Unclonable Non-interactive Zero-Knowledge

Ruta Jawale(✉) and Dakshita Khurana

University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA
jawale2@illinois.edu

Abstract. A non-interactive ZK (NIZK) proof enables verification of NP statements without revealing secrets about them. However, an adversary that obtains a NIZK proof may be able to clone this proof and distribute arbitrarily many copies of it to various entities: this is inevitable for any proof that takes the form of a classical string. In this paper, we ask whether it is possible to rely on quantum information in order to build NIZK proof systems that are impossible to clone.

We define and construct *unclonable non-interactive zero-knowledge arguments (of knowledge)* for NP, addressing a question first posed by Aaronson (CCC 2009). Besides satisfying the zero-knowledge and argument of knowledge properties, these proofs additionally satisfy unclonability. Very roughly, this ensures that no adversary can split an honestly generated proof of membership of an instance x in an NP language $\mathcal{L}$ and distribute copies to multiple entities that all obtain accepting proofs of membership of x in $\mathcal{L}$. Our result has applications to *unclonable signatures of knowledge*, which we define and construct in this work; these *non-interactively* prevent replay attacks.

Keywords: Unclonable · Zero-Knowledge · Quantum Money

1 Introduction

Zero-knowledge (ZK) [27] proofs allow a prover to convince a verifier about the truth of an (NP) statement, without revealing secrets about it. These are among the most widely used cryptographic primitives, with a rich history of study.

Enhancing Zero-Knowledge. ZK proofs for NP are typically defined via the simulation paradigm. A simulator is a polynomial-time algorithm that mimics the interaction of an adversarial verifier with an honest prover, given only the statement, i.e., $x \in \mathcal{L}$, for an instance x of an NP language $\mathcal{L}$. A protocol satisfies zero-knowledge if it admits a simulator that generates a view for the verifier, which is indistinguishable from the real view generated by an honest prover. This captures the intuition that any information obtained by a verifier upon observing an honestly generated proof, could have been generated by the verifier "on its own" by running the simulator.

K.-M. Chung and Y. Sasaki (Eds.): ASIACRYPT 2024, LNCS 15492, pp. 94–128, 2025.
https://doi.org/10.1007/978-981-96-0947-5_4

Despite being widely useful and popular, there are desirable properties of proof systems that (standard) simulation-based security does not capture. For example, consider (distributions over) instances x of an NP language $\mathcal{L}$ where it is hard to find an NP witness w corresponding to a given instance x. In an "ideal" world, given just the description of one such NP statement $x \in \mathcal{L}$, it is difficult for an adversary to find an NP witness w, and therefore to output *any* proofs of membership of $x \in \mathcal{L}$. And yet, upon obtaining a *single proof* of membership of $x \in \mathcal{L}$, it may suddenly become feasible for an adversary to make many copies of this proof, thereby generating *several* correct proofs of membership of $x \in \mathcal{L}$.

Unfortunately, this attack is inevitable for classical non-interactive proofs: given any proof string, an adversary can always make multiple copies of it. And yet, there is hope to prevent such an attack quantumly, by relying on the *no-cloning* principle.

Indeed, a recent series of exciting works have combined cryptography with the no-cloning principle to develop quantum money [2,24,34,48,49], quantum tokens for digital signatures [16], quantum copy-protection [1,3,8,23], unclonable encryption [6,7,19,28,39], unclonable decryption [26], one-out-of-many unclonable security [35], and more. In this work, we combine zero-knowledge and unclonability to address a question first posed by Aaronson [1]:

Can we construct unclonable quantum proofs?
How do these proofs relate to quantum money or copy-protection?

1.1 Our Results

We define and construct unclonable non-interactive zero-knowledge argument of knowledge (NIZKAoK). We obtain a construction in the common reference string (CRS) model, as well as one in the quantum(-accessible) random oracle model (QROM). The CRS model allows a trusted third-party to set up a structured string that is provided to both the prover and verifier. On the other hand, the QROM allows both parties quantum access to a truly random function $\mathcal{O}$.

In what follows, we describe our contributions in more detail.

Definitional Contributions. Before discussing how we formalize the concept of unclonability for NIZKs, it will be helpful to define hard distributions over NP instance-witness pairs.

Hard Distributions over Instance-Witness Pairs. Informally, an efficiently samplable distribution over instance-witness pairs of a language $\mathcal{L}$ is a "hard" distribution if given an instance sampled randomly from this distribution, it is hard to find a witness. Then, unclonable security requires that no adversary given an instance x sampled randomly from the distribution, together with an honestly generated proof, can output *two accepting proofs* of membership of $x \in \mathcal{L}$.

More specifically, a hard distribution $(\mathcal{X}, \mathcal{W})$ over $R_{\mathcal{L}}$ satisfies the following: for any polynomial-sized (quantum) circuit family $\{C_\lambda\}_{\lambda \in \mathbb{N}}$,

$$\Pr_{(x,w) \leftarrow (\mathcal{X}_\lambda, \mathcal{W}_\lambda)} [C_\lambda(x) \in R_{\mathcal{L}}(x)] \leq \mathsf{negl}(\lambda).$$

For the sake of simplifying our subsequent discussions and definitions, let us fix a NP language $\mathcal{L}$ with corresponding relation $\mathcal{R}$. Let $(\mathcal{X}, \mathcal{W})$ be some hard distribution over $\mathcal{R}$.

