dual-Regev public-key encryption scheme in Construction 1 has everlasting certified deletion security assuming the quantum (subexponential) hardness of* $\mathsf{LWE}_{n,q,\alpha q}^m$ *and* $\mathsf{SIS}_{n,q,\sigma\sqrt{2m}}^m$.

Proof. The proof is identical to the template used in [Por23, Theorem 7], except that the adversary is allowed to be computationally unbounded once the deletion certificate is submitted. This is in contrast with the original proof who considered forwarding the *secret key* during the security experiment. We remark that we do not invoke the strong Gaussian-collapsing property to prove the indistinguishability of the hybrids; instead we use the (stronger) notion of certified everlasting $D_{\mathbb{Z}_q^m, \frac{\sigma}{\sqrt{2}}}$-target-collapsing property of the Ajtai hash shown in Theorem 5.5. This results in the stronger notion of everlasting certified deletion security. $\square$

5.5 Dual-Regev (Leveled) Fully Homomorphic Encryption with Publicly-Verifiable Deletion

A homomorphic encryption scheme with certified deletion [BI20, Por23, BBK22] is a scheme that supports both homomorphic operations as well as certified deletion of quantum ciphertexts. Here, the two properties are thought of as *separate* features that may or may not be mutually exclusive. Several works [Por23, BBK22, BGG⁺23] have also considered the possibility of realizing both homomorphic evaluation and certified deletion *simultaneously* within a single (possibly interactive) protocol. For example, Poremba [Por23] proposed a four-message protocol that allows a client to learn the outcome of a homomorphic evaluation performed by an untrusted quantum server, while simultaneously certifying that the server has subsequently deleted all data. Bartusek and Khurana [BBK22] subsequently defined the notion of a four-message protocol for *blind delegation with certified deletion*, which can be instantiated using any FHE scheme with certified deletion. Crucially, both of the aforementioned four-message protocols require that the server is *honest* during the evaluation phase of the protocol. Finally, in a subsequent follow-up work, Bartusek et al. [BGG⁺23] constructed a *maliciously* secure bind delegation protocol with certified deletion which relied on succinct non-interactive arguments (SNARGs) for polynomial-time computation.

In this section, we recall the Dual-Regev (leveled) fully homomorphic encryption scheme with publicly-verifiable deletion introduced by Poremba [Por23]. The scheme is based on the *dual variant* of of the (leveled) FHE scheme by Gentry, Sahai and Waters [GSW13, Mah18]. Using our main result on certified-everlasting target-collapsing hashes in Theorem 4.4, we then prove the scheme achieves certified-everlasting security assuming the quantum hardness of LWE and SIS. Contrary to related works [Por23, BBK22, BGG+23], we only consider the basic notion of FHE with publicly-verifiable deletion which treats both properties as separate features.

Parameters. Let $\lambda \in \mathbb{N}$ be the security parameter and let $n \in \mathbb{N}$. Let L be an upper bound on the depth of the polynomial-sized Boolean circuit which is to be evaluated. We choose the following set of parameters for the Dual-Regev leveled FHE scheme (each parameterized by λ).

- a prime modulus $q \geq 2$.
- an integer $m \geq 2n \log q$.
- an integer $N = (m+1) \cdot \lceil \log q \rceil$.
- a noise ratio $\alpha \in (0,1)$ such that

$$\sqrt{8(m+1)} \leq \alpha q \leq \frac{q}{\sqrt{8}(m+1) \cdot (N+1)^L}.$$

Construction 2 (Dual-Regev leveled FHE scheme with certified deletion)**.** *Let $\lambda \in \mathbb{N}$ be the security parameter. The Dual-Regev (leveled)* FHE *scheme* $\mathsf{DualFHECD} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}, \mathsf{Del}, \mathsf{Vrfy})$ *with certified deletion consists of the following algorithms.*

$\mathsf{KeyGen}(1^\lambda, 1^L) \to (\mathsf{pk}, \mathsf{sk})$: *sample* $\bar{\mathbf{A}} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$ *and vector* $\bar{\mathbf{x}} \xleftarrow{\$} \{0,1\}^m$ *and let* $\mathbf{A} = [\bar{\mathbf{A}} \| \bar{\mathbf{A}} \cdot \bar{\mathbf{x}} \pmod q]^\intercal$. *Output* $(\mathsf{pk}, \mathsf{sk})$, *where* $\mathsf{pk} = \mathbf{A} \in \mathbb{Z}_q^{(m+1) \times n}$ *and* $\mathsf{sk} = (-\bar{\mathbf{x}}, 1) \in \mathbb{Z}_q^{m+1}$.

$\mathsf{Enc}(\mathsf{pk}, x) \to (\mathsf{vk}, |\mathsf{CT}\rangle)$: *to encrypt a bit* $x \in \{0,1\}$, *parse the public key as* $\mathbf{A} \in \mathbb{Z}_q^{(m+1)\times n} \leftarrow \mathsf{pk}$ *and generate the following pair consisting of a verification key and ciphertext for a random* $\mathbf{Y} \in \mathbb{Z}_q^{n \times N}$ *with columns* $\mathbf{y}_1, \ldots, \mathbf{y}_N \in \mathbb{Z}_q^n$:

$$\mathsf{vk} \leftarrow (\mathbf{A}, \mathbf{Y}), \qquad |\mathsf{CT}\rangle \leftarrow \sum_{\mathbf{S} \in \mathbb{Z}_q^{n \times N}} \sum_{\mathbf{E} \in \mathbb{Z}_q^{(m+1) \times N}} \rho_{q/\sigma}(\mathbf{E})\, \omega_q^{-\operatorname{Tr}[\mathbf{S}^\intercal \mathbf{Y}]} \, |\mathbf{A} \cdot \mathbf{S} + \mathbf{E} + x \cdot \mathbf{G}\rangle \,,$$

where $\mathbf{G} = [\mathbf{I} \,\|\, 2\mathbf{I} \,\|\, \ldots \,\|\, 2^{\lceil \log q \rceil - 1}\mathbf{I}] \in \mathbb{Z}_q^{(m+1) \times N}$ *denotes the* gadget matrix *and where* $\sigma = 1/\alpha$.

$\mathsf{Eval}(\mathsf{C}_0, \mathsf{C}_1) \to \mathsf{C}_0\mathsf{C}_1\mathsf{C}$: *to apply a* NAND *gate onto two registers* C_0 *and* C_1 *(possibly part of a larger ciphertext), append an ancilla system* $|\mathbf{0}\rangle_\mathsf{C}$, *and apply the unitary* U_{NAND}, *defined by*

$$U_{\mathsf{NAND}} : \quad |\mathbf{X}\rangle_{\mathsf{C}_0} \otimes |\mathbf{Y}\rangle_{\mathsf{C}_1} \otimes |\mathbf{Z}\rangle_{\mathsf{C}} \quad \to \quad |\mathbf{X}\rangle_{\mathsf{C}_0} \otimes |\mathbf{Y}\rangle_{\mathsf{C}_1} \otimes |\mathbf{Z} + \mathbf{G} - \mathbf{X} \cdot \mathbf{G}^{-1}(\mathbf{Y}) \pmod q\rangle_{\mathsf{C}} \,,$$

where $\mathbf{X}, \mathbf{Y}, \mathbf{Z} \in \mathbb{Z}_q^{(m+1)\times N}$ *and* $\mathbf{G}^{-1}$ *is the (non-linear) inverse operation such that* $\mathbf{G} \circ \mathbf{G}^{-1} = \mathbf{I}$. *Output the resulting registers* $\mathsf{C}_0\mathsf{C}_1\mathsf{C}$.

$\mathsf{Dec}(\mathsf{sk}, \mathsf{C}) \to \{0,1\}$ **or** $\perp$: *measure the register* C *in the computational basis to obtain* $\mathbf{C} \in \mathbb{Z}_q^{(m+1)\times N}$ *and compute* $c = \mathsf{sk}^\intercal \cdot \mathbf{c}_N \in \mathbb{Z} \cap (-\frac{q}{2}, \frac{q}{2}]$, *where* $\mathbf{c}_N \in \mathbb{Z}_q^{m+1}$ *is the* N*-th column of* $\mathbf{C}$; *output* 0, *if* c *is closer to* 0 *than to* $\lfloor \frac{q}{2} \rfloor$, *and output* 1, *otherwise.*

$\mathsf{Del}(|\mathsf{CT}\rangle) \to \pi$: *measure* $|\mathsf{CT}\rangle$ *in the Fourier basis with outcomes* $\pi = (\pi_1 | \ldots | \pi_N) \in \mathbb{Z}_q^{(m+1)\times N}$.

