Non-Interactive Zero-Knowledge Proofs with Certified Deletion*

Kasra Abbaszadeh[1] and Jonathan Katz[2]

[1] University of Maryland
kasraz@umd.edu
[2] Google
jkatz2@gmail.com

Abstract. We introduce the notion of non-interactive zero-knowledge (NIZK) proofs with *certified deletion*. Our notion enables the recipient of a (quantum) NIZK proof to delete the proof and obtain a (classical) certificate proving such deletion. We define this notion and propose two candidate constructions from standard cryptographic assumptions. Our first construction is based on classical NIZK proofs and quantum-hard one-way functions, but needs both the prover and verifier to run quantum algorithms. We then present an extension that allows the prover to be classical; this is based on the learning with errors problem and requires an instance-independent interactive setup between the prover and verifier.

Our results have applications to *revocable signatures of knowledge* and *revocable anonymous credentials*, which we also define and construct.

Keywords: quantum cryptography, certified deletion, non-interactive zero-knowledge, revocable cryptography, anonymous credentials.

1 Introduction

Quantum computation enables novel cryptographic capabilities that are known to be impossible in the classical world. These include primitives such as quantum money [50], unconditionally secure key agreement [16], one-shot signatures [7], copy protection [1], secure software leasing [8], unclonable encryption [28,20], and certified deletion [19,11]. Many of these results rely on the *no-cloning* property of quantum states. *Quantum copy protection* [1] guarantees that, given a single copy of a protected function f, no adversary can generate two copies of f.

Although copy protection has notable applications, e.g., public-key quantum money [2], building copy protection schemes from standard assumptions remains a challenging open problem. Motivated by this, Ananth et al. [8] introduced the weaker notion of *secure software leasing* (which also goes by the names *revocation* or *certified deletion*). At a high level, this notion enables a function f to be encoded into a quantum state that can be securely leased to a user; later, the user can provably delete that state, at which point the user is no longer able to

* Work supported in part by NSF award CNS-2154705.

execute f. Roughly speaking, then, copy protection prevents cloning altogether, whereas when using a revocation scheme, cloning is possible but not once a user wishes to later produce a deletion certificate.

Several prior works studied secure software leasing for specific cryptographic functionalities. Ananth et al. [9] and Agrawal et al. [5] independently introduced revocable public key encryption, where a decryption key is leased to a user; when the key is returned, the user loses the ability to decrypt. Morimae et al. [40] studied digital signatures with revocable signing keys or revocable signatures. In the former case, a party can lease a signing key to a user; once the key is revoked, the user cannot generate new signatures. In the latter case, a signature is leased, which can be deleted after being verified.

We extend this line of research and consider non-interactive zero-knowledge (NIZK) proofs [17]. An NIZK proof system enables a prover holding a witness for an NP statement to generate a proof of the truth of the statement without leaking any information about the witness. A fundamental barrier of a classical NIZK proof is that it can be verified arbitrarily many times by anyone who obtains it; in some settings, a prover may wish to allow verification for a limited time. To address this, we define *NIZK with certified deletion* (NIZK-CD), which enables recipients to certifiably delete the proofs they are given. The deletion certificate can be validated by the prover who generated the original proof; once a verifier generates a valid certificate, they can no longer return accepting proofs.

1.1 Our Contributions

We define NIZK-CD and propose constructions in the common reference string (CRS) model based on quantum-secure NIZK proofs and one-way functions. Deletion certificates and their corresponding validation algorithm are classical. In our first construction, the prover and verifier run quantum algorithms. We then extend this construction, based on learning with errors (LWE) [46], to allow for a classical prover who remotely prepares the proof for the (quantum) verifier.

As a natural application, we construct *revocable signature of knowledge* from NIZK-CD. We then use this to obtain *revocable anonymous credentials*, without relying on conventional blocklisting or expiration-based approaches [15,4,21].

Concurrent work. Concurrent work by Çakan et al. [22] defines *NIZK with certified deniability*, a stronger guarantee than certified deletion. Roughly, NIZK with certified deletion guarantees that once a user certifiably deletes a proof, the user cannot generate a proof that will be accepted by the honest verification algorithm; NIZK with certified deniability ensures that once a user certifiably deletes a proof, they have no advantage in convincing even a dishonest verifier about the truth of the corresponding statement. Çakan et al. [22] proposed a construction of NIZK with certified deniability in the random-oracle model. Their construction, however, carries quantum deletion certificates; hence, the prover runs quantum algorithms for both proof generation and certificate validation. It is an interesting open problem to realize NIZKs with certified deniability where the deletion certificate – or, ideally, the entire communication – is classical.

On the negative side, Çakan et al. [22] further showed the impossibility of NIZK with certified deniability in the plain model, where the security reduction makes use of the adversary in a black-box way. We believe that the same result would hold in the CRS model as long as the common reference is a classical string. Another interesting open problem is bypassing this impossible barrier.

1.2 Related Work

We discuss prior work on copy protection and certified deletion.

Copy protection and unclonable primitives. Aaronson [1] defined copy protection and presented a copy protection scheme for any unlearnable Boolean function relative to a quantum oracle. Later, it was shown that a classical oracle suffices [3]. Coladangelo et al. [25] proposed copy protection for (multi-bit) point functions and compute-and-compare functions in the quantum random-oracle model. Copy protection for decryption schemes and pseudorandom functions can be realized from compute-and-compare program obfuscation for unpredictable distributions, indistinguishability obfuscation (iO), and one-way functions [5]. Liu et al. [37] built bounded collusion-resistant copy protection for functionalities including pseudorandom functions from iO and the LWE assumptions.

Goyal et al. [29], and Jawale et al. [33] studied copy-protection for NIZK proofs, also called *unclonable NIZK*. They showed that this notion is equivalent to public-key quantum money [2], which is currently only known to exist under the assumption of iO. In this work, we consider the weaker notion of NIZK-CD, and show how to realize this notion based on weaker assumptions while also reducing the need for quantum communication (in our second construction).

Certified deletion and revocable cryptography. Unruh [49] introduced revocable encryption where the recipient of a quantum ciphertext can return it and lose all information about the message. Broadbent et al. [19] studied quantum one-time pad encryption with certified deletion, where a quantum ciphertext can be collapsed into a classical deletion certificate. Several recent works [31,44,11,10,12,23] extend this idea to advanced functionalities such as public-key and attribute-based encryption. Kitagawa et al. [36] and Bartusek et al. [13] replaced privately verifiable certificates with publicly verifiable ones under the assumption of one-way functions and one-way state generators [41]. Certified deletion has also been studied for the revocation of cryptographic keys [5,9,23], digital signatures [40], secret sharing [14,34], and obfuscation [10].

Revocation has also been considered for general programs by Ananth et al. [8]. However, their scheme relies on quantum-secure iO.

2 Technical Overview

In this section, we give a high-level overview of our techniques.

2.1 Definition of NIZK-CD

We define NIZK-CD, a tuple of algorithms $\langle \mathsf{Setup}, \mathsf{Prove}, \mathsf{Verify}, \mathsf{Delete}, \mathsf{Certify} \rangle$. The first three algorithms, Setup, Prove, and Verify, are defined similarly to the standard NIZK. In particular, Setup generates the CRS and its trapdoor. Prove and Verify are used to generate and verify a quantum NIZK proof π, respectively. The only difference is that Prove additionally outputs a private and classical certification key ck. Delete collapses π into a classical deletion certificate cert. The certificate is validated by running Certify on input cert and ck.

The primitive satisfies the basic security requirements of a standard NIZK, i.e., completeness, computational soundness, and computational zero knowledge. One can naturally strengthen single-theorem zero knowledge to a multi-theorem variant [27] and then also soundness to simulation extractibility [47,48].

We can achieve the security goal of deletion by two definitions. The first, followed by simplicity, relies on the concept of efficiently samplable (quantumly) hard distributions over NP instance-witness pairs. Consider $(\mathcal{X}, \mathcal{W})$ as such a distribution where $\mathcal{X}$ and $\mathcal{W}$ are the instances and the witnesses, respectively. Let $(x, w) \leftarrow (\mathcal{X}, \mathcal{W})$ be a hard instance-witness pair, and π be a NIZK-CD proof generated on inputs x and w. We require that no efficient quantum adversary given the instance x and the proof π can return both a proof π^* and a certificate cert such that π^* passes Verify and cert pass Certify algorithms successfully.

However, this definition does not capture the case in which the adversary receives more than one proof for different instances, and it does not support any security guarantees against malleability attacks. To address this limitation, we strengthen the definition to ensure that from any adversary that returns both an accepting proof and a valid certificate, one can extract the witness even in the case that the adversary is given oracle access to the prover algorithm.

2.2 Constructions of NIZK-CD

We propose a generic compiler to transform any classical NIZK to a NIZK-CD. The only assumption that we require is a quantum-secure commitment, which can be realized from quantum-hard one-way functions [26] in the CRS model.

Let $c \leftarrow \mathsf{Com}(\mathsf{crs}, m, r)$ be a commitment to a message m under a randomness r and a common reference string crs. Given an NP relation R, we generate a NIZK-CD proof for an instance-witness pair $(x, w) \in R$ as follows. The prover samples strings r_0 and r_1 and generates $\forall b \in \{0,1\} : c_b = \mathsf{Com}(\mathsf{crs}, b, r_b)$. Then, the prover produces a NIZK proof σ for $(x, w) \in R \bigvee \wedge_b c_b = \mathsf{Com}(\mathsf{crs}, 1-b, r_b)$. Given σ, c_0, and c_1, one can validate whether x is satisfied if σ accepts, and they have at least one r_b that refutes the commitment part of the relation.

The prover generates $|\psi\rangle := |0\rangle|r_0\rangle + |1\rangle|r_1\rangle$ and sends the NIZK-CD proof $\pi := (|\psi\rangle, \sigma, \{c_b\}_{b\in\{0,1\}})$. Let $\mathsf{ck} := (r_0, r_1)$ be the certification key and $U^{\mathsf{com}}_{c_0,c_1}$ as

$$|b\rangle|r\rangle|0\rangle \xrightarrow{U^{\mathsf{com}}_{c_0,c_1}} |b\rangle|r\rangle|\mathsf{Cmt} - \mathsf{Cmp}(\mathsf{crs}, b, r_b, c_b)\rangle,$$

where $\mathsf{Cmt} - \mathsf{Cmp}$ is a commit-and-compare function that commits to b using randomness r, returns 1 if it equals c_b, and returns 0 otherwise. The verifier

can verify the proof by applying $U^{\mathsf{com}}_{c_0,c_1}$ to $|\psi\rangle$ and measure commit-and-compare register. If the measured result is 1, i.e., there exists at least one r_b such that $c_b = \mathsf{Com}(\mathsf{crs}, b, r_b)$ and it suffices to infer $\exists w : (x, w) \in R$, if σ also passes the verification algorithm of the classical NIZK. Moreover, for honestly-generated proofs, the commit-and-compare register is always 1, and the post-measurement state remains the same as $|\psi\rangle$; hence, π can be re-verified for arbitrary times. The verifier can delete $|\psi\rangle$ by applying a Hadamard measurement, which yields a string d such that $d \cdot (r_0 \oplus r_1) = 0$ and then all information about strings r_0, r_1 is lost as the state collapses to $|0\rangle + (-1)^{d\cdot(r_0\oplus r_1)}|1\rangle$. The deletion certificate is $\mathsf{cert} := d$, and the prover validates it using (r_0, r_1), tracked as certification key.

More precisely, deletion security follows the adaptive hardcore bit-property of one-way functions, showed by several recent works [13,40]. This property states that given any one-way function f, no efficient adversary on input $y_0 = f(r_0)$ and $y_1 = f(r_1)$ and a superposition $|r_0\rangle + |r_1\rangle$ can output both a preimages r such that $f(r) \in \{y_0, y_1\}$ and an string d such that $d \cdot (r_0 \oplus r_1) = 0$ with an advantage more than $1/2$. Since the commitment scheme satisfies hiding and binding, one can view Com as a one-way function, and the adaptive hardcore bit property holds for the commitment function. This implies that the recipient of a NIZK-CD proof cannot output both an accepting deletion certificate cert and a proof π^*; due to the definition of $U^{\mathsf{com}}_{c_0,c_1}$, measuring the quantum state included in π^* in the computational basis should yield a valid commitment randomness r_b for $c_b = \mathsf{Com}(\mathsf{crs}, b, r_b)$, and this contradicts the adaptive hardcore bit property. The advantage can be reduced to negligible via parallel repetition. Completeness, zero knowledge, and extractability are borrowed from the classical NIZK σ.

Classical prover. We can observe that the prover only needs quantumness to create the state $|\psi\rangle$ and send it to the verifier. Other components of proof generation and deletion are based on classical computation and communication. We present an extension of our construction that allows a classical prover to remotely prepare $|\psi\rangle$ on the verifier's device, while the verifier does not learn any further information about the strings r_0, r_1, and the bit u. Then, the rest of the NIZK-CD construction remains the same as what was described above.

We first recall the notion of *noisy trapdoor claw-free (NTCF)* functions. Given a fixed key k, a pair of functions $f_{k,0}, f_{k,1} : \mathcal{X} \to \mathcal{Y}$ of an NTCF family satisfy the following properties. $f_{k,0}$ and $f_{k,1}$ share the same range. It is computationally hard to find a claw, i.e., a pair (r_0, r_1) where $f_{k,0}(r_0) = f_{k,1}(r_1)$. There exists a trapdoor td that allows to efficiently find two preimages r_0 and r_1 of any image y, i.e., for all $b \in \{0, 1\}$ we have $f_{k,b}(r_b) = y$. Moreover, the adaptive hardcore bit property holds, i.e., given y and $|r_0\rangle + |r_1\rangle$, where r_0 and r_1 are preimages of y, no adversary can return both one of the preimages and a string d such that $d \cdot (r_0 \oplus r_1) = 0$. The NTCF family can be constructed under LWE [18].

Assume that the key k for an NTCF functions and its trapdoor td are sampled and sent by the prover. The verifier generates the state $|\phi\rangle$ defined as follows.

$$|\phi\rangle := \sum_{r\in\mathcal{X}} |0\rangle|r\rangle \ + \ |1\rangle|r\rangle$$

Let $U_{f_{k,0},f_{k,1}}$ be a unitary quantum operation defined as below.

$$|b\rangle|r\rangle|0\rangle \xrightarrow{U_{f_{k,0},f_{k,1}}} |b\rangle|r\rangle|f_{k,b}(r)\rangle$$

The verifier applies $U_{f_{k,0},f_{k,1}}$ to $|\phi\rangle$ and measures the image register to obtain an image y and a state $|0\rangle|r_0\rangle + |1\rangle|r_1\rangle$, where (r_0, r_1) is the claw. $|\psi\rangle$ is used for NIZK-CD. The verifier sends y, and the prover recovers (r_0, r_1) using td.