A Weaker Definition: Unclonable Security. For NIZKs satisfying standard completeness, soundness and ZK, we define a simple, natural variant of unclonable security as follows. Informally, a proof system satisfies unclonable security if, given an honest proof for an instance and witness pair (x, w) sampled from a hard distribution $(\mathcal{X}, \mathcal{W})$, no adversary can produce two proofs that verify with respect to x except with negligible probability.

Definition 1. *(Unclonable Security of NIZK). A NIZK proof* $(\mathsf{Setup}, \mathsf{Prove}, \mathsf{Verify})$ *satisfies unclonable security if for every language* $\mathcal{L}$ *and every hard distribution* $(\mathcal{X}, \mathcal{W})$ *over* $R_{\mathcal{L}}$*, for every poly-sized quantum circuit family* $\{C_\lambda\}_{\lambda \in \mathbb{N}}$*,*

$$\Pr_{(x,w) \leftarrow (\mathcal{X}_\lambda, \mathcal{W}_\lambda)} \left[\begin{array}{c} \mathsf{Verify}(\mathsf{crs}, x, \pi_1) = 1 \\ \textit{and } \mathsf{Verify}(\mathsf{crs}, x, \pi_2) = 1 \end{array} \middle| \begin{array}{c} (\mathsf{crs},\mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda) \\ \pi \leftarrow \mathsf{Prove}(\mathsf{crs}, x, w) \\ \pi_1, \pi_2 \leftarrow C_\lambda(x, \pi) \end{array} \right] \leq \mathsf{negl}(\lambda).$$

In the definition above, we aim to capture the intuition that one of the two proofs output by the adversary can be the honest proof they received, but the adversary cannot output any other correct proof for the same statement. Of course, such a proof is easy to generate if the adversary is able to find the witness w for x, which is exactly why we require hardness of the distribution $(\mathcal{X}, \mathcal{W})$ to make the definition non-trivial.

We also remark that unclonable security of proofs *necessitates* that the proof π keep hidden any witnesses w certifying membership of x in $\mathcal{L}$, as otherwise an adversary can always clone the proof π by generating (from scratch) another proof for x given the witness w.

A Stronger Definition: Unclonable Extractability. We can further strengthen the definition above to require that any adversary generating two (or more) accepting proofs of membership of $x \in \mathcal{L}$ given a single proof, must have generated one of the two proofs "from scratch" and must therefore "know" a valid witness w for x. This will remove the need to refer to hard languages.

In more detail, we will say that a proof system satisfies *unclonable extractability* if, from any adversary $\mathcal{A}$ that on input a single proof of membership of $x \in \mathcal{L}$ outputs two proofs for x, then we can extract a valid witness w from $\mathcal{A}$ for at least one of these statements with high probability. Our (still, simplified) definition of unclonable extractability is as follows.

Definition 2 (Unclonable Extractability). *A proof* $(\mathsf{Setup}, \mathsf{Prove}, \mathsf{Verify})$ *satisfies unclonable security there exists a QPT extractor* $\mathcal{E}$ *which is an oracle-aided circuit such that for every language* $\mathcal{L}$ *with corresponding relation* $\mathcal{R}_{\mathcal{L}}$ *and for every non-uniform polynomial-time quantum adversary* $\mathcal{A}$*, for every instance-witness pair* $(x, w) \in \mathcal{R}_{\mathcal{L}}$ *and* $\lambda = \lambda(|x|)$*, such that there is a polynomial* $p(\cdot)$

satisfying:

$$\Pr\left[\mathsf{Verify}(\mathsf{crs},x,\pi_1)=1 \bigwedge \mathsf{Verify}(\mathsf{crs},x,\pi_2)=1 \middle| \begin{smallmatrix}(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Setup}(1^\lambda)\\ \pi\leftarrow\mathsf{Prove}(\mathsf{crs},x,w)\\ \pi_1,\pi_2\leftarrow\mathcal{A}_\lambda(\mathsf{crs},x,\pi,z)\end{smallmatrix}\right] \geq \frac{1}{p(\lambda)},$$

there is also a polynomial $q(\cdot)$ such that

$$\Pr[(x,w_{\mathcal{A}})\in\mathcal{R}_{\mathcal{L}}|w_{\mathcal{A}}\leftarrow\mathcal{E}^{\mathcal{A}}(x)]\geq\frac{1}{q(\lambda)}.$$

In fact, in the technical sections, we further generalize this definition to consider a setting where the adversary obtains an even larger number (say $k-1$) input proofs on instances $x_1,\ldots,x_{k-1}$, and outputs k or more proofs. Then we require the extraction of an NP witness corresponding to any proofs that attempt to "clone" honestly generated proofs (i.e. the adversary outputs two or more proofs w.r.t. the same instance $x_i\in\{x_1,\ldots,x_{k-1}\}$). All our theorem statements hold w.r.t. this general definition. Finally, we also consider definitions and constructions in the quantum-accessible random oracle model (QROM); these are natural generalizations of the definitions above, so we do not discuss them here.

We also show that the latter definition of unclonable extractability implies the former, i.e. unclonable security. Informally, this follows because the extractor guaranteed by the definition of extractability is able to obtain a witness w for x from any adversary, which contradicts hardness of the distribution $(\mathcal{X},\mathcal{W})$. We refer the reader to the full version [33] for a formal proof of this claim.