$\mathsf{Vrfy}(\mathsf{vk}, \mathsf{pk}, \pi) \to \{0,1\}$: *to verify the deletion certificate* $\pi = (\pi_1\| \dots \|\pi_N) \in \mathbb{Z}_q^{(m+1)\times N}$*, parse* $(\mathbf{A} \in \mathbb{Z}_q^{(m+1)\times n}, (\mathbf{y}_1\| \dots \|\mathbf{y}_N) \in \mathbb{Z}_q^{n\times N}) \leftarrow \mathsf{vk}$ *and output* $\top$*, if both* $\mathbf{A}^\intercal \cdot \pi_i = \mathbf{y}_i \pmod q$ *and* $\|\pi_i\| \leq \sqrt{m+1}/\sqrt{2}\alpha$ *for every* $i \in [N]$*, and output* $\bot$*, otherwise.*

For additional details on the correctness of the scheme, we refer to Section 9 of [Por23].

Theorem 5.8. *Let* $\lambda \in \mathbb{N}$ *be the security parameter and let* L *be an upper bound on the size of the Boolean circuit which is to be evaluated. Let* $n \in \mathbb{N}$*, let* $q \geq 2$ *be a prime modulus and let* $m \geq 2n \log q$*. Let* $N = (m+1) \cdot \lceil \log q \rceil$*. Let* $\alpha \in (0,1)$ *be a noise ratio such that*

$$\sqrt{8(m+1)N} \leq \alpha q \leq \frac{q}{\sqrt{8}(m+1) \cdot (N+1)^L}.$$

Then, $\mathsf{DualFHECD}$ *in Construction 2 has everlasting certified deletion security assuming the quantum (subexponential) hardness of* $\mathsf{SIS}^m_{n,q,\sigma\sqrt{2m}}$ *and* $\mathsf{LWE}^m_{n,q,\alpha q}$*.*

Proof. The proof is identical to the template in [Por23, Theorem 10], except that the adversary is allowed to be computationally unbounded once the deletion certificate is submitted. This is in contrast with the original proof who considered forwarding the *secret key* during the security experiment. We remark that we do not invoke the strong Gaussian-collapsing property to prove the indistinguishability of the hybrids; instead we use the (stronger) notion of certified everlasting $D_{\mathbb{Z}_q^m, \frac{\sigma}{\sqrt{2}}}$-target-collapsing property of the Ajtai hash function shown in Theorem 5.5. This results in the stronger notion of everlasting certified deletion security. □

6 Publicly-Verifiable Deletion from Balanced Binary-Measurement TCR

In this section, we show how to build a variety of cryptographic primitives with PVD from a specific type of hash function that we call *balanced binary-measurement target-collision-resistant*.

Definition 6.1 (Balanced Binary-Measurement TCR Hash)**.** *A hash function family* $\mathcal{H} = \{H_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}\}_{\lambda\in\mathbb{N}}$ *is* balanced binary-measurement target-collision-resistant *if:*

1. *There exists a family of efficiently computable* single-output-bit *measurement functions* $\mathcal{M} = \{\{M[h] : \{0,1\}^{m(\lambda)} \to \{0,1\}\}_{h\in H_\lambda}\}_{\lambda\in\mathbb{N}}$ *such that* $\mathcal{H}$ *is* $\mathcal{M}$*-target-collision-resistant (Definition 4.2).*

2. *There exists a constant* $\delta > 0$ *such that*[12]

$$\Pr_{h\leftarrow H_\lambda, x\leftarrow\{0,1\}^{m(\lambda)}}\left[\left|\frac{A_{h,x,0} - A_{h,x,1}}{A_{h,x,0} + A_{h,x,1}}\right| \leq 1-\delta\right] = 1 - \mathrm{negl}(\lambda),$$

where $A_{h,x,b} := |\{x' \in h^{-1}(h(x)) : M[h](x') = b\}|$*.*

Remark 6.2. *By Lemma 4.14 and Theorem 4.4, any balanced binary-measurement TCR* $\mathcal{H}$ *with associated measurement function* $\mathcal{M}$ *is also* $\mathcal{M}$*-target-collapsing and certified everlasting* $\mathcal{M}$*-target-collapsing.*

[12]It is also straightforward to generalize our results to any $\delta(\lambda) = 1/\mathrm{poly}(\lambda)$.

6.1 Commitments

A *canonical quantum bit commitment* [Yan22] consists of a family of pairs of unitaries $\{(Q_{\lambda,0}, Q_{\lambda,1})\}_{\lambda\in\mathbb{N}}$. To commit to a bit b, the committer applies $Q_{\lambda,b}$ to the all-zeros state $|0\rangle$ to obtain a state on registers C and R, and sends register C to the receiver. To open, the committer sends the bit b and the remaining state on register R. The receiver applies $Q^\dagger_{\lambda,b}$ to registers (C, R), measures the result in the standard basis, and accepts if all zeros are observed.

Definition 6.3 (Computational Hiding)**.** *A canonical quantum bit commitment $\{(Q_{\lambda,0}, Q_{\lambda,1})\}_{\lambda\in\mathbb{N}}$ satisfies* computational hiding *if for any QPT adversary $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$,*

$$|\Pr[\mathcal{A}_\lambda(\mathrm{Tr}_R(Q_{\lambda,0}|0\rangle)) = 1] - \Pr[\mathcal{A}_\lambda(\mathrm{Tr}_R(Q_{\lambda,1}|0\rangle)) = 1]| = \mathrm{negl}(\lambda).$$

Definition 6.4 (Honest Binding)**.** *A canonical quantum bit commitment $\{(Q_{\lambda,0}, Q_{\lambda,1})\}_{\lambda\in\mathbb{N}}$ satisfies* honest binding *if for any auxiliary family of states $\{|\psi_\lambda\rangle\}_{\lambda\in\mathbb{N}}$ on register Z and any family of physically realizable unitaries $\{U_\lambda\}_{\lambda\in\mathbb{N}}$ on registers R, Z,*

$$\left\| \left(Q_{\lambda,1} |0\rangle\!\langle 0| \, Q^\dagger_{\lambda,1} \right) U \left(Q_{\lambda,0} |0\rangle \, |\psi\rangle \right) \right\| = \mathrm{negl}(\lambda).$$

Definition 6.5 (Publicly-Verifiable Deletion)**.** *A canonical quantum bit commitment $\{(Q_{\lambda,0}, Q_{\lambda,1})\}_{\lambda\in\mathbb{N}}$ has* publicly-verifiable deletion *if there exists a measurement $\{V_\lambda\}_{\lambda\in\mathbb{N}}$ on register R, a measurement $\{D_\lambda\}_{\lambda\in\mathbb{N}}$ on register C, and a classical predicate $\mathsf{Ver}(\cdot,\cdot) \to \{\top, \bot\}$ that satisfy the following properties.*

- ***Correctness of deletion.*** *For any $b \in \{0, 1\}$, it holds that*

$$\Pr[\mathsf{Ver}(\mathsf{vk}, \pi) = \top : (\mathsf{vk}, \pi) \leftarrow (V_\lambda \otimes D_\lambda) Q_{\lambda,b} |0\rangle] = 1 - \mathrm{negl}(\lambda).$$

- ***Certified everlasting hiding.*** *For any QPT adversary $\mathcal{A} = \{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$, it holds that*

$$\mathsf{TD}\left(\mathsf{EvExp}_{\mathcal{A}}(\lambda, 0), \mathsf{EvExp}_{\mathcal{A}}(\lambda, 1)\right) = \mathrm{negl}(\lambda),$$

  where $\mathsf{EvExp}_{\mathcal{A}}(\lambda, b)$ is the following experiment.