We remark that state preparation is instance-independent and although the prover and verifier communicate for multiple rounds, π is still a non-interactive proof as it can be verified as many times without need for further interactions.

2.3 Revocable Signatures of Knowledge

A signature of knowledge is a digital signature in which messages are signed with respect to an instance of an NP language using the corresponding witness as signing key. Informally, it requires that if an adversary, given a signature to a message m with respect to an instance x, can output two signatures for m with respect to the same instance x, they *must know* the witness. Revocable signature of knowledge enables the recipient of the signature to delete the signature after it has been verified. This primitive can be constructed from simulation extractable NIZK-CD, where it just suffices to attach the message m to the proved instance. Revocable signatures of knowledge are used for revocable anonymous credentials, where the signed messages represent access tokens. Goyal et al. [29] and Jawale et al. [33] previously built (anonymous) revocable credentials from unclonable NIZKs. Despite ours, their schemes are based on post-quantum iO and inherently require quantum communication for the credential generation and deletion.

3 Preliminaries

We use λ to denote the security parameter. We use negl as a generic negligible function. For a set S, we use $x \leftarrow S$ to indicate that x is sampled uniformly from S. We define $[n] := \{0, 1, \ldots, n-1\}$. The term PPT stands for probabilistic polynomial time and QPT stands for quantum polynomial time.

Quantum conventions. A register X is a Hilbert space $\mathbb{C}^{2^n}$. An n-qubit pure state on register X is a unit vector $|\psi\rangle \in \mathbb{C}^{2^n}$. A mixed state on register X, described by a density matrix $\rho \in \mathbb{C}^{2^n \times 2^n}$, is a positive semi-definite Hermitian operator with trace 1. Also, a quantum operation F is a completely positive trace-preserving map from a register X to a register Y, i.e., on input a density matrix ρ on register X, the operation F returns $F(\rho)$ on register Y. A unitary operation $U : X \to X$ is a quantum operation that satisfies $U^\dagger U = UU^\dagger = I^X$, where I^X is identity. A projector Π is a Hermitian operator such that $\Pi^2 = \Pi$. A projective measurement is a collection of projectors $\{\Pi_i\}_i$ with $\sum_i \Pi_i = I$.

Densities and distances. Let $\mathcal{X}$ be a finite domain. A density on $\mathcal{X}$ is a function $f : \mathcal{X} \to [0, 1]$ such that $\sum_{x \in \mathcal{X}} f(x) = 1$. $\mathcal{D}_{\mathcal{X}}$ denotes the set of densities

on $\mathcal{X}$. For any $f \in \mathcal{D}_{\mathcal{X}}$, $\mathsf{Supp}(f) = \{x \in \mathcal{X} : f(x) > 0\}$. Given two densities f_0 and f_1 on $\mathcal{X}$, the Hellinger distance is defined as follows.

$$H^2(f_0, f_1) := 1 - \sum_{x \in \mathcal{X}} \sqrt{f_0(x) f_1(x)}$$

For two density matrices ρ and σ, their trace distance is defined as follows.

$$\|\rho - \sigma\|_{\mathsf{tr}} = \frac{1}{2}\|\rho - \sigma\|_1 = \frac{1}{2}\mathsf{Tr}\left[\sqrt{(\rho - \sigma)^2}\right],$$

where $\|\cdot\|_1$ is the trace norm.

Lemma 3.1. *Let $\mathcal{X}$ be a finite set, $f_0, f_1 \in \mathcal{D}_{\mathcal{X}}$, and $|\psi_b\rangle := \sum_{x \in \mathcal{X}} \sqrt{f_b(x)}\,|x\rangle$ for $b \in \{0,1\}$. We have*

$$\||\psi_0\rangle\langle\psi_0| - |\psi_1\rangle\langle\psi_1|\|_{\mathsf{tr}} = \sqrt{1 - (1 - H^2(f_0, f_1))^2}.$$

Theorem 3.1. ***(Holevo-Helstrom)*** *[30,32] Consider the experiment in which one of two quantum states ρ and σ is given to some distinguisher, each with probability $\frac{1}{2}$. The advantage of any distinguisher that can correctly determine which state was sent is at most $\frac{1}{2} + \frac{1}{2}\|\rho - \sigma\|_{\mathsf{tr}}$.*

3.1 The Learning with Errors Hardness Assumption

We recall the definition of the learning with errors (LWE) problem. For real positive B and integer q, the discrete truncated Gaussian distribution over $\mathbb{Z}_q$ with parameter B is a distribution on $\{x \in \mathbb{Z}_q : \|x\| \leq B\}$ with a density as

$$D_{\mathbb{Z}_q,B}(x) := \frac{e^{\frac{-\pi\|x\|^2}{B}}}{\sum_{x' \in \mathbb{Z}_q, \|x'\| \leq B} e^{\frac{-\pi\|x'\|^2}{B}}}.$$

For some higher dimension d, the truncated discrete Gaussian distribution over $\mathbb{Z}_q^d$ with parameter B is a distribution on $\{x \in \mathbb{Z}_q^d : \|x\| \leq B\sqrt{d}\}$ with the density

$$\forall x = (x_1, x_2, \ldots, x_d) \in \mathbb{Z}_q^d : \quad D_{\mathbb{Z}_q^d,B}(x) = D_{\mathbb{Z}_q,B}(x_1), D_{\mathbb{Z}_q,B}(x_2), \ldots, D_{\mathbb{Z}_q,B}(x_d).$$

We then define LWE that underlies several hardness assumptions in this paper.

Definition 3.1. ***(LWE)*** *Let $n(\lambda), m(\lambda), q(\lambda)$ be polynomials in λ. Moreover, let $\mathcal{X} = \mathcal{X}(\lambda)$ be a distribution over $\mathbb{Z}$. The $\mathsf{LWE}_{m,n,q,\mathcal{X}}$ problem is to distinguish between the distributions $(A, As + e)$ and (A, u), where $A \leftarrow \mathbb{Z}_q^{m \times n}$, $s \leftarrow \mathbb{Z}_q^n$, $e \leftarrow \mathcal{X}^m$, $u \leftarrow \mathbb{Z}_q^m$, such that m is, at most, polynomial in $n \log q$.*

We assume no QPT algorithm can solve $\mathsf{LWE}_{m,n,q,\mathcal{X}}$ with some non-negligible advantage in λ, even when given access to a quantum polynomial-size advice state depending on the parameters m, n, q, and $\mathcal{X}$ of the problem. We refer to this assumption as the $\mathsf{LWE}_{m,n,q,\mathcal{X}}$ assumption. It can be shown [46,42] that

for any $\alpha > 0$ such that $\sigma = \alpha q \geq 2\sqrt{n}$, $\mathsf{LWE}_{m,n,q,D_{\mathbb{Z}_{q,\sigma}}}$ is at least as hard as the shortest independent vector problem within a factor of $\gamma = \tilde{O}(n/\alpha)$, where $\tilde{O}$ hides logarithmic factors, in the *worst case* dimension n in lattices. The best known algorithm to solve the problem runs in time $2^{\tilde{O}(n/log\gamma)}$. We assume the hardness against polynomial-time quantum adversaries where γ is super-polynomial in n. We also recall two additional properties. The first shows that it is possible to generate LWE samples $(A, As + e)$ with a trapdoor that can recover s from the samples. We state this in the following Theorem.

Theorem 3.2. *[39] Let $n, m \geq 1$ and $q \geq 2$ be such that $m = \Omega(n \log q)$. There is an efficient randomized algorithm $\mathsf{Gen}(1^n, 1^m, q)$ that returns a matrix $A \in \mathbb{Z}_q^{n \times m}$ and a trapdoor td such that the distribution of A is negligibly close to uniform. There is an efficient deterministic algorithm Inv such that on input A, td, and a sample $As + e$, where $\|e\| \leq q/(c\sqrt{n \log q})$ and c is a universal constant, outputs vectors s and e with a high overwhelming probability.*

The second property is the existence of a "lossy mode" for LWE.

Theorem 3.3. *[6] $\mathcal{X} = \mathcal{X}(\lambda)$ is an efficiently sampleable distribution on $\mathbb{Z}_q$. Define a lossy sampler $\tilde{A} \leftarrow \mathsf{LSY}(1^m, 1^n, 1^\ell, q, x)$, s.t. $\tilde{A} = BC + F$, $B \leftarrow \mathbb{Z}_q^{m \times \ell}$, $C \leftarrow \mathbb{Z}_q^{\ell \times n}$, $F \leftarrow \mathbb{Z}_q^{m \times n}$. Under $\mathsf{LWE}_{m,\ell,q,\mathcal{X}}$ assumption, the distribution of $\tilde{A}$ is computationally indistinguishable from uniform $\tilde{A} \leftarrow \mathbb{Z}_q^{m \times n}$.*

3.2 Noisy Trapdoor Claw-Free Hash Function Families

We recall noisy trapdoor claw-free (NTCF) hash functions introduced by [18]. Given two finite sets $\mathcal{X}$ and $\mathcal{Y}$, a trapdoor claw-free family of functions satisfies the following properties. For a public key k, the functions $\{f_{k,b} : \mathcal{X} \to \mathcal{Y}\}_{b \in \{0,1\}}$ are both injective and have the same range and are invertible given a trapdoor td, i.e., on input td and an image $y \in \mathcal{Y}$ it is feasible to efficiently output $x_0, x_1 \in \mathcal{X}$ such that $f_0(x_0) = f_1(x_1) = y$. Furthermore, the pair of functions should be claw-free, i.e., it is computationally hard for an attacker to find two preimages x_0, x_1 such that $f_0(x_0) = f_1(x_1)$ without the trapdoor. The functions also satisfy the adaptive hardcore bit property, which states that it is computationally hard for an attacker to generate a non-trivial tuple (b, d, x_b) with a non-negligible probability more than $\frac{1}{2}$ the such that the equation $d \cdot (x_0 \oplus x_1) = 0$ is satisfied; note that x_{1-b} is a unique element such that $f_{1-b}(x_{1-b}) = f_b(x_b)$.

Unfortunately, we are not aware of any exact constructions of the trapdoor claw-free functions. Instead, Brakerski et al. [18] proposed a construction for noisy trapdoor claw-free functions, which relaxes the requirements as follows. First, the range of functions is not $\mathcal{Y}$, but instead $\mathcal{D}_\mathcal{Y}$, the set of probability densities over $\mathcal{Y}$. The trapdoor injective pair property is then defined according to the support of the output densities. The use of densities as the output of the functions requires considering additional requirements. In this paper, we need a quantum polynomial-time algorithm that efficiently prepares a superposition

over the range of the function, i.e., given a function key k and a bit $b \in \{0,1\}$, the algorithm can prepare the following quantum state.

$$\frac{1}{\sqrt{\mathcal{X}}} \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \sqrt{f_{k,b}(x)y}|x\rangle|y\rangle$$

The construction proposed in [18] is unable to exactly produce the above state; however, it is possible to create a superposition with coefficients such that $f_{k,b}(x)$ is approximated by another function $f'_{k,b}(x)$ and the resulting state is within a negligible distance from the above state. $f'_{k,b}(x)$ supports membership checks efficiently without the need for the trapdoor, and the inversion algorithm should operate properly on the images in the support of $f'_{k,b}(x)$. The adaptive hardcore bit property needs to also be slightly modified. The set $\mathcal{X}$ might not be a subset of binary strings. We first assume the existence of an injective, efficiently invertible map $J : \mathcal{X} \to \{0,1\}^w$ and consider the adaptive hardcore bit property to hold for a subset of all non-zero strings. The formal definition is as follows.

Definition 3.2. ***(NTCF)*** *[18] $\mathcal{F} := \{f_{k,b} : \mathcal{X} \to \mathcal{D}_\mathcal{Y}\}_{k \in \mathcal{K}, b \in \{0,1\}}$ is a NTCF hash function family if the following properties are satisfied.*

Key generation: *A* PPT*,* $\mathsf{NTCF.Gen}_\mathcal{F}$*, samples a key $k \in \mathcal{K}$ and a trapdoor* td*.*

Trapdoor Injective Pair: *For all $k \in \mathcal{K}$, $b \in \{0,1\}$, distinct $x, x' \in \mathcal{X}$,* $\mathsf{Supp}(f_{k,b}(x)) \cap \mathsf{Supp}(f_{k,b}(x')) = \emptyset$*. An efficient deterministic algorithm* $\mathsf{Inv}_\mathcal{F}$ *exists such that for all $k \in \mathcal{K}$, $b \in \{0,1\}$, $x \in \mathcal{X}$, and $y \in \mathsf{Supp}(f_{k,b}(x))$, it holds that* $\mathsf{Inv}(td, b, y) = x$*. Moreover, given a key $k \in \mathcal{K}$, there exists a perfect matching $\mathcal{R}_k \subseteq \mathcal{X} \times \mathcal{X}$ such that $f_{k,0}(x_0) = f_{k,1}(x_1)$ if and only if $(x_0, x_1) \in \mathcal{R}_k$.*

Range Superposition: *For all $k \in \mathcal{K}$, $b \in \{0,1\}$, $f'_{k,b} : \mathcal{X} \to \mathcal{D}_\mathcal{Y}$ exists where:*

- *For any claw $(x_0, x_1) \in \mathcal{R}_k$ with image $y \in \mathsf{Supp}(f'_{k,b}(x_b))$ it holds that* $\mathsf{Inv}_\mathcal{F}(\mathsf{td}, b, y) = x_b$ *as well as* $\mathsf{Inv}_\mathcal{F}(\mathsf{td}, b \oplus 1, y) = x_{b \oplus 1}$*.*
- *There exists an efficient deterministic algorithm* $\mathsf{Chk}_\mathcal{F}$ *where on input $k \in \mathcal{K}$, $b \in \{0,1\}$, $x \in \mathcal{X}$, $y \in \mathcal{Y}$, it outputs 1 if $y \in \mathsf{Supp}(f'_{k,b}(x))$ and 0 otherwise.*
- *For all $k \in \mathcal{K}$, $b \in \{0,1\}$, we have $\mathbb{E}_{x \leftarrow X}[H^2(f_{k,b}(x), f'_{k,b}(x))] \leq \mathsf{negl}(\lambda)$. In addition, there exists a* QPT *algorithm* $\mathsf{Samp}_\mathcal{F}$ *such that on input $k \in \mathcal{K}$ and $b \in \{0,1\}$ outputs the following quantum state.*

$$|\psi'\rangle = \frac{1}{\sqrt{|\mathcal{X}|}} \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \sqrt{(f'_{k,b}(x))(y)}|x\rangle|y\rangle.$$

Given $|\psi\rangle = \frac{1}{\sqrt{|\mathcal{X}|}} \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \sqrt{(f_{k,b}(x))(y)}|x\rangle|y\rangle$, Lemma 3.1 implies that

$$\||\psi\rangle\langle\psi| - |\psi'\rangle\langle\psi'|\|_{\mathsf{tr}} \leq \mathsf{negl}(\lambda).$$

Adaptive Hardcore Bit: *For all keys $k \in \mathcal{K}$ and a polynomial $\ell(\lambda)$:*

- *For all $b \in \{0,1\}$, $x \in \mathcal{X}$, there exists a subset of strings $\mathcal{G}_{k,b,x} \subseteq \{0,1\}^{\ell(\lambda)}$ such that $\Pr_{d \leftarrow \{0,1\}^{\ell(\lambda)}}[d \notin \mathcal{G}_{k,b,x}] \leq \mathsf{negl}(\lambda)$. Moreover, there exists a PPT algorithm to efficiently check membership in $\mathcal{G}_{k,b,x}$ given k, b, x and td.*
- *There exists an efficiently computable injection $J : \mathcal{X} \to \{0,1\}^{\ell(\lambda)}$ such that J can also be efficiently inverted on its range, and the following holds. Let*

  $H_k := \{(b, x_b, d, d \cdot (J(x_0) \oplus J(x_1)) | b \in \{0,1\}, (x_0, x_1) \in R_k, d \in \mathcal{G}_{k,0,x} \cap \mathcal{G}_{k,1,x}\}$,
  $\bar{H}_k := \{(b, x_b, d, u \oplus 1) | (b, x_b, d, u) \in H_k\}$.