Moreover, we can generically boost the unclonable-extractor's success probability from $1/q(\lambda)$ to $1-\mathsf{negl}(\lambda)$ with respect to a security parameter λ. For details, see Sect. 4.2 and Sect. 5.2.

Realizations of Unclonable NIZK, and Relationship with Quantum Money. We obtain realizations of unclonable NIZKs in both the common reference string (CRS) and the quantum random oracle (QRO) models, assuming public-key quantum money mini-scheme and other (post-quantum) standard assumptions. We summarize these results below.

Theorem 1 (Informal). *Assuming public-key quantum money mini-scheme, public-key encryption, perfectly binding and computationally hiding commitments, and adaptively sound NIZK arguments for* NP*, there exists an unclonable-extractable NIZK argument of knowledge scheme in the CRS model.*

Adaptively sound NIZK arguments for NP exist assuming the polynomial quantum hardness of LWE [40].

Theorem 2 (Informal). *Assuming public-key quantum money mini-scheme and honest verifier zero-knowledge arguments of knowledge sigma protocols for* NP*, there exists an unclonable-extractable NIZK argument of knowledge scheme in the QROM.*

Is Quantum Money Necessary for Unclonable NIZKs? Our work builds unclonable NIZKs for NP by relying on any (public-key) quantum money scheme (mini-scheme), in conjuction with other assumptions such as NIZKs for NP. Since constructions of public-key quantum money mini-scheme are only known based on post-quantum indistinguishability obfuscation [2,50], it is natural to wonder whether the reliance on quantum money is inherent. We show that this is indeed the case, by proving that unclonable NIZKs in fact imply public-key quantum money mini-scheme.

Theorem 3 (Informal). *Unclonable NIZK arguments for NP imply public-key quantum money mini-scheme.*

Applications Unclonable Signatures of Knowledge. A (classical) signature scheme asserts that a message m has been signed on behalf of a public key pk. However, in order for this signature to be authenticated, the public key pk must be proven trustworthy through a certification chain rooted at a trusted public key PK. However, as [21] argue, this reveals too much information; it should be sufficient for the recipient to only know that *there exists* a public key pk with a chain of trust from PK. To solve this problem, [21] propose *signatures of knowledge* which allow a signer to sign *on behalf of an instance x of an* NP*-hard language* without revealing its corresponding witness w. Such signatures provide an anonymity guarantee by hiding the pk of the sender.

While this is ideal for many applications, anonymity presents the following downside: a receiver cannot determine whether they were the intended recipient of this signature. In particular, anonymous signatures are more susceptible to *replay attacks*. Replay attacks are a form of passive attack whereby an adversary observes a signature and retains a copy. The adversary then leverages this signature, either at a later point in time or to a different party, to impersonate the original signer. The privacy and financial consequences of replay attacks are steep. They can lead to data breach attacks which cost millions of dollars annually and world-wide [32].

In this work, we construct a signature of knowledge scheme which is the first *non-interactive* signature in the CRS model that is *naturally secure against replay attacks*. Non-interactive, replay attack secure signatures have seen a lot of recent interest including a line of works in the bounded quantum storage model [11] and the quantum random oracle model [10]. Our construction is in the CRS model and relies on the quantum average-case hardness of NP problems, plausible cryptographic assumptions, and the axioms of quantum mechanics. We accomplish this by defining *unclonable signatures of knowledge*: if an adversary, given a signature of a message m with respect to an instance x, can produce two signatures for m which verify with respect to the same instance x, then our extractor is able to extract a witness for x.

Theorem 4 (Informal). *Assuming public-key quantum money mini-scheme, public-key encryption, perfectly binding and computationally hiding commitments, and simulation-sound NIZK arguments for* NP*, there exists an unclonable-extractable signature of knowledge in the CRS model.*

Our construction involves showing that an existing compiler can be augmented using unclonable NIZKs to construct unclonable signatures of knowledge. The authors of [21] construct signatures of knowledge from CPA secure dense cryptosystems [44,45] and simulation-sound NIZKs for NP [42,43]. Signatures of knowledge are signature schemes in the CRS model for which we associate an instance x in a language $\mathcal{L}$. This signature is simulatable, so there exists a simulator which can create valid signatures without knowledge of a witness for x. Additionally, the signature is extractable which means there is an extractor which is given a trapdoor for the CRS and a signature, and is able to produce a witness for x. We show that, by switching the simulation-sound NIZKs for unclonable simulation-extractable NIZKs (and slightly modifying the compiler), we can construct unclonable signatures of knowledge.

Relationship with Revocation. A recent exciting line of work obtains *certified deletion* for time-lock puzzles [46], non-local games [25], information-theoretic proofs of deletion with partial security [22], encryption schemes [13,18], device-independent security of one-time pad encryption with certified deletion [36], public-key encryption with certified deletion [30], commitments and zero-knowledge with certified everlasting hiding [31], and fully-homomorphic encryption with certified deletion [9,12–14,41]. While certified everlasting deletion of secrets has been explored in the context of *interactive* zero-knowledge proofs [31], there are no existing proposals for *non-interactive* ZK satisfying variants of certified deletion. Our work provides a pathway to building such proofs.

In this work, we construct a quantum *revocable/unclonable anonymous credentials* protocol in which the issuer of credentials uses a pseudonym to anonymize themselves, receivers of credentials do not require any trusted setup, and the issuer has the ability to remove access from other users. Our work follows a line of work on (classical) revocation for anonymous credentials schemes using NIZK [4,15,20].