  - *Prepare $Q_{\lambda,b}|0\rangle$, measure register R with V_λ to obtain vk, and send (vk, C) to $\mathcal{A}_\lambda$.*
  - *Parse $\mathcal{A}_\lambda$'s output as a deletion certificate π and a left-over state ρ. If $\mathsf{Ver}(\mathsf{vk}, \pi) = \bot$, output $\bot$, and otherwise output ρ.*

Construction. We construct a quantum canonical bit commitment with PVD as follows. Let $\mathcal{H} = \{H_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}\}_{\lambda\in\mathbb{N}}$ be a balanced binary-measurement TCR hash with associated measurement function $\mathcal{M} = \{\{M[h]\}_{h\in H_\lambda}\}_{\lambda\in\mathbb{N}}$, and let $m = m(\lambda)$, $n = n(\lambda)$. For any $h \in H_\lambda, y \in \{0,1\}^n$, and $b \in \{0,1\}$, we will define the state

$$|\psi_{h,y,b}\rangle := \frac{1}{\sqrt{|h^{-1}(y)|}} \sum_{x:h(x)=y} (-1)^{M[h](x)} |x\rangle.$$

- Consider the following procedure $S_{\lambda,b}$. Sample $h \leftarrow H_\lambda$ and for $i \in [\lambda]$, prepare the state

$$\frac{1}{\sqrt{2^m}} \sum_{x \in \{0,1\}^m} (-1)^{b \cdot M[h](x)} |x\rangle |h(x)\rangle ,$$

and measure the second register to obtain y_i and left-over state $|\psi_{h,y_i,b}\rangle$. Then, output

$$(h, y_1, \dots, y_\lambda), \bigotimes_{i \in [\lambda]} |\psi_{h,y_i,b}\rangle .$$

Now, $Q_{\lambda,b}$ will be the purification of $S_{\lambda,b}$, where the output register is C and the auxiliary register is R. That is, $Q_{\lambda,b}$ prepares the state

$$\frac{1}{\sqrt{|H_\lambda| 2^{\lambda m}}} \sum_{h, x_1, \dots, x_\lambda} (-1)^{b \cdot \bigoplus_{i \in [\lambda]} M[h](x_i)} |h, h(x_1), \dots, h(x_\lambda)\rangle_R |h, h(x_1), \dots, h(x_\lambda), x_1, \dots, x_\lambda\rangle_C .$$

- V_λ measures register R in the standard basis to obtain $\mathsf{vk} = (h, y_1, \dots, y_\lambda)$. D_λ measures register C in the standard basis to obtain $(h, y_1, \dots, y_\lambda, x_1, \dots, x_\lambda)$, and outputs $\pi = (x_1, \dots, x_\lambda)$.

- $\mathsf{Ver}((h, y_1, \dots, y_\lambda), (x_1, \dots, x_\lambda))$ outputs $\top$ iff $h(x_i) = y_i$ for all $i \in [\lambda]$.

Theorem 6.6. *The above construction satisfies computational hiding, honest binding, and publicly-verifiable deletion. Thus, assuming the existence of a balanced binary-measurement TCR hash, there exists a quantum canonical bit commitment with* PVD.

Proof. First we argue computational hiding. On a commitment to b, the receiver sees the mixed state

$$\mathop{\mathbb{E}}_{h, y_1, \dots, y_\lambda} \left[\bigotimes_{i \in [\lambda]} |\psi_{h,y_i,b}\rangle \right] ,$$

where the expectation is over sampling $h \leftarrow \mathcal{H}$ and measuring random $y_1, \dots, y_\lambda$. Note the following two facts.

1. Given any state $|\psi_{h,y,b}\rangle$, let $M[h]\left(|\psi_{h,y,b}\rangle\right)$ be the mixed state that results from measuring the bit $M[h](\cdot)$ on $|\psi_{h,y,b}\rangle$. By the $\mathcal{M}$-target-collapsing of $\mathcal{H}$, we have that for any $b \in \{0,1\}$,

$$\mathop{\mathbb{E}}_{h,y} \left[|\psi_{h,y,b}\rangle \right] \approx_c \mathop{\mathbb{E}}_{h,y} \left[M[h]\left(|\psi_{h,y,b}\rangle\right) \right] ,$$

where $\approx_c$ denotes computational indistinguishability. The case of $b = 0$ follows directly by definition of $\mathcal{M}$-target-collapsing and the case of $b = 1$ follows because a reduction can efficently map $|\psi_{h,y,0}\rangle$ to $|\psi_{h,y,1}\rangle$ using the fact that $M[h]$ is efficiently computable.

2. For any h, y, $M[h]\left(|\psi_{h,y,0}\rangle\right)$ and $M[h]\left(|\psi_{h,y,1}\rangle\right)$ are equivalent states, which follows by definition.

Thus, we can run the following hybrid argument.

- Hyb_0: The receiver is given a commitment to 0.
- $\mathsf{Hyb}_1 \dots \mathsf{Hyb}_\lambda$: In Hyb_i, we switch $|\psi_{h,y,0}\rangle$ to $M[h]\left(|\psi_{h,y,0}\rangle\right)$. This is computationally indistinguishable from Hyb_{i-1} by the first fact above.
- $\mathsf{Hyb}_{\lambda+1}$: Switch $M[h]\left(|\psi_{h,y_i,0}\rangle\right)$ to $M[h]\left(|\psi_{h,y_i,1}\rangle\right)$ for all $i \in [\lambda]$. This is perfectly indistinguishable from Hyb_λ by the second fact above.
- $\mathsf{Hyb}_{\lambda+2} \dots \mathsf{Hyb}_{2\lambda+1}$: In $\mathsf{Hyb}_{i+\lambda+1}$, we switch $M[h]\left(|\psi_{h,y_i,1}\rangle\right)$ to $|\psi_{h,y_i,1}\rangle$. This is computationally indistinguishable from $\mathsf{Hyb}_{i+\lambda}$ by the first fact above.

This completes the proof of computational hiding. Next, since $\mathcal{H}$ satisfies *certified everlasting* $\mathcal{M}$-target-collapsing, we see that each hybrid is *statistically close* when the receiver outputs a valid deletion certificate. Thus, the same proof establishes publicly-verifiable deletion.

Finally, we show honest binding. For this, it suffices to demonstrate a measurement on register C that accepts with probability 1 on the output of $Q_{\lambda,0}$ and with probability $\mathrm{negl}(\lambda)$ on the output of $Q_{\lambda,1}$. This suffices because any U that breaks honest binding must then necessarily affect the result of this measurement by a non-$\mathsf{negl}(\lambda)$ amount, which is impossible since U does not operate on C.

The measurement takes the classical part of the output $(h, y_1, \dots, y_\lambda)$ and attempts to project the quantum part onto

$$|\psi_{h,y_1,0}\rangle\langle\psi_{h,y_1,0}| \otimes \cdots \otimes |\psi_{h,y_\lambda,0}\rangle\langle\psi_{h,y_\lambda,0}| \,.$$

Clearly this accepts the output of $S_{\lambda,0}$ with probability 1, so it suffices to show that the output of $S_{\lambda,1}$ is accepted with probability $\mathrm{negl}(\lambda)$. To see this, we bound

$$\begin{aligned}
&\mathop{\mathbb{E}}_{h,y_1,\dots,y_\lambda}\left[\prod_{i\in[\lambda]} |\langle\psi_{h,y_i,1}|\psi_{h,y_i,0}\rangle|^2\right] \\
&\mathop{\mathbb{E}}_{h,y_1,\dots,y_\lambda}\left[\prod_{i\in[\lambda]} \left(\frac{1}{|h^{-1}(y_i)|}\left(\sum_{x:h(x)=y_i}(-1)^{M[h]}\langle x|\right)\left(\sum_{x:h(x)=y_i}|x\rangle\right)\right)^2\right] \\
&= \mathop{\mathbb{E}}_{h,y_1,\dots,y_\lambda}\left[\prod_{i\in[\lambda]}\left(\frac{1}{|h^{-1}(y_i)|}\left(|\{x : h(x)=y_i, M[h](x)=0\}| - |\{x : h(x)=y_i, M[h](x)=1\}|\right)\right)^2\right] \\
&\leq (1-\delta)^{2\lambda} + \mathrm{negl}(\lambda) \\
&= \mathrm{negl}(\lambda),
\end{aligned}$$

where the inequality follows from property (2) of Definition 6.1.

□

6.2 Public-Key Encryption

Definition 6.7 (Trapdoor Phase-Recoverability)**.** *We say that a balanced binary-measurement TCR hash has* trapdoor phase-recoverability *if there exist algorithms* Samp, Recover *with the following properties.*

- $\mathsf{Samp}(1^\lambda)$: *The sampling algorithm samples a uniformly random function* $h \in H_\lambda$ *along with a trapdoor* td.