  For any QPT algorithm $\mathcal{A}$ it holds that

$$\left| \Pr_{\mathsf{td},k \leftarrow \mathsf{NTCF.Gen}(1^\lambda)}[\mathcal{A}(k) \in H_k] - \Pr_{\mathsf{td},k \leftarrow \mathsf{NTCF.Gen}(1^\lambda)}[\mathcal{A}(k) \in \bar{H}_k] \right| \leq \mathsf{negl}(\lambda).$$

Theorem 3.4. *[18] Assuming the polynomial-time quantum hardness of LWE, there exists an NTCF hash function family.*

One can consider an amplified adaptive hardcore bit property such that the adversary cannot return a set $\{(b_i, x_{i,b_i}, d_i, u_i)\}_{i \in [n]}$ where n is polynomial in the security parameter λ, and each tuple satisfies $d_i \cdot (x_{i,b_i} \oplus x_{i,1-b_i}) = u_i$, so that $(x_{i,b_i}, x_{i,1-b_i})$ is a claw. The property is formally defined as follows.

Definition 3.3. ***(Amplified Adaptive Hardcore Bit)*** *An NTCF function family $\mathcal{F}$ satisfies the amplified adaptive hardcore bit property if, for any QPT algorithm $\mathcal{A}$ and a polynomial $n = \ell(\lambda)$, the following is at most $\mathsf{negl}(\lambda)$.*

$$\Pr\left[\begin{array}{c} \forall i \in [n] : (k_i, \mathsf{td}_i) \leftarrow \mathsf{NTCF.Gen}(1^\lambda) \\ \{(b_i, x_{i,b_i}, d_i, u_i)\}_{i \in [n]} \leftarrow \mathcal{A}(\{k_i\}_{i \in [n]}) \\ \forall \beta \in \{0,1\} : x_{i,\beta} = \mathsf{Inv}(\mathsf{td}_i, \beta, y_i) \end{array} : \begin{array}{c} \forall i \in [n] : d_i \in \mathcal{G}_{k,0,x} \cap \mathcal{G}_{k,1,x} \\ \wedge \\ u_i = d_i \cdot (J(x_{i,0}) \oplus J(x_{i,1})) \end{array}\right]$$

Theorem 3.5. *[45,35] Any NTCF family of functions satisfies the amplified adaptive hardcore bit property.*

We also note that recently Morimae et al. [40] introduced a similar notion of adaptive hardcore bit property for general one-way functions (OWFs), beyond those based on the LWE assumption, and showed the following result.

Theorem 3.6. *[40] Given $\ell(\lambda), \kappa(\lambda), n(\lambda) \in \mathbb{N}$, for any quantum-hard OWF $f : \{0,1\}^{\ell(\lambda)} \to \{0,1\}^{\kappa(\lambda)}$, and any QPT adversary $\mathcal{A}$,*

$$\Pr\left[\begin{array}{c} \forall i \in [n] : x_{i,0}, x_{i,1} \leftarrow \{0,1\}^{2\ell(\lambda)}, u_i \leftarrow \{0,1\} \\ \{(x_i, d_i)\}_{i \in [n]} \leftarrow \mathcal{A}(\otimes_{i \in [n]} \frac{|x_{i,0}\rangle + (-1)^{u_i} |x_{i,1}\rangle}{\sqrt{2}}, \{f(x_{i,b})\}_{i,b}) \end{array} : \begin{array}{c} \wedge_{i \in [n]} f(x_i) \in \{f(x_{i,0}), f(x_{i,1})\} \\ \wedge \\ \wedge_{i \in [n]} d_i \cdot (x_{i,0} \oplus x_{i,1}) = u_i \end{array}\right] \leq \mathsf{negl}(\lambda).$$

3.3 Other Useful Cryptographic Primitives and Lemmas

We recall the notion of commitment schemes in the CRS model, which is a central building block for our NIZK-CD constructions throughout this paper.

Definition 3.4. ***(Commitment)*** *Let $n(\lambda), \ell(\lambda), \kappa(\lambda)$ be polynomials.* Com *is a quantum-secure commitment if the following syntax and properties hold.*

- $(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)$: *on input λ, output* crs*, and trapdoor* td*.*
- $c \leftarrow \mathsf{Com}(\mathsf{crs}, m, r)$*: on input* crs*, a message $m \in \{0,1\}^{n(\lambda)}$, and a randomness $r \in \{0,1\}^{\ell(\lambda)}$, output a commitment $c \in \{0,1\}^{\kappa(\lambda)}$.*

Statistical Binding: *For any algorithm $\mathcal{A}$ and any sufficiently large $\lambda \in \mathbb{N}$,*

$$\Pr\left[\begin{array}{c}(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda) \\ (m_0, r_0, m_1, r_1) \leftarrow \mathcal{A}(\mathsf{crs})\end{array} : \begin{array}{c}\mathsf{Com}(\mathsf{crs}, m_0, r_0) = \mathsf{Com}(\mathsf{crs}, m_1, r_1) \\ \wedge\ m_0 \neq m_1\end{array}\right] \leq \mathsf{negl}(\lambda).$$

Computational Hiding: *For any* QPT *distinguisher $\mathcal{D}$, any sufficiently large $\lambda \in \mathbb{N}$, parameters $(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)$, and any $m_0, m_1 \in \{0,1\}^{n(\lambda)}$,*

$$\left|\Pr\left[\begin{array}{c} r_0 \leftarrow \{0,1\}^{\ell(\lambda)} \\ c_0 \leftarrow \mathsf{Com}(\mathsf{crs}, m_0, r_0)\end{array} : \mathcal{D}(\mathsf{crs}, c_0) = 1\right]\right.$$
$$\left. - \Pr\left[\begin{array}{c} r_1 \leftarrow \{0,1\}^{\ell(\lambda)} \\ c_1 \leftarrow \mathsf{Com}(\mathsf{crs}, m_1, r_1)\end{array} : \mathcal{D}(\mathsf{crs}, c_1) = 1\right]\right| \leq \mathsf{negl}(\lambda).$$

Theorem 3.7. *[26] Assuming a quantum-hard one-way function, there exists a statistically binding and computationally hiding commitment.*

We recall the notion of non-interactive zero-knowledge (NIZK) arguments in the CRS model. We provide two definitions of NIZK as follows. The first one is a single-theorem definition and ensures that no efficient adversary can output an accepting proof for any unsatisfied instance. The second one is a multi-theorem definition and ensures that from any efficient adversary that can output an accepting proof, one can efficiently extract a valid witness to the relation.

Definition 3.5. ***(NIZK for NP)*** *Let any* NP *relation R with a corresponding language L. $\Pi = \langle \mathsf{Setup}, \mathsf{Prove}, \mathsf{Verify} \rangle$ is a quantum-secure NIZK for* NP *in the CRS model if it satisfies the following syntax and security properties.*

- $(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)$: *on input λ, output* crs *and a trapdoor* td*.*
- $\pi \leftarrow \mathsf{Prove}(\mathsf{crs}, x, w)$: *on input* crs *and a pair $(x, w) \in R$, output a proof π.*
- $\{0,1\} \leftarrow \mathsf{Verify}(\mathsf{crs}, x, \pi)$: *on input* crs*, x, and π, output accept or reject.*

Perfect Completeness: *For every security parameter $\lambda \in \mathbb{N}$ and $(x, w) \in R$,*

$$\Pr\left[\begin{array}{c}(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda) \\ \pi \leftarrow \mathsf{Prove}(\mathsf{crs}, x, w)\end{array} : \mathsf{Verify}(\mathsf{crs}, x, \pi)\right] = 1.$$

Adaptive Computational Soundness: *For any* QPT *adversary algorithm* $\mathcal{A}$ *and any sufficiently large security parameter* λ*,*

$$\Pr\left[\begin{array}{c}(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Setup}(1^\lambda)\\(x,\pi)\leftarrow\mathcal{A}(\mathsf{crs})\end{array}:\mathsf{Verify}(\mathsf{crs},x,\pi)=1\wedge x\notin L\right]\leq\mathsf{negl}(\lambda).$$

Adaptive Computational Zero-Knowledge: *There exists a* QPT *simulator* $\mathsf{Sim}=(\mathsf{Sim}_0,\mathsf{Sim}_1)$ *where for every* QPT *adversary* $\mathcal{A}$*, every* QPT *distinguisher* $\mathcal{D}$*, and any sufficiently large* $\lambda\in\mathbb{N}$*,*

$$\left|\Pr\left[\begin{array}{c}(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Setup}(1^\lambda)\\(x,w,\xi)\leftarrow\mathcal{A}(\mathsf{crs})\\\pi\leftarrow\mathsf{Prove}(\mathsf{crs},x,w)\end{array}:\mathcal{D}(\mathsf{crs},x,\pi,\xi)=1\right]-\right.$$
$$\left.\Pr\left[\begin{array}{c}(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Sim}_0(1^\lambda)\\(x,w,\xi)\leftarrow\mathcal{A}(\mathsf{crs})\\\pi\leftarrow\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},x)\end{array}:\mathcal{D}(\mathsf{crs},x,\pi,\xi)=1\right]\right|\leq\mathsf{negl}(\lambda).$$

Theorem 3.8. *[43] Assuming polynomial quantum hardness of LWE, there exists a quantum-secure non-interactive, adaptively computationally sound, and adaptively computationally zero-knowledge argument for NP.*

We also propose a definition with stronger security properties.

Definition 3.6. ***(Simulation-Extractable NIZK for NP)*** *Let* R *be any* NP *relation with language* L*. Then,* $\Pi=\langle\mathsf{Setup},\mathsf{Prove},\mathsf{Verify}\rangle$ *is a quantum-secure simulation-extractable NIZK for NP in the CRS model if it satisfies the properties of Definition 3.5 and also the following additional properties.*

Adaptive Multi-Theorem Computational Zero-Knowledge: *There exists* QPT *simulator* $\mathsf{Sim}=(\mathsf{Sim}_0,\mathsf{Sim}_1)$*, such that for any* QPT *adversary algorithm* $\mathcal{A}$ *and sufficiently large* $\lambda\in\mathbb{N}$*,*

$$\left|\Pr\left[(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Setup}(1^\lambda):\mathcal{A}^{\mathsf{Prove}(\mathsf{crs},\cdot,\cdot)}(\mathsf{crs})=1\right]-\right.$$
$$\left.\Pr\left[(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Sim}_0(1^\lambda):\mathcal{A}^{\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},\cdot,\cdot)}(\mathsf{crs})=1\right]\right|\leq\mathsf{negl}(\lambda),$$

where the simulator algorithm Sim_1 *discards its fourth input value.*

Simulation Soundness: *Let* $\mathsf{Sim}=(\mathsf{Sim}_0,\mathsf{Sim}_1)$ *be the simulator given by the adaptive multi-theorem computational zero-knowledge. For every* QPT *algorithm* $\mathcal{A}$ *and sufficiently large* $\lambda\in\mathbb{N}$*, the following probability is, at most,* $\mathsf{negl}(\lambda)$*.*

$$\Pr\left[\begin{array}{c}(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Sim}_0(1^\lambda)\\(x,\pi)\leftarrow\mathcal{A}^{\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},\cdot,\cdot)}(\mathsf{crs})\end{array}:\mathsf{Verify}(\mathsf{crs},x,\pi)=1\wedge x\notin L\wedge x\notin Q\right],$$

where Q *is the list of queries from* $\mathcal{A}$ *to* Sim_1*.*

Simulation Extractability: *Let* $\mathsf{Sim}=(\mathsf{Sim}_0,\mathsf{Sim}_1)$ *be the simulator given by the adaptive multi-theorem computational zero-knowledge property. There exists*

a QPT *extractor* Ext *such that for every* QPT *algorithm* $\mathcal{A}$ *and sufficiently large* $\lambda \in \mathbb{N}$*, the following probability is, at most,* $\mathsf{negl}(\lambda)$*.*

$$\Pr\left[\begin{array}{c}(\mathsf{crs},\mathsf{td}) \leftarrow \mathsf{Sim}_0(1^\lambda)\\ (x,\pi) \leftarrow \mathcal{A}^{\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},\cdot,\cdot)}(\mathsf{crs}) \\ w \leftarrow \mathsf{Ext}(\mathsf{crs},\mathsf{td},x,\pi)\end{array} : \mathsf{Verify}(\mathsf{crs},x,\pi)=1 \wedge (x,w)\notin R \wedge x \notin Q\right],$$

where Q *is the list of queries from* $\mathcal{A}$ *to* Sim_1*.*

Remark 3.1. It is known [27,47,48,33] that multi-theorem simulation-extractable NIZK, i.e., Definition 3.5, satisfies Definition 3.6 since adaptive multi-theorem zero-knowledge implies adaptive single-theorem zero-knowledge property, and also simulation-soundness implies adaptive computational soundness. Moreover, one can show that the simulation extractability implies simulation soundness.