In particular, our construction involves noting that NIZK proof systems that are unclonable can also be viewed as supporting a form of certified deletion/revocation, where in order to delete, an adversary must simply return the entire proof. In other words, the (quantum) certificate of deletion is the proof itself, and this certificate can be verified by running the NIZK verification procedure on the proof. The unclonability guarantee implies that an adversary cannot keep with itself or later have the ability to generate *another proof* for the same instance x. In the other direction, in order to offer certifiable deletion, a NIZK must necessarily be unclonable. To see why, note that if there was an adversary who could clone the NIZK, we could use this adversary to obtain two copies, and provably delete one of them. Even though the challenger for the certifiable deletion game would be convinced that its proof was deleted, we would still be left with another correct proof.

1.2 Related Works

This work was built upon the foundations of and novel concepts introduced by prior literature. We will briefly touch upon some notable such results in this section.

Unclonable Encryptions. *Unclonable encryption* [6,7,19,28,39] imagines an interaction between three parties in which one party receives a quantum ciphertext and splits this ciphertext in some manner between the two remaining parties. At some later point, the key of the encryption scheme is revealed, yet both parties should not be able to simultaneouly recover the underlying message. While our proof systems share the ideology of unclonability, we do not have a similar game-based definition of security. This is mainly due to proof systems offering more structure which can take advantage of to express unclonability in terms of simulators and extractors.

Signature Tokens. Prior work [17] defines and constructs *signature tokens* which are signatures which involve a quantum signing token which can only be used once before it becomes inert. The setting they consider is where a client wishes to delegate the signing process to a server, but does not wish the server to be able to sign more than one message. They rely on quantum money [2] and the no-cloning principle to ensure the signature can only be computed once. For our unclonable signatures of knowledge result, we focus on the setting where a client wishes to authenticate themselves to a server and wants to prevent an adversary from simultaneously, or later, masquerading as them.

One-shot Signatures. The authors of [5] introduce the notion of *one-shot signatures* which extend the concept of signature tokens to a scenario where the client and server only exchange classical information to create a one-use quantum signature token. They show that these signatures can be plausibly constructed in the CRS model from post-quantum indistinguishability obfuscation. Unless additional measures for security, which we discussed in our applications section, are employed, classical communication can be easily copied and replayed at a later point. In contrast, we prevent an adversary from simultaneously, or later, authenticating with the client's identity.

Post-quantum Fiat-Shamir. Our QROM results are heavily inspired by the recent post-quantum Fiat-Shamir result [37] which proves the post-quantum security of NIZKs in the compressed quantum(-accessible) random oracle model (compressed QROM). These classical NIZKs are the result of applying Fiat-Shamir to post-quantum sigma protocols which are HVZKAoKs. We further extend, and crucially rely upon, their novel proof techniques to prove extractability (for AoK) and programmability (for ZK) to achieve extractability and programmability for some protocols which output quantum proofs.

1.3 Concurrent Works

Unclonable Commitments and Proofs. A recent, concurrent work [29] defines and constructs unclonable commitments and interactive unclonable proofs. They additionally construct commitments in the QROM that are unclonable with respect to any verification procedures, and they show that it is impossible to have (interactive) proofs with the same properties. The authors also observe a similar relationship between non-interactive unclonable proofs and public-key quantum money via unclonable commitments. They also briefly mention a connection between unclonable commitments and unclonable credentials.

In contrast, we define unclonable-extractable proofs which we construct in the *non-interactive* setting in *both* the crs model and the QROM. We also show a relationship between non-interactive unclonable-extractable proofs and quantum money in *both* the crs model and the QROM. Our work also *formalizes* the relationship between unclonable-extractable proofs and unclonable *anonymous* credentials.

2 Technical Overview

In this section, we give a high-level overview of our construction and the techniques underlying our main results.

2.1 Unclonable Extractable NIZKs in the CRS Model

Our construction assumes the existence of public-key encryption, classical bit commitments where honestly generated commitment strings are perfectly binding, along with

- *Public-key quantum money mini-scheme* (which is known assuming post-quantum $i\mathcal{O}$ and injective OWFs [50]). At a high level, public-key quantum money mini-scheme consists of two algorithms: Gen and Ver. Gen on input a security parameter, outputs a (possibly mixed-state) quantum banknote $\rho_\$$ along with a classical serial number s. Ver is public, takes a quantum money banknote, and outputs either a classical serial number s, or $\perp$ indicating that its input is an invalid banknote. The security guarantee is that no efficient adversary given an honest banknote $\rho_\$$ can output two notes $\rho_{\$,0}$ and $\rho_{\$,1}$ that both pass the verification and have serial numbers equal to that of $\rho_\$$.
- *Post-quantum NIZKs for NP*, which are known assuming the post-quantum hardness of LWE. These satisfy (besides completeness) (1) soundness, i.e., no efficient prover can generate accepting proofs for false NP statements, and (2) zero-knowledge, i.e., the verifier obtains no information from an honestly generated proof beyond what it could have generated on *its own* given the NP statement itself.

Construction. Given these primitives, the algorithms $(\mathsf{Setup}, \mathsf{Prove}, \mathsf{Verify})$ of the unclonable extractable NIZK are as follows.