- $\mathsf{Recover}(\mathsf{td}, y, X)$: *There exist constants* c, ϵ *such that with probability* $1 - \mathrm{negl}(\lambda)$ *over* $(h, \mathsf{td}) \leftarrow \mathsf{Samp}(1^\lambda)$,

$$\Pr_{x \leftarrow \{0,1\}^m} \left[\mathsf{Recover}(\mathsf{td}, h(x), |\psi_{h,h(x),0}\rangle) \to 0\right] \geq c + \epsilon,$$
$$\Pr_{x \leftarrow \{0,1\}^m} \left[\mathsf{Recover}(\mathsf{td}, h(x), |\psi_{h,h(x),1}\rangle) \to 0\right] \leq c - \epsilon,$$

where

$$|\psi_{h,y,b}\rangle \coloneqq \frac{1}{\sqrt{|h^{-1}(y)|}} \sum_{x:h(x)=y} (-1)^{M[h](x)} |x\rangle .$$

Theorem 6.8. *Assuming the existence of a binary-measurement TCR hash* $\mathcal{H}$ *with trapdoor phase-recoverability, there exists public-key encryption with* PVD.

Proof. This follows from essentially the same construction as commitments. Let $\mathcal{M}$ be the measurement function associated with $\mathcal{H}$ and let $(\mathsf{Samp}, \mathsf{Invert})$ be the associated trapdoor algorithms. Then, the PKE with PVD is defined as follows.

- $\mathsf{Gen}(1^\lambda)$: Sample $(h, \mathsf{td}) \leftarrow \mathsf{Samp}(1^\lambda)$ and set $\mathsf{pk} \coloneqq h, \mathsf{sk} \coloneqq \mathsf{td}$.

- $\mathsf{Enc}(\mathsf{pk}, b)$: For $i \in [\lambda]$, prepare the state

$$\frac{1}{\sqrt{2^m}} \sum_{x \in \{0,1\}^m} (-1)^{b \cdot M[h](x)} |x\rangle |h(x)\rangle ,$$

and measure the second register to obtain y_i and left-over state $|\psi_{h,y_i,b}\rangle$. Then, set

$$|\mathsf{CT}\rangle \coloneqq \left(y_1, \dots, y_\lambda, \bigotimes_{i \in [\lambda]} |\psi_{h,y_i,b}\rangle \right), \quad \mathsf{vk} \coloneqq (h, y_1, \dots, y_\lambda).$$

- $\mathsf{Dec}(\mathsf{sk}, |\mathsf{CT}\rangle)$: Parse $|\mathsf{CT}\rangle$ as $(y_1, \dots, y_\lambda, X_1, \dots, X_\lambda)$, for $i \in [\lambda]$ run

$$b_i \leftarrow \mathsf{Recover}(\mathsf{td}, y_i, X_i),$$

and output 0 if $|\{i : b_i = 0\}|/\lambda > c$, and output 1 otherwise.

- $\mathsf{Del}(|\mathsf{CT}\rangle)$: Parse $|\mathsf{CT}\rangle$ as $(y_1, \dots, y_\lambda, X_1, \dots, X_\lambda)$ and measure X_i in the standard basis to obtain $\pi \coloneqq (x_1, \dots, x_\lambda)$.

- $\mathsf{Vrfy}(\mathsf{vk}, \pi)$: Output $\top$ iff $h(x_i) = y_i$ for all $i \in [\lambda]$.

Correctness follows from a standard Hoeffding inequality and correctness of deletion (Definition 5.1) is immediate. Certified deletion security (Definition 5.2) follows from the $\mathcal{M}$-target-collapsing and certified everlasting $\mathcal{M}$-target-collapsing of $\mathcal{H}$, using the same hybrid argument as in the proof of Theorem 6.6. $\square$

6.3 A Generic Compiler

Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Del}, \mathsf{Vrfy})$ be the encryption scheme defined last section, let $\mathcal{A} = \{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$ be an adversary, let $p(\lambda)$ be a polynomial, and let $\mathcal{Z} = \{Z_\lambda(\mathsf{aux})\}_{\mathsf{aux}\in\{0,1\}^{p(\lambda)},\lambda\in\mathbb{N}}$ be a (static or interactive) family of distributions that is semantically-secure against $\mathcal{A}$ with respect to aux. That is, in the static case, it holds that for any $\mathsf{aux} \in \{0,1\}^{p(\lambda)}$,

$$\left|\Pr\left[\mathcal{A}_\lambda(Z_\lambda(\mathsf{aux})) = 1\right] - \Pr\left[\mathcal{A}_\lambda(Z_\lambda(0^{p(\lambda)})) = 1\right]\right| \le \mathrm{negl}(\lambda),$$

and in the interactive case,

$$\left|\Pr\left[\mathcal{A}_\lambda^{Z_\lambda(\mathsf{aux})} = 1\right] - \Pr\left[\mathcal{A}_\lambda^{Z_\lambda(0^{p(\lambda)})} = 1\right]\right| \le \mathrm{negl}(\lambda),$$

where $\mathcal{A}_\lambda^{Z_\lambda(\mathsf{aux})}$ indicates that $\mathcal{A}_\lambda$ can interact with $Z_\lambda(\mathsf{aux})$, which is the description of an interactive machine initialized with aux.

Lemma 6.9. *Given any $\mathcal{A}, \mathcal{Z}$ as described above, define the experiment $\mathsf{EvEnc}_{\mathcal{A},\mathcal{Z},\lambda}(b)$ as follows.*

- *Sample $(h, \mathsf{td}) \leftarrow \mathsf{Gen}(1^\lambda)$ and $(|\mathsf{CT}\rangle, \mathsf{vk}) \leftarrow \mathsf{Enc}(h, b)$.*
- *Run $\mathcal{A}_\lambda(h, \mathsf{vk}, |\mathsf{CT}\rangle, Z_\lambda(\mathsf{td}))$, and parse their output as a deletion certificate π and a left-over quantum state ρ.*
- *If $\mathsf{Vrfy}(\mathsf{vk}, \pi) = \top$, output ρ, and otherwise output $\bot$.*

Then it holds that

$$\mathsf{TD}\left(\mathsf{EvEnc}_{\mathcal{A},\mathcal{Z},\lambda}(0), \mathsf{EvEnc}_{\mathcal{A},\mathcal{Z},\lambda}(1)\right) = \mathrm{negl}(\lambda).$$

Proof. First, we confirm that $\mathcal{H}$ is $(\mathcal{M}, \mathcal{Z})$-target-collision-resistant. To see this, we first use the semantic security of $\mathcal{Z}$ to switch to a hybrid where $\mathcal{A}_\lambda$ receives $Z_\lambda(0)$ rather than $Z_\lambda(\mathsf{td})$, and then appeal directly to the fact that $\mathcal{H}$ is $\mathcal{M}$-target-collision-resistant (Theorem 6.16). Then by Lemma 4.14 and Theorem 4.4, we have that $\mathcal{H}$ is certified everlasting $(\mathcal{M}, \mathcal{Z})$-target-collapsing. Using the same hybrid argument as in the proof of Theorem 6.6 then completes the proof. □

By instantiating $\mathcal{Z}$ with various crytographic primitives, we immediately gives the following applications. We do not write formal definitions of each of these primitives, and instead refer the reader to [BK22] for these.

Corollary 6.10. *Assuming the existence of a balanced binary-measurement TCR hash with trapdoor phase-recoverability, and post-quantum*

$$X \in \left\{ \begin{array}{r} \textit{quantum fully-homormophic encryption, attribute-based encryption,} \\ \textit{witness encryption, timed-release encryption} \end{array} \right\},$$

there exists X with PVD.

The implications to witness encryption and timed-release encryption follow immediately by encrypting td with the appropriate encryption scheme (and in the case of timed-release encryption, considering the class of parallel-time-bounded adversaries). We briefly remark on the other two implications.

- **Fully-homomorphic encryption.** If we encrypt td using a *quantum* fully-homomorphic encryption (QFHE) scheme, then we obtain (Q)FHE with publicly-verifiable deletion. The reason we need QFHE for the compiler is for evaluation correctness: we need to decrypt $|\mathsf{CT}\rangle$ homomorphically under the QFHE (using td) in order to obtain a (Q)FHE encryption of the plaintext, which can then be operated on.

- **Attribute-based encryption.** If we encrypt td using an attribute-based encryption (ABE) scheme, we immediately obtain a correct ABE scheme with certified deletion. In order to argue that this scheme has certified deletion security, we appeal to Lemma 6.9 with an interactive Z_λ that runs the ABE security game, encrypting its input td into the challenge ciphertext.

6.4 Balanced Binary-Measurement TCR from Almost-Regular OWFs

Definition 6.11 (Almost-Regular Function)**.** *A function $\mathcal{F} = \{f_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}\}$ is almost-regular if there exists efficiently computable polynomials $r(\lambda)$ and $p(\lambda)$ such that for all $\lambda \in \mathbb{N}$ and $x \in \{0,1\}^{m(\lambda)}$,*

$$\frac{1}{p(\lambda)} \cdot 2^{r(\lambda)} \leq \left|\{x' \in \{0,1\}^{n(\lambda)} : f_\lambda(x') = f_\lambda(x)\}\right| \leq p(\lambda) \cdot 2^{r(\lambda)}.$$

Note that we assume $r(\lambda)$ is efficiently computable, which means that the regularity of $\mathcal{F}$ is *known*. This is often contrasted with the more general class of functions that are *unknown* regular. Throughout this work, we always means *known* regular.