Theorem 3.9. *[48,33] Assuming a quantum-secure one-way function and a quantum-secure IND-CPA secure encryption scheme, any quantum-secure NIZK for NP can be transformed into a quantum-secure simulation-extractable NIZK.*

Corollary 3.1. *Assuming polynomial quantum hardness of learning with errors, there exists a quantum-secure simulation-extractable NIZK for NP exists.*

Proof. This follows from Theorems 3.8 and 3.9; IND-CPA encryption can be achieved from the quantum hardness of learning with errors [46]. □

Finally, we provide the cryptographic definition of the signature of knowledge.

Definition 3.7. ***(Signature of Knowledge)*** *Let* R *be an* NP *relation with language* L *and message space* $\mathcal{M}$*.* $\Sigma = \langle \mathsf{Setup}, \mathsf{Sign}, \mathsf{Verify}\rangle$ *is a quantum-secure* SimExt*-secure signature of knowledge if the following syntax and properties hold.*

- $(\mathsf{crs},\mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)$ *: on input* λ*, output a* crs *and trapdoor* td*.*
- $\sigma \leftarrow \mathsf{Sign}(\mathsf{crs},x,w,m)$ *: on input* crs*, pair* $(x,w) \in R$*, and message* $m \in \mathcal{M}$*, output a signature of knowledge* σ *to the message* m*.*
- $\{0,1\} \leftarrow \mathsf{Verify}(\mathsf{crs},x,m,\sigma)$ *: on input* crs*,* x*,* m*, and* σ*, accept or reject.*

Correctness: *For every* $\lambda \in \mathbb{N}$*, pair* $(x,w) \in R$ *and message* $m \in \mathcal{M}$*,*

$$\Pr\left[\begin{array}{c}(\mathsf{crs},\mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)\\ \sigma \leftarrow \mathsf{Sign}(\mathsf{crs},x,w,m)\end{array} : \mathsf{Verify}(\mathsf{crs},x,m,\sigma)=1\right] = 1.$$

Simulation: *There exist a* QPT *simulator algorithm* $\mathsf{Sim} = (\mathsf{Sim}_0,\mathsf{Sim}_1)$ *such that for every* QPT *algorithm* $\mathcal{A}$ *and sufficiently large* $\lambda \in \mathbb{N}$*,*

$$\left|\Pr\left[(\mathsf{crs},\mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda) : \mathcal{A}^{\mathsf{Sign}(\mathsf{crs},\cdot,\cdot,\cdot)}(\mathsf{crs})=1\right] - \Pr\left[(\mathsf{crs},\mathsf{td}) \leftarrow \mathsf{Sim}_0(1^\lambda) : \mathcal{A}^{\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},\cdot,\cdot,\cdot)}(\mathsf{crs})=1\right]\right| \leq \mathsf{negl}(\lambda),$$

where the simulator algorithm Sim_1 *discards its fifth input value.*

Extraction: *Let* $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1)$ *be the simulators given by the simulation property. There exist a* QPT *extractor algorithm* Ext *such that for every* QPT *algorithm* $\mathcal{A}$ *and sufficiently large* $\lambda \in \mathbb{N}$*,*

$$\Pr\left[\begin{array}{c}(\mathsf{crs},\mathsf{td}) \leftarrow \mathsf{Sim}_0(1^\lambda) \\ (x,m,\sigma) \leftarrow \mathcal{A}^{\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},\cdot,\cdot,\cdot)}(\mathsf{crs}) : \\ w \leftarrow \mathsf{Ext}(\mathsf{crs},\mathsf{td},x,m,\sigma)\end{array} \begin{array}{c}\mathsf{Verify}(\mathsf{crs},x,m,\sigma)=1 \\ \wedge\ (x,w)\notin R\ \wedge\ (x,m)\notin Q\end{array}\right] \leq \mathsf{negl}(\lambda).$$

where Q *is the list of queries from* $\mathcal{A}$ *to* Sim_1*.*

Theorem 3.10. *[24,33] Given quantum-secure simulation extractable NIZK for NP, there exists a quantum-secure* SimExt*-secure signature of knowledge.*

4 NIZK Arguments with Certified Deletion

In this section, we introduce the notion of a non-interactive zero-knowledge with certified deletion (NIZK-CD) and define its security properties. This primitive allows to transform any NIZK argument for NP to a NIZK construction where proofs can be deleted by the recipients after being verified, and deletion can be substantiated via a deletion certificate. We provide two different definitions of NIZK-CD. The first one is motivated by simplicity, establishes a single-theorem NIZK-CD, and guarantees that no adversary receiving honestly generated proofs for hard NP instances can output both an accepting proof and a valid deletion certificate. In the second definition, we present a multi-theorem NIZK-CD with a guarantee that from any adversary, even having the oracle access to NIZK-CD simulators, returning both an accepting proof and deletion certificate for some instance, one can extract a valid witness corresponding to the instance.

Definition 4.1. (Hard Distribution) *Given an NP relation* R*, an efficiently samplable distribution* $(\mathcal{X},\mathcal{W})$ *over* R *is hard if for every* QPT *algorithm* $\mathcal{A}$ *and sufficiently large security parameter* λ*,*

$$\Pr[(x,w) \leftarrow (\mathcal{X},\mathcal{W}) : (x,\mathcal{A}(x)) \in R] \leq \mathsf{negl}(\lambda).$$

Definition 4.2. (NIZK with Certified Deletion) *Let any* NP *relation* R *with language* L*.* $\Gamma = \langle \mathsf{Setup},\mathsf{Prove},\mathsf{Verify},\mathsf{Delete},\mathsf{Certify}\rangle$ *is a NIZK-CD if it satisfies the following syntax and properties.*

- $(\mathsf{crs},\mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)$*: on input* λ*, output a classical* crs *and trapdoor* td*.*
- $(\pi,\mathsf{ck}) \leftarrow \mathsf{Prove}(\mathsf{crs},x,w)$*: on input* crs *and a hard NP instance-witness pair* $(x,w)\in\mathcal{R}$*, output a quantum proof* π *and a classical certification key* ck*.*
- $\{0,1\} \leftarrow \mathsf{Verify}(\mathsf{crs},x,\pi)$*: on input* crs*,* x*, and* π*, output accept or reject.*
- $\mathsf{cert} \leftarrow \mathsf{Delete}(\pi)$*: on input* π*, output a classical deletion certificate* cert*.*
- $\{0,1\} \leftarrow \mathsf{Certify}(\mathsf{ck},\mathsf{cert})$*: on input* ck *and* cert*, output accept or reject.*

Perfect Completeness: *For every* $\lambda \in \mathbb{N}$ *and every* $(x, w) \in R$,

$$\Pr\left[\begin{array}{cc} (\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda) & \mathsf{Verify}(\mathsf{crs}, x, \pi) = 1 \\ (\pi, \mathsf{ck}) \leftarrow \mathsf{Prove}(\mathsf{crs}, x, w) : & \wedge \\ \mathsf{cert} \leftarrow \mathsf{Delete}(\pi) & \mathsf{Certify}(\mathsf{ck}, \mathsf{cert}) = 1 \end{array}\right] = 1.$$

Adaptive Computational Soundness: *For every* QPT *algorithm* $\mathcal{A}$ *and a sufficiently large security parameter* λ,

$$\Pr\left[\begin{array}{c} (\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda) \\ (x, \pi) \leftarrow \mathcal{A}(\mathsf{crs}) \end{array} : \ \mathsf{Verify}(\mathsf{crs}, x, \pi) = 1 \wedge x \notin L\right] \leq \mathsf{negl}(\lambda).$$

Adaptive Computational Zero-Knowledge: *There exists a* QPT *algorithm* $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1)$ *such that for every* QPT *algorithm* $\mathcal{A}$, QPT *distinguisher* $\mathcal{D}$, *sufficiently large* λ,

$$\left|\Pr\left[\begin{array}{c} (\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda) \\ (x, w, \xi) \leftarrow \mathcal{A}(\mathsf{crs}) \\ (\pi, \mathsf{ck}) \leftarrow \mathsf{Prove}(\mathsf{crs}, x, w) \end{array} : \mathcal{D}(\mathsf{crs}, x, \pi, \xi) = 1\right] - \right.$$
$$\left.\Pr\left[\begin{array}{c} (\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Sim}_0(1^\lambda) \\ (x, w, \xi) \leftarrow \mathcal{A}(\mathsf{crs}) \\ (\pi, \mathsf{ck}) \leftarrow \mathsf{Sim}_1(\mathsf{crs}, \mathsf{td}, x) \end{array} : \mathcal{D}(\mathsf{crs}, x, \pi, \xi) = 1\right]\right| \leq \mathsf{negl}(\lambda).$$

Deletion Security: *For every* QPT *algorithm* $\mathcal{A}$, *sufficiently large* λ, *and hard distribution* $(\mathcal{X}, \mathcal{W})$ *over* $\mathcal{R}$,

$$\Pr\left[\begin{array}{cc} (\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda) & \mathsf{Verify}(\mathsf{crs}, x, \pi^*) = 1 \\ (x, w) \leftarrow (\mathcal{X}, \mathcal{W}) & \wedge \\ (\pi, \mathsf{ck}) \leftarrow \mathsf{Prove}(\mathsf{crs}, x, w) : & \\ (\pi^*, \mathsf{cert}) \leftarrow \mathcal{A}(\mathsf{crs}, x, \pi) & \mathsf{Certify}(\mathsf{ck}, \mathsf{cert}) = 1 \end{array}\right] \leq \mathsf{negl}(\lambda).$$

We present the definition of multi-theorem simulation-extractable NIZK-CD.

Definition 4.3. (Simulation-Extractable NIZK with Certified Deletion) *Let* R *be an* NP *with language* L. $\Gamma = \langle \mathsf{Setup}, \mathsf{Prove}, \mathsf{Verify}, \mathsf{Delete}, \mathsf{Certify} \rangle$ *is a simulation-extractable NIZK-CD if it satisfies the properties in Definition 4.2 and the following zero-knowledge, simulation extraction, and deletion properties.*

Adaptive Multi-Theorem Computational Zero-Knowledge: *There exists* QPT *simulator algorithm* $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1)$ *such that for every* QPT *algorithm* $\mathcal{A}$ *and sufficiently large* $\lambda \in \mathbb{N}$,

$$\left|\Pr\left[(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda) : \mathcal{A}^{\mathsf{Prove}(\mathsf{crs}, \cdot, \cdot)}(\mathsf{crs}) = 1\right] - \right.$$
$$\left.\Pr\left[(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Sim}_0(1^\lambda) : \mathcal{A}^{\mathsf{Sim}_1(\mathsf{crs}, \mathsf{td}, \cdot, \cdot)}(\mathsf{crs}) = 1\right]\right| \leq \mathsf{negl}(\lambda),$$

where $\mathcal{A}$ *only receives proofs from the oracles, and certifying keys are discarded. Moreover, the simulation algorithm* Sim_1 *discards its fourth input.*

Simulation Extractability: *Let* $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1)$ *be the simulator given by the adaptive multi-theorem computational zero-knowledge property. A* QPT *extractor* Ext *exists where for any* QPT *adversary* $\mathcal{A}$ *and sufficiently large* $\lambda \in \mathbb{N}$*,*

$$\Pr\left[\begin{array}{c}(\mathsf{crs},\mathsf{td}) \leftarrow \mathsf{Sim}_0(1^\lambda)\\ (x,\pi) \leftarrow \mathcal{A}^{\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},\cdot,\cdot)}(\mathsf{crs}) \\ w \leftarrow \mathsf{Ext}(\mathsf{crs},\mathsf{td},x,\pi)\end{array} : \begin{array}{c}\mathsf{Verify}(\mathsf{crs},x,\pi)=1\\ \wedge (x,w)\notin R \wedge x \notin Q\end{array}\right] \leq \mathsf{negl}(\lambda),$$

where Q *is the list of queries from* $\mathcal{A}$ *to* Sim_1*, and* $\mathcal{A}$ *only receives the proof.*

Simulation Extractability with Deletion: *Let* $(\mathsf{Sim}_0, \mathsf{Sim}_1)$ *be simulators given by the multi-theorem zero knowledge. There exists a* QPT *extractor* Ext-Del *s.t. for every* QPT *algorithm* $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ *and every sufficiently large* $\lambda \in \mathbb{N}$*,*

$$\Pr\left[\begin{array}{c}(\mathsf{crs},\mathsf{td}) \leftarrow \mathsf{Sim}_0(1^\lambda)\\ (x,\xi) \leftarrow \mathcal{A}_0^{\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},\cdot,\cdot)}(\mathsf{crs}) \\ (\pi,\mathsf{ck}) \leftarrow \mathsf{Sim}_1(\mathsf{crs},\mathsf{td},x,\perp) \\ (\pi^*,\mathsf{cert}) \leftarrow \mathcal{A}_1^{\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},\cdot,\cdot)}(\mathsf{crs},\xi,x,\pi) \\ w \leftarrow \mathsf{Ext\text{-}Del}(\mathsf{crs},\mathsf{td},x,\pi^*,\mathsf{cert})\end{array} : \begin{array}{c}\mathsf{Verify}(\mathsf{crs},x,\pi^*)=1\\ \wedge \\ [\mathsf{Certify}(\mathsf{ck},\mathsf{cert})=1 \ \vee \ (x,w)\notin R] \wedge \ x \notin Q\end{array}\right] \leq \mathsf{negl}(\lambda),$$

where Q *is the list of queries, and* $\mathcal{A}$ *only receives the proof from the oracle* Sim_1*.*

Remark 4.1. In our constructions, Setup and Certify are classical while Prove, Verify, and Delete are quantum algorithms. Moreover, the Prove algorithm might be interactive between a classical prover and a quantum verifier, i.e., the prover remotely prepares required quantum states in the verifier's device.

We note that the connection between different notions of zero-knowledge, soundness, and extraction for NIZK arguments that are described in Remark 3.1 also holds for NIZK-CD. The following states that the simulation extractability with deletion implies both simulation extractibility and deletion security.

Theorem 4.1. *Simulation extractability with deletion defined in Definition 4.3 implies simulation extractibility as defined in Definition 4.3 and deletion security as defined in Definition 4.2.*

Proof. First, consider an adversary $\mathcal{B}$ that breaks simulation extractibility with a non-negligible advantage. One can build an adversary $\mathcal{A} = (A_0, A_1)$ that breaks simulation extractibility with deletion with the same advantage. In particular, A_0 runs B to get an instance x and a corresponding proof π^*. The instance x is submitted to the simulator Sim_1, and π^* is included in ξ. The algorithm A_1 receives a proof π from Sim_1, which can be deleted to generate a valid deletion

certificate cert. Afterwards, A_1 can return produced cert as a valid certificate and π^* included in ξ as an accepting proof corresponding to the instance x.