$\underline{\text{SETUP}}(1^\lambda)$: The setup algorithm samples a public key pk of a public-key encryption, the common reference string crs of a classical (post-quantum) NIZK for NP, along with a perfectly binding, computationally hiding classical commitment to 0^λ with uniform randomness t, i.e. $c = \mathsf{Com}(0^\lambda; t)$. It outputs $(\mathsf{pk}, \mathsf{crs}, c)$.

$\underline{\text{PROVE}}$: Given the CRS $(\mathsf{pk}, \mathsf{crs}, c)$, instance x and witness w, output $(\rho_\$, s, ct, \pi)$ where

- The state $\rho_\$ \leftarrow \mathsf{Gen}$ is generated as a quantum banknote with associated serial number s.
- The ciphertext $ct = \mathsf{Enc}_{\mathsf{pk}}(w; u)$ is an encryption of the witness w with randomness u.
- The proof string π is a (post-quantum) NIZK for the following statement using witness (w, u):

$$\mathsf{EITHER}\ (\exists w, u : ct = \mathsf{Enc}_{\mathsf{pk}}(w; u) \wedge R_L(x, w) = 1)\ \mathsf{OR}\ (\exists r : c = \mathsf{Com}(s; r))\,,$$

  where we recall that pk and c were a part of the CRS output by the Setup algorithm.

$\underline{\text{VERIFY}}$: Given CRS $(\mathsf{pk}, \mathsf{crs}, c)$, instance x and proof $(\rho_\$, s, ct, \pi)$, check that (1) $\mathsf{Ver}(\rho_\$)$ outputs s and (2) π is an accepting NIZK argument of the statement above.

Analysis. Completeness, soundness/argument of knowledge and ZK for this construction follow relatively easily, so we focus on unclonable extractability in this overview. Recall that unclonable extractability requires that no adversary, given an honestly generated proof for $x \in \mathcal{L}$, can split this into *two accepting proofs* for $x \in \mathcal{L}$ (as long as it is hard to find a witness for x). Towards a contradiction, suppose an adversary splits a proof into 2 accepting proofs $(\rho_{\$,0}, s_1, ct_1, \pi_1)$, $(\rho_{\$,1}, s_2, ct_2, \pi_2)$. Then,

- If $s_1 = s_2 = s$, the adversary given one bank note with serial number s generated two valid banknotes $\rho_{\$,0}$ and $\rho_{\$,1}$ that both have the same serial number s. This contradicts the security of quantum money.
- Otherwise, there is a $b \in \{1, 2\}$ such that $s_b \neq s$. Then, consider an indistinguishable hybrid where the adversary obtains a simulated proof generated *without witness* w as follows: (1) sample quantum banknote $\rho_\$$ with serial number s, (2) sample public key pk along with secret key sk, (3) generate $c = \mathsf{Com}(s; t)$, $ct = \mathsf{Enc}_{\mathsf{pk}}(0; u)$, (4) generate proof π using witness t (since $c = \mathsf{Com}(s; t)$) instead of using witness w. Send common reference string $(\mathsf{pk}, \mathsf{crs}, c)$ and proof $(\rho_\$, s, ct, \pi)$ to the adversary. Now, the proof that the adversary generates with $s_b \neq s$ *must* contain $\mathsf{ct}_b = \mathsf{Enc}_{\mathsf{pk}}(w; u)$, since c being generated as a commitment to $s \neq s_b$ along with the perfect binding property implies that $(\nexists\ r : c = \mathsf{Com}(s_b; r))$. That is, given instance x, the adversary can be used to compute a witness w for x by decrypting ciphertext ct_b, thereby contradicting the hardness of the distribution.

Our technical construction in Sect. 4.4, while conceptually the same, is formalized slightly differently. It uses NIZKs with an enhanced simulation-extraction property, which can be generically constructed from NIZK (see Sect. 4.1). Having constructed unclonable extractable arguments in the CRS model, in the next section, we analyze a construction of unclonable extractable arguments in the QROM.

2.2 Unclonable Extractable NIZK in the QROM

We now turn our attention to the QRO setting in which we demonstrate a protocol which is provably unclonable. Our construction assumes the existence of public-key quantum money mini-scheme and a *post-quantum sigma protocol for NP*. A sigma protocol (P, V) is an interactive three-message honest-verifier protocol: the prover sends a commitment message, the verifier sends a uniformly random challenge, and the prover replies by opening its commitment at the locations specified by the random challenge.

Construction. The algorithms (Prove, Verify) of the unclonable extractable NIZK in the QROM are as follows.

Prove: Given an instance x and witness w, output $(\rho_\$, s, \alpha, \beta, \gamma)$ where

- The quantum banknote $\rho_\$$ is generated alongside associated serial number s.
- P is run to compute the sigma protocol's commitment message as α given (x, w) as input.
- The random oracle is queried on input (α, s, x) in order to obtain a challenge β.
- P is run, given as input (x, w, α, β) and its previous internal state, to compute the sigma protocol's commitment openings as γ.

Verify: Given instance x and proof $(\rho_\$, s, \alpha, \beta, \gamma)$, check that (1) the quantum money verifier accepts $(\rho_\$, s)$, (2) the random oracle on input (α, s, x) outputs β, and (3) V accepts the transcript (α, β, γ) with respect to x.