Definition 6.12 (Balanced Function)**.** *A function $\mathcal{F} = \{f_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}\}_{\lambda\in\mathbb{N}}$ is δ-*balanced *for some constant $\delta \in [0,1)$ if there exists a family of sets $\{\mathsf{BAD}_\lambda \subset \{0,1\}^{n(\lambda)}\}_{\lambda\in\mathbb{N}}$ such that*

1. $|\mathsf{BAD}_\lambda|/2^{n(\lambda)} = \mathrm{negl}(\lambda)$.

2. $\Pr_{x\leftarrow\{0,1\}^{m(\lambda)}}[f_\lambda(x) \in \mathsf{BAD}_\lambda] = \mathrm{negl}(\lambda)$.

3. *For every $z \notin \mathsf{BAD}_\lambda$, $\Pr_{x\leftarrow\{0,1\}^{m(\lambda)}}[f_\lambda(x) = z] \cdot 2^{n(\lambda)} \in [1-\delta, 1+\delta]$.*

Definition 6.13 (One-Way Function)**.** *A function $\mathcal{F} = \{f_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{\ell(\lambda)}\}$ is one-way if for any QPT adversary $\mathcal{A} = \{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$,*

$$\Pr\left[f_\lambda(x') = f(x) : \begin{array}{r} x \leftarrow \{0,1\}^{m(\lambda)} \\ x' \leftarrow \mathcal{A}_\lambda(f(x)) \end{array}\right] = \mathrm{negl}(\lambda).$$

We say that $\mathcal{F}$ is one-way over its range *if for any QPT adversary $\mathcal{A} = \{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$,*

$$\Pr\left[f_\lambda(x) = y : \begin{array}{r} y \leftarrow \{0,1\}^{\ell(\lambda)} \\ x \leftarrow \mathcal{A}_\lambda(y) \end{array}\right] = \mathrm{negl}(\lambda).$$

Definition 6.14 (Universal Hash)**.** *A hash function family* $\mathcal{H} = \{H_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}\}_{\lambda\in\mathbb{N}}$ *is called* $t(\lambda)$*-universal if for each distinct* $x_1,\ldots,x_{t(\lambda)} \in \{0,1\}^{m(\lambda)}$ *and* $y_1,\ldots,y_{t(\lambda)} \in \{0,1\}^{n(\lambda)}$*, it holds that*

$$\Pr_{h\leftarrow H_\lambda}\left[h(x_1) = y_1 \wedge \cdots \wedge h(x_{t(\lambda)}) = y_{t(\lambda)}\right] = 2^{-n(\lambda)\cdot t(\lambda)}.$$

Imported Theorem 6.15 ([HHK+09])**.** *Let* $\mathcal{F} = \{f_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{\ell(\lambda)}\}$ *be an almost-regular one-way function. Then there exists* $n(\lambda) < m(\lambda)$ *and* $\delta \in [0,1)$ *such that for any* 3λ*-universal hash family* $\mathcal{H} = \{H_\lambda : \{0,1\}^{\ell(\lambda)} \to \{0,1\}^{n(\lambda)}\}_{\lambda\in\mathbb{N}}$ *where each* $h \in H_\lambda$ *can be described by* $s(\lambda)$ *bits, the function*

$$\mathcal{F}' = \left\{f'_\lambda : \{0,1\}^{s(\lambda)+m(\lambda)} \to \{0,1\}^{s(\lambda)+n(\lambda)}\right\}_{\lambda\in\mathbb{N}}, \text{ where } f'_\lambda(h,x) \coloneqq (h, h(f_\lambda(x))),$$

is δ*-balanced and one-way over its range.*

Now consider any balanced function $\mathcal{F} = \{f_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}\}_{\lambda\in\mathbb{N}}$ that is one-way over its range, and define the family of hash functions

$$\mathcal{H}^{\mathcal{F}} = \left\{H_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}\right\}_{\lambda\in\mathbb{N}}$$

as follows. For each $\Delta \in \{0,1\}^{n(\lambda)}$, define $f_\Delta : \{0,1\}^{n(\lambda)} \to \{0,1\}^{n(\lambda)}$ to, on input z, output the lexicographically first element of $\{z, z\oplus\Delta\}$.[13] Then we define

$$H_\lambda \coloneqq \{h_{\lambda,\Delta} \coloneqq f_\Delta \circ f_\lambda\}_{\Delta\in\{0,1\}^{n(\lambda)}}.$$

We will also define the family of measurement functions

$$\mathcal{M} = \left\{\{M[h_{\lambda,\Delta}]\}_{h_{\lambda,\Delta}\in H_\lambda}\right\}_{\lambda\in\mathbb{N}}$$

as follows. The predicate $M[h_{\lambda,\Delta}] : \{0,1\}^m \to \{0,1\}$ takes x as input, computes $z \coloneqq f_\lambda(x)$, and outputs 0 if $z < z\oplus\Delta$ and 1 if $z > z\oplus\Delta$ (where ordering is lexicographical).

Theorem 6.16. *Let* $\delta \in [0,1)$ *be a constant and* $\mathcal{F} = \{f_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}\}_{\lambda\in\mathbb{N}}$ *be a* δ*-balanced function that is one-way over its range. Let* $\mathcal{H}^{\mathcal{F}}$ *and* $\mathcal{M}$ *be as defined above. Then,* $\mathcal{H}^{\mathcal{F}}$ *is a balanced binary-measurement TCR hash with associated measurement function* $\mathcal{M}$*.*

Imported Theorem 6.15 and Theorem 6.6 immediately give the following corollary.

Corollary 6.17. *Assuming almost-regular one-way functions, there exists a quantum canonical bit commitment with* PVD*.*

Proof. (Of Theorem 6.16) First, we check property (2) of Definition 6.1. By properties (2) and (3) of Definition 6.12, it holds that with $1 - \mathrm{negl}(\lambda)$ probability over the sampling of $h \leftarrow H_\lambda$ and $x \leftarrow \{0,1\}^m$,

$$\left|\frac{|\{x' \in h^{-1}(h(x))\} : M[h] = 0| - |\{x' \in h^{-1}(h(x))\} : M[h] = 1|}{|\{x' \in h^{-1}(h(x))\} : M[h] = 0| + |\{x' \in h^{-1}(h(x))\} : M[h] = 1|}\right| \le \delta.$$

[13] We don't need to worry about the case when $\Delta = 0^{n(\lambda)}$ since we'll be sampling Δ uniformly, but one could define f_Δ to be the identity in that case.

Next, we check property (1). Throughout this proof, we will drop indexing by λ for convenience. Suppose there exists a QPT adversary $\mathcal{A}$ that breaks the $\mathcal{M}$-target-collision-resistance of $\mathcal{H}$. That is, the following experiment outputs 1 with $\mathsf{non\text{-}negl}(\lambda)$ probability.

$\underline{\mathsf{Exp}_{\mathsf{TCR}}}$

- The challenger samples $\Delta \leftarrow \{0,1\}^n$ and prepares the state $1/\sqrt{2^m}\sum_{x\in\{0,1\}^m}|x\rangle$ on register X. It applies h_Δ on X to a fresh register Y and measures $y \in \{0,1\}^n$, and then measures $P[h_\Delta]$ on X to obtain a bit b and left-over state on register X. The challenger sends (Δ, y, b) and register X to $\mathcal{A}$.
- $\mathcal{A}$ outputs a string $x' \in \{0,1\}^n$.
- Output 1 if $h_\Delta(x') = y$ and $M[h_\Delta](x') = 1 - b$.

We now define an adversary $\mathcal{A}'$ that breaks the one-wayness of $\mathcal{F}$ over its range.

$\underline{\mathsf{Exp}_{\mathsf{OW}}}$

- The challenger samples $z \leftarrow \{0,1\}^n$ and sends z to $\mathcal{A}'$.
- $\mathcal{A}'$ prepares the state $1/\sqrt{2^m}\sum_{x\in\{0,1\}^m}|x\rangle$ on register X, applies f on X to a fresh register Z, and measures $z' \in \{0,1\}^n$. If $z' = z$, then measure register X to obtain x', and return x'. Otherwise, set $\Delta := z \oplus z'$, set $b = 0$ if $z' < z$ and $b = 1$ otherwise, and set $y = f_\Delta(z)$. Then, initialize $\mathcal{A}$ with (Δ, y, b) and register X. Run $\mathcal{A}$ and forward its output x' to the challenger.
- Output 1 if $f(x') = z$.