Similarly, consider an adversary $\mathcal{B}$ that can break the deletion security with a non-negligible advantage. One can build an adversary $\mathcal{A} = (A_0, A_1)$ where A_0 samples a hard instance x and submits it to Sim_1. A_1 receives a proof π corresponding to the instance x from the oracle. Then, A_1 runs B on input x and π to get a valid deletion certificate and an accepting transcript where the success probability is the same as the success probability of $\mathcal{B}$. □

5 Constructions of NIZK-CD from Standard Assumptions

In this section, we propose NIZK-CD constructions from standard cryptographic assumptions. First, we propose a construction where the required assumption is a quantum-hard one-way function. Second, we replace quantum communication with entirely classical communication under the standard LWE assumption.

5.1 NIZK-CD from OWF with Classical Certificates

We show that NIZK-CD can be constructed from one-way functions.

Theorem 5.1. *Assuming quantum-hard one-way functions and quantum-secure simulation-extractable NIZK, there exists a simulation-extractable NIZK-CD.*

Proof. Assume $\Sigma = \langle \mathsf{Setup}, \mathsf{Com} \rangle$ to be a quantum secure, statistically binding and computationally hiding which can be realized from one-way functions [26], and $\Pi = \langle \mathsf{Setup}, \mathsf{Prove}, \mathsf{Verify} \rangle$ to be any simulation-extractable NIZK. Our NIZK-CD construction is as follows.

- $(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)$: $\mathsf{crs}_\Sigma, \mathsf{td}_\Sigma \leftarrow \Sigma.\mathsf{Setup}(1^\lambda)$ and $\mathsf{crs}_\Pi, \mathsf{td}_\Pi \leftarrow \Pi.\mathsf{Setup}(1^\lambda)$, and output the parameters $\mathsf{crs} := (\mathsf{crs}_\Sigma, \mathsf{crs}_\Pi)$ and $\mathsf{td} := (\mathsf{td}_\Sigma, \mathsf{td}_\Pi)$.
- $(\pi, \mathsf{ck}) \leftarrow \mathsf{Prove}(\mathsf{crs}, x, w)$: For $n(\lambda), \ell(\lambda)$, sample randomness $r_{i,b} \leftarrow \{0,1\}^{\ell(\lambda)}$, and $\forall i \in [n], \forall b \in \{0,1\}$ compute $c_{i,b} = \mathsf{Com}(\mathsf{crs}_\Sigma, b^{n(\lambda)}, r_{i,b})$. Then, given the instance $x^* := (x, \{c_{i,b}\}_{i\in[n],b\in\{0,1\}})$ and witness $w^* := (w, \{r_{i,b}\}_{i\in[n],b\in\{0,1\}})$, invoke $\Pi.\mathsf{Prove}(\mathsf{crs}, x^*, w^*)$ and generate a NIZK proof σ for the relation R^*,

$$(x, w) \in R \quad \bigvee_{i\in[n]} \quad \wedge_{b\in\{0,1\}} c_{i,b} = \mathsf{Com}(\mathsf{crs}_\Sigma, (1-b)^{n(\lambda)}, r_{i,b}). \tag{1}$$

  Given uniform bits $u_i \leftarrow \{0,1\}$ for all $i \in [n]$, prepare

$$|\psi\rangle := \bigotimes_{i\in[n]} \frac{1}{\sqrt{2}} \left(|0\rangle|r_{i,0}\rangle + (-1)^{u_i}|1\rangle|r_{i,1}\rangle\right). \tag{2}$$

  Output $\pi := (\{c_{i,b}\}_{i\in[n],b\in\{0,1\}}, \sigma, |\psi\rangle)$ and $\mathsf{ck} := \{u_i, r_{i,b}\}_{i\in[n],b\in\{0,1\}}$.

- $\{0,1\} \leftarrow \mathsf{Verify}(\mathsf{crs}, x, \pi)$: Parse π as $\{c_{i,b}\}_{i\in[n],b\in\{0,1\}}, \sigma, |\psi\rangle$, run the verifier $v_\sigma \leftarrow \Pi.\mathsf{Verify}(\mathsf{crs}, x^*, \sigma)$, where $x^* := (x, \{c_{i,b}\}_{i\in[n],b\in\{0,1\}})$. Let $U^{\mathsf{com}}_{c_0,c_1}$ be a unitary operation with respect to the commitments c_0 and c_1 as follows.

$$|b\rangle|r\rangle|0\rangle \xrightarrow{U^{\mathsf{com}}_{c_0,c_1}} |b\rangle|r\rangle|\mathsf{Cmt} - \mathsf{Cmp}(\mathsf{crs}_\Sigma, b, r, c_b)\rangle, \tag{3}$$

where the commit-and-compare function is defined as below.

$$\mathsf{Cmt} - \mathsf{Cmp}(\mathsf{crs}_\Sigma, b, r, c_b) = \begin{cases} 1, & \mathsf{Com}(\mathsf{crs}_\Sigma, b^{n(\lambda)}, r) = c_b \\ 0, & \text{Otherwise} \end{cases} \tag{4}$$

Add ancilla qubits, and apply $U = \bigotimes_{i\in[n]} U^{\mathsf{com}}_{c_{i,0},c_{i,1}}$ to $|\psi\rangle$,

$$\begin{aligned} &\xrightarrow{U} \bigotimes_{i\in[n]} \frac{1}{\sqrt{2}}(|0\rangle|r_{i,0}\rangle|\mathsf{Cmt} - \mathsf{Cmp}(\mathsf{crs}_\Sigma, 0, r_{i,0}, c_{i,0})\rangle \\ &+ (-1)^{u_i}|1\rangle|r_{i,1}\rangle|\mathsf{Cmt} - \mathsf{Cmp}(\mathsf{crs}_\Sigma, 1, r_{i,1}, c_{i,1})\rangle). \end{aligned} \tag{5}$$

$\forall i \in [n]$, measure the right-most registers $v_i = \mathsf{Cmt} - \mathsf{Cmp}(\mathsf{crs}_\Sigma, 0, r_{i,0}, c_{i,0})$. Output $v = v_\sigma \bigwedge_{i\in[n]} v_i$, where $v = 1$ indicates accept and $v = 0$ otherwise.

- $\mathsf{cert} \leftarrow \mathsf{Delete}(\pi)$: Parse π as $\{c_{i,b}\}_{i\in[n],b\in\{0,1\}}, \sigma, |\psi\rangle = \bigotimes_{i\in[n]}|\psi_i\rangle$ such that $|\psi_i\rangle = \sum_{b\in\{0,1\}} \frac{1}{\sqrt{2}}(-1)^{b\cdot u_i}|b\rangle|r_{i,b}\rangle$. $\forall i \in [n]$, measure each state $|\psi_i\rangle$ in the Hadamard basis, yielding an outcome string $d_i \in \{0,1\}^{\ell(\lambda)}$ such that it holds that $d_i \cdot (r_{i,0} \oplus r_{i,1}) = u_i$. We define the deletion certificate $\mathsf{cert} := \{d_i\}_{i\in[n]}$.
- $\{0,1\} \leftarrow \mathsf{Certify}(\mathsf{ck}, \mathsf{cert})$: Parse ck as $\{u_i, r_{i,b}\}_{i\in[n],b\in\{0,1\}}$ and cert as $\{d_i\}_{i\in[n]}$. Validate whether for all $i \in [n]$ it holds that $d_i \cdot (r_{i,0} \oplus r_{i,1}) = u_i$.

Next, we prove each of the security properties of the proposed construction.

Perfect Completeness: Completeness must be shown with respect to both proof verification and certificate validation. Consider the former case. Following the perfect completeness of Π, we ensure that the proof σ is accepting and $v_\sigma = 1$ with a probability of 1. Then, it suffices to show that for all $i \in [n]$, $v_i = 1$. As the commitment algorithm Com is deterministic, and the commitments are generated honestly, i.e., $c_i = \mathsf{Com}(\mathsf{crs}_\Sigma, b_i^{n(\lambda)}, r_{i,b})$, we ensure that $\forall i \in [n]$ and $\forall b \in \{0,1\}$, we have $\mathsf{Cmt} - \mathsf{Cmp}(\mathsf{crs}_\Sigma, b_i, r_{i,b}, c_{i,b}) = 1$. Therefore, the bit v_i is measured as one with a probability of 1. Consider completeness with respect to deletion. We parse the sate $|\psi\rangle$ as $\bigotimes_{i\in[n]}|\psi_i\rangle$, s.t. $|\psi_i\rangle = \sum_{b\in\{0,1\}} \frac{1}{\sqrt{2}}(-1)^{b\cdot u_i}|b\rangle|r_{i,b}\rangle$. The verifier measures each $|\psi_i\rangle$ in the Hadamard basis, which yields an outcome string $d_i \in \{0,1\}^{\ell(\lambda)}$, and it holds that $u_i = d_i \cdot (r_{i,0} \oplus r_{i,1})$. Therefore, the $\mathsf{Certify}$ algorithm always accepts the deletion certificate cert.

Adaptive Multi-Theorem Computational Zero-Knowledge: Consider the simulators $\Pi.Sim = (\Pi.Sim_0, \Pi.\mathsf{Sim}_1)$. We then show $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1)$ for adaptive multi-theorem computational zero-knowledge of our construction.

- $(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Sim}_0(1^\lambda)$: Run the algorithms $(\mathsf{crs}_\Pi, \mathsf{td}_\Pi) \leftarrow \Pi.\mathsf{Sim}_1(1^\lambda)$ and $(\mathsf{crs}_\Sigma, \mathsf{td}_\Sigma) \leftarrow \Sigma.\mathsf{Setup}(1^\lambda)$. Output $\mathsf{crs} := (\mathsf{crs}_\Pi, \mathsf{crs}_\Sigma)$ and $\mathsf{td} := (\mathsf{td}_\Pi, \mathsf{td}_\Sigma)$.

- $(\pi, \mathsf{ck}) \leftarrow \mathsf{Sim}_1(\mathsf{crs}, \mathsf{td}, x)$: Sample $r'_{i,b} \leftarrow \{0,1\}^{\ell(\lambda)}$ and $\forall i \in [n], \forall b \in \{0,1\}$ compute $c'_{i,b} = \mathsf{Com}(\mathsf{crs}_\Sigma, b^{n(\lambda)}, r'_{i,b})$. Given $x^* := (x, \{c'_{i,b}\}_{i\in[n],b\in\{0,1\}})$, query $\Pi.\mathsf{Sim}_1$ on input x^* to get σ'. Sample $u'_i \leftarrow \{0,1\}$, prepare $|\psi'\rangle$, and output the proof $\pi := (\{c'_{i,b}\}_{i\in[n],b\in\{0,1\}}, \sigma', |\psi'\rangle)$ and certificate $\mathsf{ck} := \{u'_i, r'_{i,b}\}_{i\in[n],b\in\{0,1\}}$.

Reduction: Suppose that there exists a QPT adversary algorithm $\mathcal{A}$ such that for some polynomial $p(\lambda)$,

$$\Big| \Pr\Big[\mathsf{crs}, \mathsf{td} \leftarrow \mathsf{Setup}(1^\lambda) : \mathcal{A}^{\mathsf{Prove}(\mathsf{crs},\cdot,\cdot)}(\mathsf{crs}) = 1\Big] - \Pr\Big[\mathsf{crs}, \mathsf{td} \leftarrow \mathsf{Sim}_0(1^\lambda) : \mathcal{A}^{\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},\cdot,\cdot)}(\mathsf{crs}) = 1\Big] \Big| \geq \frac{1}{p(\lambda)}.$$

We construct a QPT adversary $\mathcal{B}$ for the adaptive multi-theorem computational zero-knowledge property of the underlying NIZK Π as follows.

1. Receive crs_Π from $\Pi.\mathsf{Setup}$ or $\Pi.\mathsf{Sim}_0$, crs_Σ from $\Sigma.\mathsf{Setup}$, and then send $\mathsf{crs} := (\mathsf{crs}_\Pi, \mathsf{crs}_\Sigma)$ to the adversary $\mathcal{A}$.

2. For each query (x, w), $r_{i,b} \leftarrow \{0,1\}^{\ell(\lambda)}$, $c_{i,b} = \mathsf{Com}(\mathsf{crs}_\Sigma, b^{n(\lambda)}, r_{i,b})$ for all $i \in [n]$ and $b \in \{0,1\}$. Then, given instance $x^* := (x, \{c_{i,b}\}_{i\in[n],b\in\{0,1\}})$ and witness $w^* := (w, \{r_{i,b}\}_{i\in[n],b\in\{0,1\}})$, receive the real or simulated proof σ by query either Prove on input (x^*, w^*) or $\Pi.\mathsf{Sim}_1$ on input x^*. Moreover, sample bits $u_i \leftarrow \{0,1\}$ and prepares $|\psi\rangle$ as defined in Equation 2. The proof $\pi = \{c_{i,b}\}_{i\in[n],b\in\{0,1\}}, \sigma, |\psi\rangle$ is sent to the adversary algorithm $\mathcal{A}$.

3. Output the result of $\mathcal{A}$.

As commitment randomnesses $\{r_{i,b}\}_{i\in[n],b\in\{0,1\}}$ and exponents $\{u_i\}_{i\in[n],b\in\{0,1\}}$ are uniformly sampled, the real and simulated quantum states, i.e., $|\psi\rangle$ and $|\psi'\rangle$, respectively, are statistically indistinguishable. Moreover, computational hiding of the commitment scheme Com ensures that two sets $\{c_{i,b}\}_{i\in[n],b\in\{0,1\}}$ and $\{c'_{i,b}\}_{i\in[n],b\in\{0,1\}}$ are computationally indistinguishable. Thus, $\mathcal{B}$ would have a similar and non-negligible polynomial advantage to $\mathcal{A}$ in breaking the adaptive multi-theorem computational zero-knowledge property of Π, i.e., $\frac{1}{p(\lambda)} - \mathsf{negl}(\lambda)$.