Analysis. Since the completeness, argument of knowledge and zero-knowledge properties are easy to show, we focus on unclonable extractability. Suppose an adversary was able to provide two accepting proofs $\pi_1 = (\rho_{\$,0}, s_1, \alpha_1, \beta_1, \gamma_1)$ and $\pi_2 = (\rho_{\$,1}, s_2, \alpha_2, \beta_2, \gamma_2)$ for an instance x for which it received an honestly generated proof $\pi = (\rho_\$, s, \alpha, \beta, \gamma)$. Then,

- Suppose $s_1 = s_2 = s$. In this case, the adversary given one bank note with serial number s generated two valid banknotes $\rho_{\$,0}$ and $\rho_{\$,1}$ that both have the same serial number s. This contradicts the security of quantum money.
- Otherwise, there is a $b \in [1, 2]$ such that $s_b \neq s$. By the zero-knowledge property of the underlying HVZK sigma protocol, this event also occurs when the proof π that the adversary is given is replaced with a simulated proof. Specifically, we build a reduction that locally programs the random oracle

at location (α, s, x) in order to generate a simulated proof for the adversary. Since the adversary's own proof for $s_b \neq s$ is generated by making a distinct query $(\alpha_b, s_b, x) \neq (\alpha, s, x)$, the programming on (α, s, x) does not affect the knowledge extractor for the adversary's proof, which simply rewinds the (quantum) random oracle to extract a witness for x, following [37]. This allows us to obtain a contradiction, showing that our protocol must be unclonable.

2.3 Unclonable NIZKs Imply Quantum Money Mini-Scheme

Finally, we discuss why unclonable NIZKs satisfying even the weaker definition of unclonable security (i.e., w.r.t. hard distributions) imply public-key quantum money mini-scheme. Given an unclonable NIZK, we build a public-key quantum money mini-scheme as follows.

Construction. Let $(\mathcal{X}, \mathcal{W})$ be a hard distribution over a language $\mathcal{L} \in \mathsf{NP}$. Let $\Pi = (\mathsf{Setup}, \mathsf{Prove}, \mathsf{Verify})$ be an unclonable NIZK protocol for $\mathcal{L}$.

$\underline{\text{GEN}}(1^\lambda)$: Sample $(x, w) \leftarrow (\mathcal{X}, \mathcal{W})$, $\mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, x)$, and an unclonable NIZK proof π as $\mathsf{Prove}(\mathsf{crs}, x, w)$. Output a (possibly mixed-state) quantum banknote $\rho_\$ = \pi$, and associated serial number $s = (\mathsf{crs}, x)$.

$\underline{\text{VER}}(\rho_\$, s)$: Given a (possibly mixed-state) quantum banknote $\rho_\$$ and a classical serial number s as input, parse $\rho_\$ = \pi$ and $s = (\mathsf{crs}, x)$, and output the result of $\mathsf{Verify}(\mathsf{crs}, x, \pi)$.

Analysis. The correctness of the quantum money scheme follows from the completeness of the unclonable NIZK Π. We will now argue that this quantum money scheme is unforgeable. Suppose an adversary $\mathcal{A}$ given a quantum banknote and classical serial number $(\rho_\$, s)$ was able to output two banknotes $(\rho_{\$,0}, \rho_{\$,1})$ both of which are accepted with respect to s. We can use $\mathcal{A}$ to define a reduction to the uncloneability of our NIZK Π as follows:

- The NIZK uncloneability challenger outputs a hard instance-witness pair (x, w), a common reference string crs, and an unclonable NIZK π to the reduction.
- The reduction outputs a banknote $(\rho_\$, s)$ to the adversary, where $\rho_\$ = \pi$ and $s = (\mathsf{crs}, x)$. It receives two quantum banknotes $(\rho_{\$,0}, \rho_{\$,1})$ from $\mathcal{A}$, and finally outputs two proofs (π_0, π_1) where $\pi_0 = \rho_{\$,0}$ and $\pi_1 = \rho_{\$,1}$.

If $\mathcal{A}$ succeeds in breaking unforgeability, then the quantum money verifier accepts both banknotes $(\rho_{\$,0} = \pi_0, \rho_{\$,1} = \pi_1)$, with respect to the same serial number $s = (\mathsf{crs}, x)$. By syntax of the verification algorithm, this essentially means that both *proofs* (π_0, π_1) are accepting proofs for membership of the same instance $x \in \mathcal{L}$, w.r.t. crs, leading to a break in the unclonability of NIZK.

2.4 Unclonable Signatures of Knowledge

Informally, a signature of knowledge has the following property: if an adversary, given a signature of a message m with respect to an instance x, can produce

two signatures for m which verify with respect to the same instance x, then the adversary *must know* (and our extractor will be able to extract) a witness for x.

We obtain unclonable signatures of knowledge assuming the existence of an unclonable extractable *simulation-extractable* NIZK for NP. Simulation-extractability states that an adversary which is provided any number of simulated proofs for instance and witness pairs of their choosing, cannot produce an accepting proof π for an instance x which they have not queried before and where extraction fails to find an accepting witness w. Our unclonable extractable NIZK for NP in the CRS model can, with some extra work, be upgraded to simulation-extractable.

We informally describe the construction of signatures of knowledge from such a NIZK below.

Construction. Let $(\mathsf{Setup}, \mathsf{P}, \mathsf{V})$ be non-interactive simulation-extractable, adaptive multi-theorem computational zero-knowledge, unclonable-extractable protocol for NP. Let $\mathcal{R}$ be the NP relation corresponding to $\mathcal{L}$.

Setup: The setup algorithm samples a common reference string crs of an unclonable-extractable simulation-extractable NIZK for NP. It outputs crs.