It suffices to show that $\mathcal{A}$'s input comes from the same distribution over (X, Δ, y, b) in both experiments. To see this, we describe an alternative but identical way to sample (X, Δ, y, b) in the experiment $\mathsf{Exp}_{\mathsf{TCR}}$. Recalling that $h_\Delta = f_\Delta \circ f$, the challenger could (1) apply f on X to a fresh register Z, (2) sample $\Delta \leftarrow \{0,1\}^n$, (3) apply f_Δ on Z to a fresh register Y, and (4) measure Y to obtain y and measure $M[h_\Delta]$ on X to obtain b. Note that step (4) is equivalent to instead just measuring the Z register to obtain z, defining $b = 0$ if $z < z \oplus \Delta$ and $b = 1$ if $z > z \oplus \Delta$, and defining $y = f_\Delta(z)$. Thus, we can imagine first applying f on X to a fresh register Z, measuring Z to obtain z, sampling $\Delta \leftarrow \{0,1\}^n$, and defining $y = f_\Delta(z)$. Defining $z' = z \oplus \Delta$ and using the fact that Δ was sampled uniformly at random, we see that this is exactly the same distribution that is sampled in $\mathsf{Exp}_{\mathsf{OW}}$, except that $\mathcal{A}$ is not initialized if $\Delta = 0^{n(\lambda)}$ (in which case $\mathcal{A}'$ wins the experiment anyway).

$\square$

Now, we generalize the notion of almost-regularity (Definition 6.11), balanced (Definition 6.12), and one-wayness (Definition 6.13) to function *families*, where there is a set of of $f \in F_\lambda$ associated with each security parameter. All previous definitions generalize to this setting with the requirement that they hold with $1 - \mathrm{negl}(\lambda)$ probability over $f \leftarrow F_\lambda$, and all previous claims follow. We consider families of functions with *trapdoors* that allow us to invert the function and obtain public-key encryption along with other cryptographic primitives.

Definition 6.18 (Superposition-invertible trapdoor function)**.** *We say that a function family $\mathcal{F} = \{F_\lambda\}_{\lambda\in\mathbb{N}}$ is a superposition-invertible trapdoor function if there exist algorithms* $\mathsf{Samp}, \mathsf{Invert}$ *with the following properties.*

- $\mathsf{Samp}(1^\lambda)$*: The sampling algorithm samples a uniformly random function $f \in F_\lambda$ along with a trapdoor* td*.*
- $\mathsf{Invert}(\mathsf{td}, y)$*: Given the trapdoor* td *and an image y,* Invert *outputs a state within negligible trace distance of*

$$\frac{1}{\sqrt{|f^{-1}(y)|}} \sum_{x:f(x)=y} |x\rangle\,.$$

Remark 6.19. *For the case of injective function families $\mathcal{F}$, the notion of superposition-invertible trapdoor is equivalent to the standard notion of trapdoor, since there is only one preimage per image.*

Claim 6.20. *Assuming injective trapdoor one-way functions (or more generally, superposition-invertible trapdoor almost-regular one-way functions), there exists a balanced binary-measurement TCR hash with trapdoor phase-recoverability.*

By Theorem 6.8 and Corollary 6.10, we obtain the following corollary.

Corollary 6.21. *Assuming the existence of injective trapdoor one-way functions (or more generally, superposition-invertible trapdoor almost-regular one-way functions), there exists PKE with* PVD*. Additionally assuming post-quantum*

$$X \in \left\{ \begin{array}{r} \textit{quantum fully-homormophic encryption, attribute-based encryption,} \\ \textit{witness encryption, timed-release encryption} \end{array} \right\},$$

there exists X with PVD*.*

Proof. (Of Claim 6.20) Given a superposition-invertible almost-regular one-way function, then we know from Imported Theorem 6.15 that we can compose it with a 3λ-universal hash function to obtain a δ-balanced function $\mathcal{F}$ that is one-way over its range, and Theorem 6.16 tells us that we can then obtain a balanced binary-measurement TCR hash $\mathcal{H}^{\mathcal{F}} = \{H_\lambda\}_{\lambda\in\mathbb{N}}$. It remains to check that the resulting hash has trapdoor phase-recoverability.

To see this, we observe that for any polynomials $m(\lambda), n(\lambda), t(\lambda)$, there exists a superposition-invertible $t(\lambda)$-universal hash function family $\{U_\lambda : \{0,1\}^{m(\lambda)} \to \{0,1\}^{n(\lambda)}\}_{\lambda\in\mathbb{N}}$ (without the need for a trapdoor). For example, we can use the Chor-Goldreich construction [CG89], where each hash in the family is defined by coefficients of a degree-$(t(\lambda)-1)$ univariate polynomial over a finite field, and evaluation is polynomial evaluation. To invert, use a root-finding algorithm (e.g. [CZ81]) to recover the (at most polynomial) roots, and then arrange these in superposition. Note that for a compressing universal hash from $\{0,1\}^m \to \{0,1\}^n$, one would use a finite field of size at least 2^m and define the hash output to consist of (say) the first n bits of the description of the finite field element that results from polynomial evaluation. In this case, the quantum inverter would first prepare a uniform superposition over all of the remaining $m-n$ bits of the field element, and run the above procedure in superposition.

Thus, given $h \in H_\lambda$, where $h = f_\Delta \circ f$ for $\Delta \neq 0^n$, along with a trapdoor td for f, we can efficiently prepare the state

$$|\psi_{h,y,0}\rangle = \frac{1}{\sqrt{|h^{-1}(y)|}} \sum_{x:h(x)=y} |x\rangle\,.$$

Then, the procedure $\mathsf{Recover}(\mathsf{td}, y, X)$ would measure register X in the $\{|\psi_{h,y,0}\rangle\langle\psi_{h,y,0}|, \mathbb{I} - |\psi_{h,y,0}\rangle\langle\psi_{h,y,0}|\}$ basis, and output 0 if the first outcome is observed. We have that with probability $1 - \text{negl}(\lambda)$ over the sampling of h,

$$\Pr_{x \leftarrow \{0,1\}^m}[\mathsf{Recover}(\mathsf{td}, h(x), |h, h(x), 0\rangle) \to 0] = 1,$$
$$\Pr_{x \leftarrow \{0,1\}^m}[\mathsf{Recover}(\mathsf{td}, h(x), |h, h(x), 1\rangle) \to 0] \leq (1-\delta)^2,$$

by the proof of binding in Theorem 6.6. This completes the proof.

□

6.5 Balanced Binary-Measurement TCR from Pseudorandom Group Actions

Finally, we show that the recent public-key encryption scheme of [HMY23] based on pseudorandom group actions has publicly-verifiable deletion, which follows fairly immediately from our framework. First, we need some preliminaries from [JQSY19, HMY23].

Definition 6.22 (Group Action). *Let G be a (not necessarily abelian) group, S be a set, and $\star : G \times S \to S$ be a function where we write $g \star s$ to mean $\star(g, s)$. We say that $(G, S, \star)$ is a group action if it satisfies the following:*

- *For the identity element $e \in G$ and any $s \in S$, we have $e \star s = s$.*
- *For any $g, h \in G$ and any $s \in S$, we have $(gh) \star s = g \star (h \star s)$.*

[JQSY19, HMY23] also require a number of efficiency properties from the group action, and we refer the reader to their papers for these specifications.

Definition 6.23 (Pseudorandom Group Action). *A group action $(G, S, \star)$ is* pseudorandom *if it satisfies the following:*

- *We have that*
$$\Pr_{s,t \leftarrow S}[\exists g \in G \text{ s.t. } g \star s = t] = \text{negl}(\lambda).$$
- *For any QPT adversary $\{\mathcal{A}_\lambda\}_{\lambda \in \mathbb{N}}$,*
$$\Big| \Pr_{s \leftarrow S, g \leftarrow S}[\mathcal{A}_\lambda(s, g \star s) = 1] - \Pr_{s,t \leftarrow S}[\mathcal{A}_\lambda(s, t) = 1] \Big| = \text{negl}(\lambda).$$

Given a pseudorandom group action $(G, S, \star)$, [HMY23] consider the following hash family $\mathcal{H}^{(G,S,\star)} = \{H_h\}_{h \in S_G}$, where $S_G = \{(s_0, s_1) \in S^2 : \exists g \in G \text{ s.t. } s_1 = g \star s_0\}$.