Simulation Extractability with Deletion: One can view the commitment algorithm $\mathsf{Com} : \{0,1\}^{\ell(\lambda)+1}$ as one-way function. Assume that there exists an adversary that, on input $\mathsf{Com}(\mathsf{crs}_\Sigma, b^{n(\lambda)}, r)$, can invert the function and extract b and r with a non-negligible probability. Then, the adversary can break the

hiding or binding properties with the same advantage. Lemma 3.6 implies that,

$$\Pr\left[\begin{array}{c}\forall i\in[n]: r_{i,0}, r_{i,1}\leftarrow\{0,1\}^{2\ell(\lambda)}, u_i\leftarrow\{0,1\}\\ \forall i\in[n]: c_{i,0}=\mathsf{Com}(\mathsf{crs}_\Sigma, 0^{n(\lambda)}, r_{i,0})\wedge c_{i,1}=\mathsf{Com}(\mathsf{crs}_\Sigma, 1^{n(\lambda)}, r_{i,1}) :\\ \{(b_i,r_i,d_i)\}_{i\in[n]}\leftarrow\mathcal{A}(\otimes_{i\in[n]}\frac{|0,r_{i,0}\rangle+(-1)^{u_i}|1,r_{i,1}\rangle}{\sqrt{2}}, \{c_{i,b}\}_{i,b})\\ \wedge_{i\in[n]}\mathsf{Com}(\mathsf{crs}_\Sigma, b_i^{n(\lambda)}, r_i)\in\{c_{i,0},c_{i,1}\}\\ \wedge\\ \wedge_{i\in[n]} d_i\cdot(r_{i,0}\oplus r_{i,1})=u_i\end{array}\right]\leq\mathsf{negl}(\lambda)$$

Let $\Pi.\mathsf{Sim}=(\Pi.\mathsf{Sim}_0,\Pi.\mathsf{Sim}_1)$ be the simulators of Π and $\mathsf{Sim}=(\mathsf{Sim}_0,\mathsf{Sim}_1)$ be the simulators of our construction given by the corresponding multi-theorem zero-knowledge. Let $\Pi.\mathsf{Ext}$ be the extractor given by the simulation extractibility of Π. We show an extractor $\mathsf{Ext\text{-}Del}$ that satisfies simulation extractibility with deletion for our proposed construction as follows.

1. On input crs, td, x, π, and cert, parse the proof π as $\{c_{i,b}\}_{i\in[n],b\in\{0,1\}},\sigma,|\psi\rangle$.
2. Query $\Pi.\mathsf{Ext}$ on input x^* and σ and receive the witness w^*.
3. Output w^* as w.

Reduction: Consider the case that simulation extractibility with deletion does not hold, i.e., there exists a QPT adversary algorithm $A=(A_0,A_1)$ such that given the extractor $\mathsf{Ext\text{-}Del}$, and some polynomial $p(\lambda)$,

$$\Pr\left[\begin{array}{c}(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Sim}_0(1^\lambda)\\ (x,\xi)\leftarrow\mathcal{A}_0^{\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},\cdot,\cdot)}(\mathsf{crs})\\ (\pi,\mathsf{ck})\leftarrow\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},x)\\ (\pi^*,\mathsf{cert})\leftarrow\mathcal{A}_1^{\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},\cdot,\cdot)}(\mathsf{crs},\xi,x,\pi)\\ w\leftarrow\mathsf{Ext\text{-}Del}(\mathsf{crs},\mathsf{td},x,\pi^*,\mathsf{cert})\end{array}\right. :$$

$$\left.\begin{array}{c}\mathsf{Verify}(\mathsf{crs},x,\pi^*)=1\\ \wedge\\ [\mathsf{Certify}(\mathsf{ck},\mathsf{cert})=1\ \vee\ (x,w)\notin R]\wedge\ x\notin Q\end{array}\right]\geq\frac{1}{p(\lambda)},$$

Since Sim_1 forwards queries to $\Pi.\mathsf{Sim}_1$, we know that x^* is not queried to $\Pi.\mathsf{Sim}_1$. We parse π^* as $\{c_{i,b}\}_{i\in[n],b\in\{0,1\}},\sigma,|\psi\rangle$. Since $\mathsf{Verify}(\mathsf{crs},x,\pi^*)=1$, we know that $v_\sigma=\Pi.\mathsf{Verify}(\mathsf{crs}_\Pi,x^*,\sigma)=1$. The witness w^* returned by $\Pi.\mathsf{Ext}$ is a valid witness for R^*. Thus, w^* must include w s.t. $(x,w)\in R$, or, for an $i\in[n]$, it includes $\{r_{i,b}\}_{b\in\{0,1\}}$ s.t. $c_{i,0}=\mathsf{Com}(\mathsf{crs}_\Sigma,1^{n(\lambda)},r_{i,0})$ and $c_{i,1}=\mathsf{Com}(\mathsf{crs}_\Sigma,0^{n(\lambda)},r_{i,1})$. As $\mathsf{Verify}(\mathsf{crs},x,\pi^*)=1$, we can conclude that the measurement outcomes are accepted, i.e., $v_i=1$ for all $i\in[n]$. According to the definition of U in Equation 5, each commitment $c_{i,b}$ is statistically bound to the message b. Thus, w^* must include a satisfying witness w for R; otherwise, the statistical binding property of the commitment scheme can be broken by running

Ext-Del to obtain one of the openings and measuring $|\psi\rangle$ in the standard basis to obtain the other opening for the same commitment value.

Then, as $(x, w) \in R$, the adversary needs to output a valid $\mathsf{cert} = \{d_i\}_{i\in[n]}$ to pass the experiment, that is, $\forall i \in [n], d_i \cdot (r_{i,0} \oplus r_{i,1}) = u_i$. In this case, measuring $|\psi\rangle$ in the standard basis yields $\{r_{i,b}\}_{i\in[n]}$ such that $c_{i,0} = \mathsf{Com}(\mathsf{crs}_\Sigma, b^{n(\lambda)}, r_{i,b})$; This contradicts the adaptive hard-core bit property. More precisely, we can build an algorithm $\mathcal{B}$ to break adaptive hard-core bit, where on input $\{c_{i,b}\}_{i\in[n],b\in\{0,1\}}$, $|\psi\rangle = \otimes_{i\in[n]} \frac{|r_{i,0}\rangle + (-1)^{u_i}|r_{i,1}\rangle}{\sqrt{2}}$, for an instance x, queries $x^* = (x, \{c_{i,b}\}_{i\in[n],b\in\{0,1\}})$ to $\Pi.\mathsf{Sim}_1$ and obtains a proof σ, generates $\pi := (\{c_{i,b}\}_{i\in[n],b\in\{0,1\}}, \sigma, |\psi\rangle)$, and queries (x, π) to $\mathcal{A}_1$ to receive an accepting proof π^* and a valid certificate cert. $\mathcal{B}$ can parse π^* as $\{c^*_{i,b}\}_{i\in[n],b\in\{0,1\}}, \sigma^*, |\psi^*\rangle$ and cert as $\{d_i\}_{i\in[n]}$. Measuring $|\psi^*\rangle$ in the standard basis yields $\{r^*_i\}_{i\in[n]}$ such that $c^*_{i,0} = \mathsf{Com}(\mathsf{crs}_\Sigma, 0^{n(\lambda)}, r^*_i)$ or $c^*_{i,1} = \mathsf{Com}(\mathsf{crs}_\Sigma, 1^{n(\lambda)}, r^*_i)$. $\mathcal{B}$ returns $\{(b_i, r^*_i, d_i)\}_{i\in[n]}$ to pass the experiment.

As we see, having $\mathcal{A}$, one can attack the binding property of the commitment scheme, simulation extractability of Π, or adaptive hard-core bit property of the commitments with advantage $\geq \frac{1}{p(\lambda)} - \mathsf{negl}(\lambda)$. □

5.2 NIZK-CD from LWE with Classical Communication

In this section, we show that our NIZK-CD with classical communication.

Theorem 5.2. *Assuming quantum hardness of LWE and any quantum-secure simulation-extractable NIZK, there exists a simulation-extractable NIZK-CD s.t. the entire communication and the prover algorithm are classical.*

Proof. It is well known [38] that, given LWE, there exists a statistically binding, computationally hiding, and computationally equivocal commitment, which we denote by $\Sigma = \langle \mathsf{Setup}, \mathsf{Com}\rangle$. Let $\mathcal{F} := \{f_{k,b} : \mathcal{X} \to \mathcal{D}_\mathcal{Y}\}_{k\in\mathcal{K},b\in\{0,1\}}$ be an NTCF family. Let $\Pi = \langle \mathsf{Setup}, \mathsf{Prove}, \mathsf{Verify}\rangle$ be a simulation-extractable NIZK. Our NIZK-CD construction with classical communication is described as follows.

- $(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)$: $\mathsf{crs}_\Sigma, \mathsf{td}_\Sigma \leftarrow \Sigma.\mathsf{Setup}(1^\lambda)$ and $\mathsf{crs}_\Pi, \mathsf{td}_\Pi \leftarrow \Pi.\mathsf{Setup}(1^\lambda)$, and output the parameters $\mathsf{crs} := (\mathsf{crs}_\Sigma, \mathsf{crs}_\Pi)$ and $\mathsf{td} := (\mathsf{td}_\Sigma, \mathsf{td}_\Pi)$.
- $(\mathsf{ck}, \pi) \leftarrow \mathsf{Prove}(\mathsf{crs}, x, w)$: For $n(\lambda), \ell(\lambda)$, it proceeds in two phases.

  State Preparation: Executed interactively between the prover and the verifier.
  1. The prover runs $\mathsf{NTCF.Gen}_\mathcal{F}$, generates keys $\{k_i\}_{i\in[n]}$, trapdoors $\{\mathsf{td}_{k_i}\}_{i\in[n]}$, and sends the keys to the verifier. The verifier prepares the following state.

$$|\phi\rangle := \bigotimes_{i\in[n]} \frac{1}{\sqrt{|\mathcal{X}|}} \sum_{x\in\mathcal{X}} |0\rangle|x\rangle + |1\rangle|x\rangle \tag{6}$$

  From Definition 3.2, $|\phi'\rangle$ can be turned into the following superposition.

$$\begin{aligned}|\phi'\rangle := \bigotimes_{i\in[n]} \frac{1}{\sqrt{2|\mathcal{X}|}} \sum_{x\in\mathcal{X},y\in\mathcal{Y}} \sqrt{(f'_{k_i,0}(x))(y)}|0\rangle|x\rangle|y\rangle \\ + \frac{1}{\sqrt{2|\mathcal{X}|}} \sum_{x\in\mathcal{X},y\in\mathcal{Y}} \sqrt{(f'_{k_i,1}(x))(y)}|1\rangle|x\rangle|y\rangle\end{aligned} \tag{7}$$

The verifier measures images, i.e., $|y\rangle$, in the standard basis, yielding,

$$\bigotimes_{i\in[n]} \frac{1}{\sqrt{2}}\left(|0\rangle|x_{i,0}\rangle + |1\rangle|x_{i,1}\rangle\right) \tag{8}$$

Here, for all $i \in [n]$, the tuple $(x_{i,0}, x_{i,1}) \in \mathcal{X}^2$ is a claw with respect to the measured image $y_i \in \mathcal{Y}$. Finally, the verifier sends the images $\{y_i\}_{i\in[n]}$ to the prover and applies the injection $J : \mathcal{X} \to \{0,1\}^{\ell(\lambda)}$, as defined in Definition 3.2, in the above superposition and prepares the state $|\psi\rangle$ as

$$\begin{aligned} |\psi\rangle &:= \bigotimes_{i\in[n]} \frac{1}{2}\left(|0\rangle|r_{i,0}\rangle + |1\rangle|r_{i,1}\rangle\right) \\ &\forall i \in [n], b \in \{0,1\} : r_{i,b} = J(x_{i,b}). \end{aligned} \tag{9}$$

2. For all $i \in [n]$, $b \in \{0,1\}$, prover runs $\mathsf{Inv}(\mathsf{td}_k, b, y_i)$ and $J(x_{i,b})$ to get $r_{i,b}$.

Proof Generation: The remaining parts are similar to Section 5.1. The prover generates commitments $\forall i \in [n], \forall b \in \{0,1\}, c_{i,b} = \mathsf{Com}(\mathsf{crs}_\Sigma, b^{n(\lambda)}, r_{i,b})$. Given $x^* := (x, \{c_{i,b}\}_{i\in[n],b\in\{0,1\}})$, $w^* := (w, \{r_{i,b}\}_{i\in[n],b\in\{0,1\}})$, the prover runs $\Pi.\mathsf{Prove}(\mathsf{crs}, x^*, w^*)$ and generates a NIZK proof σ for R^*, as defined in Equation 1. Output $\pi = \{c_{i,b}\}_{i\in[n],b\in\{0,1\}}, \sigma, |\psi\rangle$ and $\mathsf{ck} = \{r_{i,b}\}_{i\in[n],b\in\{0,1\}}$.

- $\{0,1\} \leftarrow \mathsf{Verify}(\mathsf{crs}, x, \pi)$: The verifier runs $v_\sigma \leftarrow \Pi.\mathsf{Verify}(\mathsf{crs}, x^*, \sigma)$. Let $U^{\mathsf{com}}_{c_0,c_1}$ and U be as before, i.e., Equation 3. Using U, the state in Equation 5 is prepared. Then, the verifier for all $i \in [n]$, measures the commit-and-compare registers $v_i = \mathsf{Cmt} - \mathsf{Cmp}(\mathsf{crs}_\Sigma, 0, r_{i,0}, c_{i,0})$. The outcome is $v = v_\sigma \bigwedge_{i\in[n]} v_i$.

- $\mathsf{cert} \leftarrow \mathsf{Delete}(\pi)$: The proof π is parsed as $\{c_{i,b}\}_{i\in[n],b\in\{0,1\}}, \sigma, |\psi\rangle$ and also the state $|\psi\rangle$ as $\bigotimes_{i\in[n]}|\psi_i\rangle$ such that $|\psi_i\rangle = \sum_{b\in\{0,1\}} \frac{1}{2}|b\rangle|r_{i,b}\rangle$. The verifier then for all $i \in [n]$ measures the state $|\psi_i\rangle$ in the Hadamard basis to get strings $d_i \in \{0,1\}^{\ell(\lambda)}$ such that $d_i \cdot (r_{i,0} \oplus r_{i,1}) = 0$. We define $\mathsf{cert} := \{d_i\}_{i\in[n]}$.

- $\{0,1\} \leftarrow \mathsf{Certify}(\mathsf{ck}, \mathsf{cert})$: The key ck is parsed as $\{r_{i,b}\}_{i\in[n],b\in\{0,1\}}$ and cert as $\{d_i\}_{i\in[n]}$. Validate whether for all $i \in [n]$ it holds $d_i \cdot (r_{i,0} \oplus r_{i,1}) = 0$.

Then, we prove each of the security properties of our NIZK-CD. Reductions for perfect completeness, adaptive multi-theorem computational zero-knowledge, and simulation extractability with deletion work basically similar to Section 5.1.