Sign: Given the CRS crs, instance x, witness w, and message m, output signature π where

- The proof string π is an unclonable-extractable simulation-extractable NIZK with tag m using witness w of the following statement:

$$(\exists w : (x, w) \in \mathcal{R}) .$$

Verify: Given CRS crs, instance x, message m, and signature π, check that π is an accepting NIZK proof with tag m of the statement above.

Analysis. The simulatability (extractability) property follows from the zero-knowledge (resp. simulation-extractability) properties of the NIZK. Suppose an adversary $\mathcal{A}$ given a signature σ was able to forge two signatures $\sigma_1 = \pi_1$ and $\sigma_2 = \pi_2$, and, yet, our extractor was to fail to extract a witness w from $\mathcal{A}$. Then,

- Either both proofs π_1 and π_2 are accepting proofs for membership of the same instance w.r.t. crs. However, this contradicts the unclonability of the NIZK.
- Otherwise there exists a proof π_i (where $i \in \{1, 2\}$) for an instance which $\mathcal{A}$ has not previously seen a proof for. We can switch to a hybrid where our signatures contain simulated proofs for the NIZK. But now, we have that the verifier accepts a proof for an instance which $\mathcal{A}$ has not seen a simulated proof for and, yet, we cannot extract a witness from $\mathcal{A}$. This contradicts the simulation extractability of the NIZK.

Roadmap. In Sect. 4, we define and construct unclonable NIZKs in the CRS model, and in Sect. 5, in the QROM. Along the way, we also show that unclonable NIZKs imply quantum money (in the CRS and QRO model respectively). Later, we show how to define and construct unclonable signatures of knowledge from unclonable NIZKs in the CRS model.

3 Preliminaries

We defer definitions to the full version [33]; below we recall some useful theorems.

3.1 Post-quantum Commitments and Encryption

Theorem 5 (Post-quantum Commitment). *[38] Assuming the polynomial quantum hardness of LWE, there exists a non-interactive commitment with perfect binding and computational hiding.*

3.2 NIZKs in the CRS Model

Theorem 6 (Post-quantum NIZK Argument for NP in the CRS Model). *[40] Assuming the polynomial quantum hardness of LWE, there exists a non-interactive adaptively computationally sound, adaptively computationally zero-knowledge argument for* NP *in the common reference string model.*

Theorem 7 (Simulation Sound Compiler). *[43] Given one-way functions and a single-theorem NIZK proof system for* NP*, then there exists a non-interactive simulation sound, adaptively multi-theorem computationally zero-knowledge proof for* NP *in the common reference string model.*

Corollary 1 (Post-quantum Simulation Sound NIZK for NP). *Assuming the polynomial quantum hardness of LWE, there exists a post-quantum non-interactive simulation sound, adaptively multi-theorem computationally zero-knowledge proof for* NP *in the common reference string model.*

Proof. This follows from Theorem 6 and Theorem 7.

3.3 NIZKs in the QRO Model

Theorem 8 (NIZKAoK in QROM [37,47]). *Let* Π *be a post-quantum sigma protocol. The Fiat-Shamir heuristic applied to* Π *yields a classical post-quantum NIZKAoK in the QROM.*

3.4 Quantum Money

Theorem 9 (Quantum Money from Subspace Hiding Obfuscation [2, 50]). *If injective one-way functions and post-quantum iO exist, then public-key quantum money exists.*

4 Unclonable Non-interactive Zero-Knowledge in the CRS Model

4.1 Simulation-Extractable NIZK

We defer the definition, and proofs to the full version [33]; below we state our results.

Simulation-Extractable Non-Interactive ZK for $\mathcal{L} \in \mathsf{NP}$

Let $\Pi = (\mathsf{Setup}, \mathsf{P}, \mathsf{V})$ be a non-interactive simulation sound, adaptively multi-theorem computationally zero-knowledge protocol for NP, and $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a post-quantum perfectly correct, IND-CPA secure encryption scheme. Let $\mathcal{R}$ be the relation with respect to $\mathcal{L} \in \mathsf{NP}$.

$\underline{\textsc{Setup}}(1^\lambda)$: Compute $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$, and $(\mathsf{crs}_\Pi, \mathsf{td}_\Pi) \leftarrow \Pi.\mathsf{Setup}(1^\lambda)$. Output $(\mathsf{crs} = (\mathsf{pk}, \mathsf{crs}_\Pi), \mathsf{td} = (\mathsf{sk}, \mathsf{td}_\Pi))$.

$\underline{\textsc{Prove}}(\mathsf{crs}, x, w)$:

- Compute $\mathsf{ct} = \mathsf{Enc}(\mathsf{pk}, w; r)$ for r sampled uniformly at random.
- Let $x_\Pi = (\mathsf{pk}, x, \mathsf{ct})$ be an instance of the following language $\mathcal{L}_\Pi$:

$$\{(\mathsf{pk}, x, \mathsf{ct}) \ : \ \exists (w, r) \ : \ \mathsf{ct} = \mathsf{Enc}(\mathsf{pk}, w; r) \ \wedge \ (x, w) \in \mathcal{R}\}.$$

- Compute proof $\pi_\Pi \leftarrow \Pi.\mathsf{P}(\mathsf{crs}_\Pi, x_\Pi, (w, r))$ for language $\mathcal{L}_\Pi$.
- Output $\pi = (\mathsf{ct}, \pi_\Pi)$.