- The algorithm $\mathsf{Samp}(1^\lambda)$ samples $s_0 \leftarrow S, g \leftarrow G$ and outputs $h = (s_0, s_1)$ as the description of the hash and $\mathsf{td} = g$ as the trapdoor.
- For an input (b, k) where $b \in \{0, 1\}$ and $k \in G$, define $h(b, k) := k \star s_b$.

Claim 6.24. *$\mathcal{H}^{(G,S,\star)}$ is a balanced binary-measurement TCR hash with trapdoor phase-recoverability.*

Proof. Define predicate family $\mathcal{M}$ as $M[h](b,k) = b$. That is, it does not depend on h, and simply outputs the first bit of its input. Then, this claim actually follows immediately from what is already proven in [HMY23]. First, [HMY23, Theorem 4.10] shows that given td and $y \in S$, it is possible to perfectly distinguish

$$\frac{1}{\sqrt{2}} |0, h_0^{-1}(y)\rangle + \frac{1}{\sqrt{2}} |1, h_1^{-1}(y)\rangle \text{ and } \frac{1}{\sqrt{2}} |0, h_0^{-1}(y)\rangle - \frac{1}{\sqrt{2}} |1, h_1^{-1}(y)\rangle ,$$

where $h_b := h(b, \cdot)$, which establishes trapdoor phase-recoverability. Next, [HMY23, Theorem 4.19] shows that $\mathcal{H}^{(G,S,\star)}$ satisfies *conversion hardness*, which is equivalent to our notion of $\mathcal{M}$-target-collision-resistance. □

By Theorem 6.8 and Corollary 6.10, we obtain the following corollary.

Corollary 6.25. *Assuming the existence pseudorandom group actions, there exists PKE with* PVD. *Additionally assuming post-quantum*

$$X \in \left\{ \begin{array}{r} \textit{quantum fully-homormophic encryption, attribute-based encryption,} \\ \textit{witness encryption, timed-release encryption} \end{array} \right\},$$

there exists X with PVD.

References

[Aar09] Scott Aaronson. "Quantum copy-protection and quantum money". In: *2009 24th Annual IEEE Conference on Computational Complexity*. IEEE. 2009, pp. 229–242 (cit. on p. 9).

[Ajt96] Miklós Ajtai. "Generating Hard Instances of Lattice Problems (Extended Abstract)". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*. Ed. by Gary L. Miller. ACM, 1996, pp. 99–108. DOI: 10.1145/237814.237838. URL: https://doi.org/10.1145/237814.237838 (cit. on pp. 4, 21).

[AKN+23] Shweta Agarwal, Fuyuki Kitagawa, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa. "Public Key Encryption with Secure Key Leasing". In: *Eurocrypt 2023 (to appear)*. 2023 (cit. on pp. 3, 9).

[AL21] Prabhanjan Ananth and Rolando L. La Placa. "Secure Software Leasing". In: *Advances in Cryptology – EUROCRYPT 2021*. Ed. by Anne Canteaut and François-Xavier Standaert. Cham: Springer International Publishing, 2021, pp. 501–530. ISBN: 978-3-030-77886-6 (cit. on p. 9).

[APV23] Prabhanjan Ananth, Alexander Poremba, and Vinod Vaikuntanathan. *Revocable Cryptography from Learning with Errors*. Cryptology ePrint Archive, Paper 2023/325. https://eprint.iacr.org/2023/325. 2023. URL: https://eprint.iacr.org/2023/325 (cit. on pp. 3, 9).

[Ban93] W. Banaszczyk. "New bounds in some transference theorems in the geometry of numbers." In: *Mathematische Annalen* 296.4 (1993), pp. 625–636. URL: http://eudml.org/doc/165105 (cit. on p. 32).

[BB84] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*. Bangalore, 1984, p. 175 (cit. on pp. 3, 9).

[BBK22] Nir Bitansky, Zvika Brakerski, and Yael Tauman Kalai. *Constructive Post-Quantum Reductions*. 2022. DOI: 10.48550/ARXIV.2203.02314. URL: https://arxiv.org/abs/2203.02314 (cit. on pp. 35, 36).

[BCM+21] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. "A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device". In: *J. ACM* 68.5 (Aug. 2021). ISSN: 0004-5411. DOI: 10.1145/3441309. URL: https://doi.org/10.1145/3441309 (cit. on p. 32).

[BGG+23] James Bartusek, Sanjam Garg, Vipul Goyal, Dakshita Khurana, Giulio Malavolta, Justin Raizes, and Bhaskar Roberts. *Obfuscation and Outsourced Computation with Certified Deletion*. Cryptology ePrint Archive, Paper 2023/265. 2023. URL: https://eprint.iacr.org/2023/265 (cit. on pp. 3, 9, 10, 35, 36).

[BI20] Anne Broadbent and Rabib Islam. "Quantum Encryption with Certified Deletion". In: *Lecture Notes in Computer Science* (2020), pp. 92–122. ISSN: 1611-3349. DOI: 10.1007/978-3-030-64381-2_4. URL: http://dx.doi.org/10.1007/978-3-030-64381-2_4 (cit. on pp. 3, 7, 9, 16, 35).

[BK22] James Bartusek and Dakshita Khurana. *Cryptography with Certified Deletion*. Cryptology ePrint Archive, Paper 2022/1178. https://eprint.iacr.org/2022/1178. 2022. URL: https://eprint.iacr.org/2022/1178 (cit. on pp. 3, 9, 11, 42).

[Bra18] Zvika Brakerski. "Quantum FHE (Almost) As Secure AsÂ Classical". In: *Advances in Cryptology – CRYPTO 2018*. Ed. by Hovav Shacham and Alexandra Boldyreva. Cham: Springer International Publishing, 2018, pp. 67–95. ISBN: 978-3-319-96878-0 (cit. on p. 32).

[CFGN96] Ran Canetti, Uri Feige, Oded Goldreich, and Moni Naor. "Adaptively Secure Multi-Party Computation". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, pp. 639–648. ISBN: 0897917855. DOI: 10.1145/237814.238015. URL: https://doi.org/10.1145/237814.238015 (cit. on p. 9).

[CG89] B. Chor and O. Goldreich. "On the Power of Two-Point Based Sampling". In: *J. Complex.* 5.1 (Apr. 1989), pp. 96–106. ISSN: 0885-064X. DOI: 10.1016/0885-064X(89)90015-0. URL: https://doi.org/10.1016/0885-064X(89)90015-0 (cit. on p. 46).

[CX22] Shujiao Cao and Rui Xue. "The Gap Is Sensitive to Size of Preimages: Collapsing Property Doesn't Go Beyond Quantum Collision-Resistance for Preimages Bounded Hash Functions". In: Springer-Verlag, 2022 (cit. on pp. 6, 15, 29).

[CZ81] David Geoffrey Cantor and Hans Zassenhaus. "A new algorithm for factoring polynomials over finite fields". In: *Mathematics of Computation* 36 (1981), pp. 587–592 (cit. on p. 46).

[DS22] Marcel Dall'Agnol and Nicholas Spooner. *On the necessity of collapsing*. Cryptology ePrint Archive, Paper 2022/786. https://eprint.iacr.org/2022/786. 2022. URL: https://eprint.iacr.org/2022/786 (cit. on pp. 6, 15, 29, 30).

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. "Trapdoors for Hard Lattices and New Cryptographic Constructions". In: *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*. STOC '08. Victoria, British Columbia, Canada: Association for Computing Machinery, 2008, pp. 197–206. ISBN: 9781605580470. DOI: 10.1145/1374376.1374407. URL: https://doi.org/10.1145/1374376.1374407 (cit. on p. 21).

[GR02] Lov K. Grover and Terry Rudolph. "Creating superpositions that correspond to efficiently integrable probability distributions". In: *arXiv: Quantum Physics* (2002) (cit. on p. 32).

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters. "Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based". In: *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*. Ed. by Ran Canetti and Juan A. Garay. Vol. 8042. Lecture Notes in Computer Science. Springer, 2013, pp. 75–92. DOI: 10.1007/978-3-642-40041-4_5. URL: https://doi.org/10.1007/978-3-642-40041-4%5C_5 (cit. on p. 35).

[HH00] L. Hales and S. Hallgren. "An improved quantum Fourier transform algorithm and applications". In: *Proceedings 41st Annual Symposium on Foundations of Computer Science*. 2000, pp. 515–525. DOI: 10.1109/SFCS.2000.892139 (cit. on p. 20).