Perfect Completeness: Again, we first show completeness with respect to proof verification and then certificate validation. Consider the former case. The perfect completeness of Π ensures that $v_\sigma = 1$ with a probability of 1. As the inversion function Inv and the map J are deterministic, the randomnesses computed by the prover using trapdoor td_k and the map J are the same as the randomnesses encoded in the state $|\psi\rangle$. Moreover, as Com is deterministic and the commitments are generated honestly, we have $\mathsf{Cmt} - \mathsf{Cmp}(\mathsf{crs}_\Sigma, b_i, r_{i,b}, c_{i,b}) = 1$. For all $i \in [n]$, v_i is measured as 1. For completeness with respect to deletion, we

have $|\psi\rangle = \bigotimes_{i\in[n]}|\psi_i\rangle$, s.t. $|\psi_i\rangle = \sum_{b\in\{0,1\}} \frac{1}{2}|b\rangle|r_{i,b}\rangle$. The verifier measures each $|\psi_i\rangle$ in the Hadamard basis to obtain $d_i \in \{0,1\}^{\ell(\lambda)}$, where $d_i \cdot (r_{i,0} \oplus r_{i,1}) = 0$.

Adaptive Multi-Theorem Computational Zero-Knowledge: Algorithms $\Pi.\mathsf{Sim} = (\Pi.\mathsf{Sim}_0, \Pi.\mathsf{Sim}_1)$ are simulators of Π. $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1)$ is as:

- $(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Sim}_0(1^\lambda)$: Run the algorithms $(\mathsf{crs}_\Pi, \mathsf{td}_\Pi) \leftarrow \Pi.\mathsf{Sim}_1(1^\lambda)$ and $(\mathsf{crs}_\Sigma, \mathsf{td}_\Sigma) \leftarrow \Sigma.\mathsf{Setup}(1^\lambda)$. Output $\mathsf{crs} := (\mathsf{crs}_\Pi, \mathsf{crs}_\Sigma)$ and $\mathsf{td} := (\mathsf{td}_\Pi, \mathsf{td}_\Sigma)$.
- $(\pi, \mathsf{ck}) \leftarrow \mathsf{Sim}_1(\mathsf{crs}, \mathsf{td}, x)$: Run $\mathsf{NTCF.Gen}_\mathcal{F}$, generate $\{k'_i\}_{i\in[n]}$, $\{\mathsf{td}_{k'_i}\}_{i\in[n]}$, and send the key k' to the adversary. For all $i \in [n]$, on input the image $y'_i \in \mathcal{Y}$, compute $x'_{i,0} \leftarrow \mathsf{Inv}(\mathsf{td}_{k'}, 0, y'_i)$ and $x'_{i,1} \leftarrow \mathsf{Inv}(\mathsf{td}_{k'}, 1, y'_i)$, and the randomnesses $r'_{i,0} = J(x'_{i,0})$ and $r'_{i,1} = J(x'_{i,1})$. Compute $\forall i \in [n], \forall b \in \{0,1\}$, $c'_{i,b} = \mathsf{Com}(\mathsf{crs}_\Sigma, b^{n(\lambda)}, r'_{i,b})$. Let $x^* := (x, \{c'_{i,b}\}_{i\in[n],b\in\{0,1\}})$. Query $\Pi.\mathsf{Sim}_1$ on input x^* to get a proof σ'. Prepare $|\psi'\rangle$, as in Equation 9, and output the proof $\pi := (\{c'_{i,b}\}_{i\in[n],b\in\{0,1\}}, \sigma', |\psi'\rangle)$ and the certificate $\mathsf{ck} := \{u'_i, r'_{i,b}\}_{i\in[n],b\in\{0,1\}}$.

  Reduction: It proceeds similarly to the reduction in Section 5.1. The additional note is that the keys k' are uniformly sampled by $\mathsf{NTCF.Gen}_\mathcal{F}$; therefore, they are indistinguishable from the real key k.

Simulation Extractability with Deletion: We can build an extractor $\mathsf{Ext\text{-}Del}$ that satisfies simulation extractibility with deletion and present the reduction the same as Section 5.1. The adaptive hard-core bit property of NTCF hash functions, as defined in Definition 3.2, prevents the adversary from deviating from the protocol. Otherwise, one can use adversary $\mathcal{A}$ to violate at least one of these properties: the statistical binding of the commitment, the simulation extractability of Π, or the adaptive hard-core bit of the NTCF functions. □

6 Revocable Signatures of Knowledge and Credentials

In this section, we discuss several applications of NIZK-CD including revocable signature of knowledge and revocable anonymous credentials.

6.1 Revocable Signature of Knowledge

We present the definition and construction of revocable signature of knowledge.

Definition 6.1. (Revocable Signature of Knowledge) *Let* NP *relation* R *with language* L *and message space* $\mathcal{M}$. $\Sigma_R = \langle \mathsf{Setup}, \mathsf{Sign}, \mathsf{Verify}, \mathsf{Delete}, \mathsf{Certify} \rangle$ *is a revocable signature of knowledge if it satisfies the following.*

- $(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)$: *on input* λ*, output* crs *and trapdoor* td.
- $(\sigma, \mathsf{ck}) \leftarrow \mathsf{Sign}(\mathsf{crs}, x, w, m)$: *on input* crs, $(x, w) \in R$, $m \in \mathcal{M}$*, output a signature of knowledge* σ *and a certification key* ck.
- $\{0,1\} \leftarrow \mathsf{Verify}(\mathsf{crs}, x, m, \sigma)$: *on input* crs, x, m, σ*, accept or reject.*

- $\mathsf{cert} \leftarrow \mathsf{Delete}(\sigma)$*: on input* σ*, output a deletion certificate* cert*.*
- $\{0,1\} \leftarrow \mathsf{Certify}(\mathsf{ck}, \mathsf{cert})$*: on input* ck *and* cert*, output accept or reject.*

Correctness: *For every* $\lambda \in \mathbb{N}$*, pair* $(x, w) \in R$ *and message* $m \in \mathcal{M}$*,*

$$\Pr\left[\begin{array}{c} \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda) \\ (\sigma, \mathsf{ck}) \leftarrow \mathsf{Sign}(\mathsf{crs}, x, w, m) \\ \mathsf{cert} \leftarrow \mathsf{Delete}(\sigma) \end{array} : \begin{array}{c} \mathsf{Verify}(\mathsf{crs}, x, m, \sigma) = 1 \\ \wedge \\ \mathsf{Certify}(\mathsf{ck}, \mathsf{cert}) = 1 \end{array}\right] = 1.$$

Simulation: *There exist a* QPT *simulator algorithm* $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1)$ *such that for every* QPT *algorithm* $\mathcal{A}$ *and sufficiently large* $\lambda \in \mathbb{N}$*,*

$$\begin{aligned} &\Big|\Pr\left[\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda) : \mathcal{A}^{\mathsf{Sign}(\mathsf{crs},\cdot,\cdot,\cdot)}(\mathsf{crs}) = 1\right] - \\ &\Pr\left[(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Sim}_0(1^\lambda) : \mathcal{A}^{\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},\cdot,\cdot,\cdot)}(\mathsf{crs}) = 1\right]\Big| \leq \mathsf{negl}(\lambda). \end{aligned}$$

where Sim_1 *discards its fifth input value.*

Extraction with Deletion: *Let* $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1)$ *be from the simulation property. There exists a* QPT *extractor algorithm* Ext-Del *such that for every* QPT *algorithm* $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ *and sufficiently large* $\lambda \in \mathbb{N}$*,*

$$\Pr\left[\begin{array}{c} (\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Sim}_0(1^\lambda) \\ (x, m) \leftarrow \mathcal{A}_0^{\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},\cdot,\cdot)}(\mathsf{crs}) \\ (\sigma, \mathsf{ck}) \leftarrow \mathsf{Sim}_1(\mathsf{crs}, \mathsf{td}, x, m) \\ (\sigma^*, \mathsf{cert}) \leftarrow \mathcal{A}_1^{\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},\cdot,\cdot)}(\mathsf{crs}, \sigma) \\ w \leftarrow \mathsf{Ext\text{-}Del}(\mathsf{crs}, \mathsf{td}, x, m, \sigma^*, \mathsf{cert}) \end{array} : \begin{array}{c} \mathsf{Verify}(\mathsf{crs}, x, m, \sigma^*) = 1 \\ \wedge \\ [\mathsf{Certify}(\mathsf{ck}, \mathsf{cert}) = 1 \ \vee \ (x, w) \notin R] \wedge \ (x, m) \notin Q \end{array}\right] \leq \mathsf{negl}(\lambda),$$

where Q *is the list of queries from* $\mathcal{A}$ *to* Sim_1*.*

Remark 6.1. Similarly to NIZK-CD, in our constructions, Setup and Certify are classical, while Sign, Verify, and Delete are quantum algorithms. Except for σ, which includes quantum information, other parameters are classical. Moreover, Sign might be interactive between a classical signer and a quantum verifier.

Remark 6.2. The extraction with deletion as defined in Definition 6.1 implies the extraction as defined in Definition 3.7; it can be proved similarly to Theorem 4.1.

Theorem 6.1. *Assuming any non-interactive simulation-extractable, adaptive multi-theorem computational zero-knowledge with certified deletion, there exists a revocable signature of knowledge.*

Proof. Let $\Gamma = \langle \mathsf{Setup}, \mathsf{Prove}, \mathsf{Verify}, \mathsf{Delete}, \mathsf{Certify} \rangle$ be a simulation-extractable NIZK-CD.

- $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda)$: Output $\mathsf{crs} \leftarrow \Gamma.\mathsf{Setup}(1^\lambda)$.
- $(\sigma, \mathsf{ck}) \leftarrow \mathsf{Sign}(\mathsf{crs}, x, w, m)$: Let $x^* = (x, m)$ be instance, $w^* = w$ witness for

$$L^* = \{(x, m) : \exists w \text{ s.t. } (x, w) \in R\}.$$

  Then, we have $(\sigma, \mathsf{ck}) \leftarrow \Gamma.\mathsf{Prove}(\mathsf{crs}, x^*, w^*)$ with respect to L^*.
- $\{0, 1\} \leftarrow \mathsf{Verify}(\mathsf{crs}, x, m, \sigma)$: Given $x^* = (x, m)$, output $v = \Gamma.\mathsf{Verify}(\mathsf{crs}, x^*, \sigma)$.
- $\mathsf{cert} \leftarrow \mathsf{Delete}(\sigma)$: Output $\mathsf{cert} = \Gamma.\mathsf{Delete}(\sigma)$.
- $\{0, 1\} \leftarrow \mathsf{Certify}(\mathsf{ck}, \mathsf{cert})$: Output $v = \Gamma.\mathsf{Certify}(\mathsf{ck}, \mathsf{cert})$.

Next, we prove the correctness, simulation, and extraction with deletion.

Correctness: Since the scheme Γ satisfies perfect completeness, for any honestly generated σ and cert, both satisfy Verify and $\mathsf{Certify}$, respectively.

Simulation: Let $\Gamma.Sim = (\Gamma.Sim_0, \Gamma.\mathsf{Sim}_1)$ be the simulators of Γ. We build $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1)$ for our construction as follows.

- $(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Sim}_0(1^\lambda)$: Output $(\mathsf{crs}_\Gamma, \mathsf{td}_\Gamma) \leftarrow \Gamma.\mathsf{Sim}_1(1^\lambda)$.
- $\sigma, \mathsf{ck} \leftarrow \mathsf{Sim}_1(\mathsf{crs}, \mathsf{td}, x, m)$: Output $(\sigma, \mathsf{ck}) \leftarrow \Gamma.\mathsf{Sim}_1(\mathsf{crs}, \mathsf{td}, x^* := (x, m))$.

Reduction: Suppose a QPT adversary $\mathcal{A}$ exists such that for polynomial $p(\lambda)$, it breaks the simulation property of Σ_R with an advantage greater than $\frac{1}{p(\lambda)}$. We construct a QPT adversary $\mathcal{B}$ for the zero-knowledge property of Γ as follows.

1. Receive real or simulated crs_Γ and send it to the adversary $\mathcal{A}$.
2. For each query (x, m, w), define $x^* := (x, m)$ and witness $w^* := w$, receive the signature σ by a query to Sign or $\Gamma.\mathsf{Sim}_1$, and send σ to $\mathcal{A}$.
3. Output the result of $\mathcal{A}$.

$\mathcal{B}$ has the same advantage $\frac{1}{p(\lambda)}$ in breaking the zero-knowledge property of Γ.

Extraction with deletion: Let $\Gamma.\mathsf{Sim} = (\Gamma.\mathsf{Sim}_0, \Gamma.\mathsf{Sim}_1)$ be the simulators of Γ and $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1)$ be the simulators of our construction. Let $\Gamma.\mathsf{Ext}$ be the extractor of Γ. We show an extractor $\mathsf{Ext\text{-}Del}$ for extractibility with deletion.

1. On input crs, td, x, m, σ, and cert, run $\Pi.\mathsf{Ext}(\mathsf{crs}, \mathsf{td}, (x, m), \sigma, \mathsf{cert})$, and receive the witness w^*.
2. Output w^* as w.

Reduction: Let $A = (A_0, A_1)$ a QPT algorithm such that given the extractor $\mathsf{Ext\text{-}Del}$, and a polynomial $p(\lambda)$, it breaks the extraction with deletion property of Σ_R with an advantage greater than $\frac{1}{p(\lambda)}$. Then, one can build an adversary algorithm $\mathcal{B} = (\mathcal{B}_0, \mathcal{B}_1)$ to break the simulation extractibility with deletion of Γ; $\mathcal{B}_0$ outputs $x^* = (x, m)$ from $\mathcal{A}_0$ and $\mathcal{B}_1$ outputs $(\sigma^*, \mathsf{cert})$ from $\mathcal{A}_1$. □

Corollary 6.1. *Assuming quantum-hard one-way functions and quantum-secure simulation-extractable NIZK, there exists revocable signature of knowledge.*

Proof. This follows from Theorem 5.1 and Theorem 6.1. □

Corollary 6.2. *Given polynomial quantum hardness of the LWE problem and quantum-secure simulation-extractable NIZK, there exists a revocable signature of knowledge with classical communication and classical signing algorithms.*

Proof. This follows from Theorem 5.2 and Theorem 6.1. □

6.2 Revocable Anonymous Credentials

We define and construct revocable anonymous credentials.