[HHK+09] Iftach Haitner, Omer Horvitz, Jonathan Katz, Chiu-Yuen Koo, Ruggero Morselli, and Ronen Shaltiel. "Reducing Complexity Assumptions for Statistically-Hiding Commitment". In: *Journal of Cryptology* 22.3 (2009), pp. 283–310. DOI: 10.1007/s00145-007-9012-8. URL: https://doi.org/10.1007/s00145-007-9012-8 (cit. on pp. 17, 44).

[HMNY21] Taiga Hiroka, Tomoyuki Morimae, Ryo Nishimaki, and Takashi Yamakawa. "Quantum Encryption with Certified Deletion, Revisited: Public Key, Attribute-Based, and Classical Communication". In: *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part I*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13090. Lecture Notes in Computer Science. Springer, 2021, pp. 606–636. DOI: 10.1007/978-3-030-92062-3_21. URL: https://doi.org/10.1007/978-3-030-92062-3%5C_21 (cit. on pp. 3, 9, 10).

[HMNY22a] Taiga Hiroka, Tomoyuki Morimae, Ryo Nishimaki, and Takashi Yamakawa. *Certified Everlasting Functional Encryption*. Cryptology ePrint Archive, Paper 2022/969. https://eprint.iacr.org/2022/969. 2022. URL: https://eprint.iacr.org/2022/969 (cit. on pp. 3, 9).

[HMNY22b] Taiga Hiroka, Tomoyuki Morimae, Ryo Nishimaki, and Takashi Yamakawa. "Certified Everlasting Zero-Knowledge Proof for QMA". In: *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13507. Lecture Notes in Computer Science. Springer, 2022, pp. 239–268. DOI: 10.1007/978-3-031-15802-5_9. URL: https://doi.org/10.1007/978-3-031-15802-5%5C_9 (cit. on pp. 3, 9).

[HMY23] Minki Hhan, Tomoyuki Morimae, and Takashi Yamakawa. “From the Hardness of Detecting Superpositions to Cryptography: Quantum Public Key Encryption and Commitments”. In: *Eurocrypt 2023 (to appear)*. 2023 (cit. on pp. 5, 8, 18, 47, 48).

[JL00] Stanisław Jarecki and Anna Lysyanskaya. “Adaptively Secure Threshold Cryptography: Introducing Concurrency, Removing Erasures”. In: *Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques*. EUROCRYPT'00. Bruges, Belgium: Springer-Verlag, 2000, pp. 221–242. ISBN: 3540675175 (cit. on p. 9).

[JQSY19] Zhengfeng Ji, Youming Qiao, Fang Song, and Aaram Yun. “General Linear Group Action on Tensors: A Candidate for Post-Quantum Cryptography”. In: *Theory of Cryptography: 17th International Conference, TCC 2019, Nuremberg, Germany, December 1–5, 2019, Proceedings, Part I*. Nuremberg, Germany: Springer-Verlag, 2019, pp. 251–281. ISBN: 978-3-030-36029-0. DOI: 10.1007/978-3-030-36030-6_11. URL: https://doi.org/10.1007/978-3-030-36030-6_11 (cit. on p. 47).

[LZ19] Qipeng Liu and Mark Zhandry. “Revisiting Post-quantum Fiat-Shamir”. In: *Advances in Cryptology – CRYPTO 2019*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Cham: Springer International Publishing, 2019, pp. 326–355. ISBN: 978-3-030-26951-7 (cit. on pp. 6, 16).

[Mah18] Urmila Mahadev. “Classical Verification of Quantum Computations”. In: *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*. 2018, pp. 259–267. DOI: 10.1109/FOCS.2018.00033 (cit. on p. 35).

[MR07] Daniele Micciancio and Oded Regev. “Worst-Case to Average-Case Reductions Based on Gaussian Measures”. In: *SIAM J. Comput.* 37.1 (2007), pp. 267–302. DOI: 10.1137/S0097539705447360. URL: https://doi.org/10.1137/S0097539705447360 (cit. on p. 21).

[MU07] Jörn Müller-Quade and Dominique Unruh. “Long-Term Security and Universal Composability”. In: *Theory of Cryptography*. Ed. by Salil P. Vadhan. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 41–60. ISBN: 978-3-540-70936-7 (cit. on p. 9).

[NC11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 10th. USA: Cambridge University Press, 2011. ISBN: 1107002176 (cit. on p. 19).

[Por23] Alexander Poremba. “Quantum Proofs of Deletion for Learning with Errors”. In: *14th Innovations in Theoretical Computer Science Conference, ITCS 2023, January 10-13, 2023, MIT, Cambridge, Massachusetts, USA*. Ed. by Yael Tauman Kalai. Vol. 251. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023, 90:1–90:14. DOI: 10.4230/LIPIcs.ITCS.2023.90. URL: https://doi.org/10.4230/LIPIcs.ITCS.2023.90 (cit. on pp. 3, 4, 6, 7, 9, 10, 15, 16, 19, 30, 31, 33–37).

[PRS17] Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. *Pseudorandomness of Ring-LWE for Any Ring and Modulus*. Cryptology ePrint Archive, Paper 2017/258. https://eprint.iacr.org/2017/258. 2017. URL: https://eprint.iacr.org/2017/258 (cit. on p. 22).

[Reg05] Oded Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *Journal of the ACM* 56.6 (2005), 34:1–34:40. ISSN: 0004-5411. DOI: 10.1145/1568318.1568324 (cit. on pp. 21, 22, 32).

[Sim98] Daniel R. Simon. "Finding collisions on a one-way street: Can secure hash functions be based on general assumptions?" In: *Advances in Cryptology — EUROCRYPT'98*. Ed. by Kaisa Nyberg. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 334–345. ISBN: 978-3-540-69795-4 (cit. on p. 5).

[SSTX09] Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. "Efficient Public Key Encryption Based on Ideal Lattices". In: *Advances in Cryptology – ASIACRYPT 2009*. Ed. by Mitsuru Matsui. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 617–635. ISBN: 978-3-642-10366-7 (cit. on p. 15).

[TL17] Marco Tomamichel and Anthony Leverrier. "A largely self-contained and complete security proof for quantum key distribution". In: *Quantum* 1 (July 2017), p. 14. ISSN: 2521-327X. DOI: 10.22331/q-2017-07-14-14. URL: https://doi.org/10.22331/q-2017-07-14-14 (cit. on p. 9).

[Unr15] Dominique Unruh. "Revocable Quantum Timed-Release Encryption". In: *J. ACM* 62.6 (Dec. 2015). ISSN: 0004-5411. DOI: 10.1145/2817206. URL: https://doi.org/10.1145/2817206 (cit. on pp. 3, 9).

[Unr16a] Dominique Unruh. "Collapse-Binding Quantum Commitments Without Random Oracles". In: *Advances in Cryptology – ASIACRYPT 2016*. Ed. by Jung Hee Cheon and Tsuyoshi Takagi. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 166–195. ISBN: 978-3-662-53890-6 (cit. on p. 4).

[Unr16b] Dominique Unruh. "Computationally Binding Quantum Commitments". In: *Advances in Cryptology – EUROCRYPT 2016*. Ed. by Marc Fischlin and Jean-Sébastien Coron. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 497–527. ISBN: 978-3-662-49896-5 (cit. on p. 4).

[Wie83] Stephen Wiesner. "Conjugate Coding". In: *SIGACT News* 15.1 (Jan. 1983), pp. 78–88. ISSN: 0163-5700. DOI: 10.1145/1008908.1008920. URL: https://doi.org/10.1145/1008908.1008920 (cit. on pp. 3, 9).

[Wil13] Mark M. Wilde. *Quantum Information Theory*. 1st. USA: Cambridge University Press, 2013. ISBN: 1107034256 (cit. on p. 19).

[Yan22] Jun Yan. "General Properties of Quantum Bit Commitments (Extended Abstract)". In: *Advances in Cryptology – ASIACRYPT 2022*. Ed. by Shweta Agrawal and Dongdai Lin. Cham: Springer Nature Switzerland, 2022, pp. 628–657. ISBN: 978-3-031-22972-5 (cit. on pp. 16, 38).

[Zha22] Mark Zhandry. “New Constructions of Collapsing Hashes”. In: *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13509. Lecture Notes in Computer Science. Springer, 2022, pp. 596–624. DOI: 10.1007/978-3-031-15982-4_20. URL: https://doi.org/10.1007/978-3-031-15982-4%5C_20 (cit. on pp. 4, 6, 15, 29).