Definition 6.2. (Revocable Anonymous Credentials) *[33] Any scheme* $\Delta_R = \langle \mathsf{Setup}, \mathsf{Sign}, \mathsf{Verify}, \mathsf{Delete}, \mathsf{Certify} \rangle$ *is a revocable anonymous credentials with respect to a set of accesses* $\{S_\lambda\}_{\lambda\in\mathbb{N}}$ *if it satisfies the following.*

- $(\mathsf{nym}, \mathsf{sk}) \leftarrow \mathsf{IssuerSetup}(1^\lambda)$: *output a pseudonym* nym *with a secret key* sk.
- $(\mathsf{cred}, \mathsf{ck}) \leftarrow \mathsf{Issue}(\mathsf{nym}, \mathsf{sk}, \mathsf{access})$: *on input* nym, sk *and requested access* access, *output an anonymous credential* cred *and a certification key* ck.
- $\{0,1\} \leftarrow \mathsf{VerifyCred}(\mathsf{nym}, \mathsf{access}, \mathsf{cred})$: *on input* nym, access, *and* cred, *output* 1 *as accept or* 0 *as reject for validating the anonymous credentials.*
- $\mathsf{cert} \leftarrow \mathsf{Delete}(\mathsf{cred})$*: on input* cred, *output a deletion certificate* cert.
- $\{0,1\} \leftarrow \mathsf{Certify}(\mathsf{ck}, \mathsf{cert})$*: on input* ck *and* cert, *accept or reject.*

Correctness: *For every* $\lambda \in \mathbb{N}$, *pair* $(x, w) \in R$ *and* $m \in \mathcal{M}$, *following is* 1.

$$\Pr\left[\begin{array}{c} \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda) \\ (\sigma, \mathsf{ck}) \leftarrow \mathsf{Sign}(\mathsf{crs}, x, w, m) \\ \mathsf{cert} \leftarrow \mathsf{Delete}(\sigma) \end{array} : \begin{array}{c} \mathsf{Verify}(\mathsf{crs}, x, m, \sigma) = 1 \\ \wedge \\ \mathsf{Certify}(\mathsf{ck}, \mathsf{cert}) = 1 \end{array}\right]$$

Revocation: *For every* QPT *algorithm* $\mathcal{A}$, *sufficiently large* λ, *and access* access, *the following probability is, at most,* $\mathsf{negl}(\lambda)$.

$$\Pr\left[\begin{array}{c} (\mathsf{nym}, \mathsf{sk}) \leftarrow \mathsf{IssuerSetup}(1^\lambda) \\ (\mathsf{cred}, \mathsf{ck}) \leftarrow \mathsf{Issue}(\mathsf{nym}, \mathsf{sk}, \mathsf{access}) \\ (\mathsf{cred}^*, \mathsf{cert}) \leftarrow \mathcal{A}(\mathsf{nym}, \mathsf{cred}) \end{array} : \begin{array}{c} \mathsf{VerifyCred}(\mathsf{nym}, \mathsf{access}, \mathsf{cred}^*) = 1 \\ \wedge \mathsf{Certify}(\mathsf{ck}, \mathsf{cert}) = 1 \end{array}\right]$$

Theorem 6.2. *Assuming any revocable signature of knowledge, there exists a revocable anonymous credentials.*

Proof. Let $(\mathcal{X}, \mathcal{W})$ be some hard NP distribution. Let Σ_R be revocable signature of knowledge. Our construction of anonymous credentials is presented as follows.

- $(\mathsf{nym}, \mathsf{sk}) \leftarrow \mathsf{IssuerSetup}(1^\lambda)$: Generate $\mathsf{crs} \leftarrow \Sigma_R.\mathsf{Setup}(1^\lambda)$, sample a pair $(x, w) \leftarrow (\mathcal{X}, \mathcal{W})$, and output $\mathsf{nym} = (\mathsf{crs}, x)$ and $\mathsf{sk} = w$.
- $(\mathsf{cred}, \mathsf{ck}) \leftarrow \mathsf{Issue}(\mathsf{nym}, \mathsf{sk}, \mathsf{access})$: Output $\mathsf{cred}, \mathsf{ck} \leftarrow \Sigma_R.\mathsf{Sign}(\mathsf{crs}, x, \mathsf{access}, w)$.
- $\{0,1\} \leftarrow \mathsf{VerifyCred}(\mathsf{nym}, \mathsf{access}, \mathsf{cred})$: Output $v = \Gamma.\mathsf{Verify}(\mathsf{crs}, x, \mathsf{access}, \sigma)$.
- $\mathsf{cert} \leftarrow \mathsf{Delete}(\mathsf{cred})$: Output $\mathsf{cert} = \Gamma.\mathsf{Delete}(\sigma)$.
- $\{0,1\} \leftarrow \mathsf{Certify}(\mathsf{ck}, \mathsf{cert})$: Output $v = \Gamma.\mathsf{Certify}(\mathsf{ck}, \mathsf{cert})$.

Next, we prove the correctness and revocation of the proposed construction.

Correctness: Since Σ_R satisfies correctness, for honestly generated credentials cred and certificate cert, both satisfy Verify and $\mathsf{Certify}$, respectively.

Revocation: Suppose that there exists a QPT adversary algorithm $\mathcal{A}$ such that for some polynomial $p(\lambda)$, it breaks revocation property of Δ. We construct a QPT adversary $\mathcal{B}$ to break the extraction with deletion of Σ_R as described below.

1. Receive simulated crs_{Σ_R} from $\Sigma_R.\mathsf{Sim}_0$, sample a pair $(x, w) \leftarrow (\mathcal{X}, \mathcal{W})$, sample an access access, query $\Sigma_R.\mathsf{Sim}_1$ on input (x, access) to get σ, and send $\mathsf{nym} = (\mathsf{crs}, x), \mathsf{cred} = \sigma$ to $\mathcal{A}$.
3. Output the credential cred^* as signature and cert as deletion certificate.

$\mathcal{B}$ has the same advantage $\frac{1}{p(\lambda)}$ in breaking the extraction with deletion of Σ_R. □

Corollary 6.3. *Assuming quantum-hard one-way functions and quantum-secure simulation-extractable NIZK, there exists revocable anonymous credentials.*

Proof. This follows from Corollary 6.1 and Theorem 6.2. □

Corollary 6.4. *Given polynomial quantum hardness of the LWE problem and quantum-secure simulation-extractable NIZK, there exists revocable anonymous credentials with classical communication and classical issuer.*

Proof. This follows from Corollary 6.2 and Theorem 6.2. □

7 Acknowledgments

We thank Ben Sela for pointing out a flaw in the publicly verifiable NIZK-CD construction proposed in a previous version of this paper. We further thank Justin Raizes for a helpful discussion on the notion of certified deniability.

References

1. Scott Aaronson. Quantum copy protection and quantum money. In *24th Annual IEEE Conference on Computational Complexity*. IEEE, July 2009.
2. Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In *44th Annual ACM Symposium on Theory of Computing (STOC)*, pages 41–60, New York, NY, USA, 2012. ACM.
3. Scott Aaronson, Jiahui Liu, Qipeng Liu, Mark Zhandry, and Ruizhe Zhang. New approaches for quantum copy protection. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology—Crypto 2021*, pages 526–555. Springer, 2021.
4. Tolga Acar and Lan Nguyen. Revocation for delegatable anonymous credentials. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *Public Key Cryptography—PKC 2011*, pages 423–440. Springer, 2011.
5. Shweta Agrawal, Fuyuki Kitagawa, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa. Public key encryption with secure key leasing. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology—Eurocrypt 2023*, pages 581–610. Springer, 2023.
6. Joël Alwen, Stephan Krenn, Krzysztof Pietrzak, and Daniel Wichs. Learning with rounding, revisited. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology—Crypto 2013*, pages 57–74. Springer, 2013.
7. Ryan Amos, Marios Georgiou, Aggelos Kiayias, and Mark Zhandry. One-shot signatures and applications to hybrid quantum/classical authentication. In *52nd Annual ACM Symposium on Theory of Computing (STOC)*, page 255–268, New York, NY, USA, 2020. ACM.
8. Prabhanjan Ananth and Rolando L. La Placa. Secure software leasing. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology—Eurocrypt 2021*, pages 501–530. Springer, 2021.
9. Prabhanjan Ananth, Alexander Poremba, and Vinod Vaikuntanathan. Revocable cryptography from learning with errors. In Guy Rothblum and Hoeteck Wee, editors, *Theory of Cryptography*, pages 93–122. Springer, 2023.
10. James Bartusek, Vipul Goyal, Dakshita Khurana, Giulio Malavolta, Justin Raizes, and Bhaskar Roberts. Software with certified deletion. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology—Eurocrypt 2024*, pages 85–111. Springer, 2024.
11. James Bartusek and Dakshita Khurana. Cryptography with certified deletion. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology—Crypto 2023*, pages 192–223. Springer, 2023.
12. James Bartusek, Dakshita Khurana, Giulio Malavolta, Alexander Poremba, and Michael Walter. Weakening assumptions for publicly-verifiable deletion. In *Theory of Cryptography (TCC) 2023, Part IV*, page 183–197. Springer, 2023.
13. James Bartusek, Dakshita Khurana, Giulio Malavolta, Alexander Poremba, and Michael Walter. Weakening assumptions for publicly-verifiable deletion. In Guy Rothblum and Hoeteck Wee, editors, *Theory of Cryptography*, pages 183–197. Springer, 2023.
14. James Bartusek and Justin Raizes. Secret sharing with certified deletion. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology—Crypto 2024*, pages 184–214. Springer, 2024.
15. Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Sha. Randomizable proofs and delegatable anonymous credentials. In Shai Halevi, editor, *Advances in Cryptology—Crypto 2009*, pages 108–125. Springer, 2009.

16. Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 2014.
17. Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In *20th Annual ACM Symposium on Theory of Computing (STOC)*, page 103–112, New York, NY, USA, 1988. ACM.
18. 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 *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 320–331, 2018.
19. Anne Broadbent and Rabib Islam. Quantum encryption with certified deletion. In Rafael Pass and Krzysztof Pietrzak, editors, *Theory of Cryptography*, pages 92–122. Springer, 2020.
20. Anne Broadbent and Sébastien Lord. Uncloneable quantum encryption via oracles, 2019. Available at https://eprint.iacr.org/2019/257.
21. Jan Camenisch, Markulf Kohlweiss, and Claudio Soriente. Solving revocation with efficient update of anonymous credentials. In Juan A. Garay and Roberto De Prisco, editors, *Security and Cryptography for Networks*, pages 454–471. Springer, 2010.
22. Alper Çakan, Vipul Goyal, and Justin Raizes. How to delete without a trace: Certified deniability in a quantum world. Cryptology ePrint Archive, Paper 2024/1832, 2024.
23. Orestis Chardouvelis, Vipul Goyal, Aayush Jain, and Jiahui Liu. Quantum key leasing for PKE and FHE with a classical lessor. Cryptology ePrint Archive, Paper 2023/1640, 2023. https://eprint.iacr.org/2023/1640.
24. Melissa Chase and Anna Lysyanskaya. On signatures of knowledge. In Cynthia Dwork, editor, *Advances in Cryptology—Crypto 2006*, pages 78–96. Springer, 2006.
25. Andrea Coladangelo, Christian Majenz, and Alexander Poremba. Quantum copy protection of compute-and-compare programs in the quantum random oracle model, 2022. Available at https://ia.cr/2020/1194.
26. Giovanni Di Crescenzo, Yuval Ishai, and Rafail Ostrovsky. Non-interactive and non-malleable commitment. In *30th Annual ACM Symposium on Theory of Computing (STOC)*, page 141–150. ACM, 1998.
27. U. Feige, D. Lapidot, and A. Shamir. Multiple non-interactive zero knowledge proofs based on a single random string. In *31st Annual Symposium on Foundations of Computer Science*, pages 308–317 vol.1, 1990.
28. Daniel Gottesman. Uncloneable encryption. *Quantum Info. Comput.*, 3(6):581–602, 2003.
29. Vipul Goyal, Giulio Malavolta, and Justin Raizes. Unclonable commitments and proofs. Cryptology ePrint Archive, Paper 2023/1538, 2023. https://eprint.iacr.org/2023/1538.
30. Carl W. Helstrom. Quantum detection and estimation theory. *J. Statist. Phys.*, 1:231–252, 1969.
31. Taiga Hiroka, Tomoyuki Morimae, Ryo Nishimaki, and Takashi Yamakawa. Quantum encryption with certified deletion, revisited: Public key, attribute-based, and classical communication. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology—Asiacrypt 2021*, pages 606–636. Springer, 2021.
32. A.S Holevo. Statistical decision theory for quantum systems. *Journal of Multivariate Analysis*, 3(4):337–394, 1973.
33. Ruta Jawale and Dakshita Khurana. Unclonable non-interactive zero-knowledge. Cryptology ePrint Archive, Paper 2023/1532, 2023. https://eprint.iacr.org/2023/1532.

34. Jonathan Katz and Ben Sela. Secret sharing with publicly verifiable deletion. Cryptology ePrint Archive, Paper 2024/1596, 2024.
35. Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Secure software leasing from standard assumptions. In Kobbi Nissim and Brent Waters, editors, *Theory of Cryptography*, pages 31–61. Springer, 2021.
36. Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Publicly verifiable deletion from minimal assumptions. In Guy Rothblum and Hoeteck Wee, editors, *Theory of Cryptography*, pages 228–245. Springer, 2023.
37. Jiahui Liu, Qipeng Liu, Luowen Qian, and Mark Zhandry. Collusion resistant copy-protection for watermarkable functionalities. In Eike Kiltz and Vinod Vaikuntanathan, editors, *Theory of Cryptography*, pages 294–323. Springer, 2022.
38. Alex Lombardi and Luke Schaeffer. A note on key agreement and non-interactive commitments. Cryptology ePrint Archive, Paper 2019/279, 2019. https://eprint.iacr.org/2019/279.
39. Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology—Eurocrypt 2012*, pages 700–718. Springer, 2012.
40. Tomoyuki Morimae, Alexander Poremba, and Takashi Yamakawa. Revocable Quantum Digital Signatures. In Frédéric Magniez and Alex Bredariol Grilo, editors, *19th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2024)*, volume 310 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 5:1–5:24, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.
41. Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In *Advances in Cryptology—Crypto 2022, Part I*, page 269–295. Springer, 2022.
42. Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-lwe for any ring and modulus. In *49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, page 461–473, New York, NY, USA, 2017. ACM.
43. Chris Peikert and Sina Shiehian. Noninteractive zero knowledge for NP from (plain) learning with errors. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology—Crypto 2019*, pages 89–114. Springer, 2019.
44. Alexander Poremba. Quantum Proofs of Deletion for Learning with Errors. In Yael Tauman Kalai, editor, *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*, volume 251 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 90:1–90:14, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.
45. Roy Radian and Or Sattath. Semi-quantum money. In *1st ACM Conference on Advances in Financial Technologies (AFT)*, page 132–146, New York, NY, USA, 2019. ACM.
46. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), 2009.
47. A. Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In *40th Annual Symposium on Foundations of Computer Science*, pages 543–553, 1999.
48. Alfredo De Santis, Giovanni Di Crescenzo, Rafail Ostrovsky, Giuseppe Persiano, and Amit Sahai. Robust non-interactive zero knowledge. In *Advances in Cryptology—Crypto 2001*, page 566–598. Springer, 2001.

49. Dominique Unruh. Revocable quantum timed-release encryption. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology—Eurocrypt 2014*, pages 129–146. Springer, 2014.
50. Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.