$\underline{\textsc{Verify}}(\mathsf{crs}, x, \pi)$:

- Output $\Pi.\mathsf{V}(\mathsf{crs}_\Pi, x_\Pi, \pi_\Pi)$.

Fig. 1. Unclonable Non-Interactive Quantum Protocol for $\mathcal{L} \in \mathsf{NP}$

Theorem 10 (Post-quantum Simulation-Extractable NIZK for NP in the CRS Model). *Let* NP *relation* $\mathcal{R}$ *with corresponding language* $\mathcal{L}$ *be given.*

Let $\Pi = (\mathsf{Setup}, \mathsf{P}, \mathsf{V})$ *be a non-interactive post-quantum simulation sound, adaptively multi-theorem computationally zero-knowledge protocol for* NP*. Let* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *be a post-quantum perfectly correct, IND-CPA secure encryption scheme.*

$(\mathsf{Setup}, \mathsf{P}, \mathsf{V})$ *as defined in Fig. 1 will be a non-interactive post-quantum simulation-extractable, adaptively multi-theorem computationally zero-knowledge argument for* $\mathcal{L}$ *in the common reference string model.*

Corollary 2 (Post-quantum Simulation-Extractable NIZK for NP in the CRS Model). *Assuming the polynomial quantum hardness of LWE, there exists a simulation-extractable, adaptively multi-theorem computationally zero-knowledge argument for* NP *in the common reference string model.*

Proof. This follows from Corollary 1 and Theorem 10.

4.2 Unclonability Definitions

We consider two definitions of unclonability for NIZKs. The first one, motivated by simplicity, informally guarantees that no adversary given honestly proofs for "hard" instances is able to output more than one accepting proof for the same instance.

Definition 3 ((Quantum) Hard Distribution). *Let an* NP *relation* $\mathcal{R}$ *be given.* $(\mathcal{X}, \mathcal{W})$ *is a (quantum) hard distribution over* $\mathcal{R}$ *if the following properties hold.*

- ***Syntax.*** $(\mathcal{X}, \mathcal{W})$ *is indexable by a security parameter* $\lambda \in \mathbb{N}$*. For every choice of* $\lambda \in \mathbb{N}$*, the support of* $(\mathcal{X}_\lambda, \mathcal{W}_\lambda)$ *is over instance and witness pairs* (x, w) *such that* $x \in \mathcal{L}$*,* $|x| = \lambda$*, and* $(x, w) \in \mathcal{R}$*.*
- ***Hardness.*** *For every polynomial-sized (quantum) circuit family* $\mathcal{A} = \{\mathcal{A}_\lambda\}_{\lambda \in \mathbb{N}}$*,*

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

Definition 4. *(Unclonable Security for Hard Instances). A proof* $(\mathsf{Setup}, \mathsf{P}, \mathsf{V})$ *satisfies unclonable security for a language* $\mathcal{L}$ *with corresponding relation* $\mathcal{R}_\mathcal{L}$ *if for every polynomial-sized quantum circuit family* $\{C_\lambda\}_{\lambda \in \mathbb{N}}$*, and for every hard distribution* $\{\mathcal{X}_\lambda, \mathcal{W}_\lambda\}_{\lambda \in \mathbb{N}}$ *over* $\mathcal{R}_\mathcal{L}$*, there exists a negligible function* $\mathsf{negl}(\cdot)$ *such that for every* $\lambda \in \mathbb{N}$*,*

$$\Pr_{(x,w) \leftarrow (\mathcal{X}_\lambda, \mathcal{W}_\lambda)} \left[\mathsf{V}(\mathsf{crs}, x, \pi_1) = 1 \bigwedge \mathsf{V}(\mathsf{crs}, x, \pi_2) = 1 \middle| \begin{smallmatrix} \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda) \\ \pi \leftarrow \mathsf{P}(\mathsf{crs}, x, w) \\ \pi_1, \pi_2 \leftarrow C_\lambda(x, \pi) \end{smallmatrix} \right] \leq \mathsf{negl}(\lambda).$$

We will now strengthen this definition to consider a variant where from any adversary $\mathcal{A}$ that on input a single proof of membership of $x \in \mathcal{L}$ outputs two proofs for x, we can extract a valid witness w for x with high probability. In fact, we can further generalize this definition to a setting where the adversary obtains an even larger number (say $k-1$) input proofs on instances $x_1, \ldots, x_{k-1}$, and outputs k or more proofs. Then we require the extraction of an NP witness corresponding to any proofs that are *duplicated* (i.e. two or more proofs w.r.t. the same instance $x_i \in \{x_1, \ldots, x_{k-1}\}$). We write this definition below.

Definition 5 ($(k-1)$-*to*-k-Unclonable Extractable NIZK). *Let security parameter* $\lambda \in \mathbb{N}$ *and* NP *relation* $\mathcal{R}$ *with corresponding language* $\mathcal{L}$ *be given. Let* $\Pi = (\mathsf{Setup}, \mathsf{P}, \mathsf{V})$ *be given such that* $\mathsf{Setup}, \mathsf{P}$ *and* V *are* $\mathsf{poly}(\lambda)$*-size quantum algorithms. We have that for any* $(x, w) \in \mathcal{R}$*,* $(\mathsf{crs}, \mathsf{td})$ *is the output of* Setup *on input* 1^λ*,* P *receives an instance and witness pair* (x, w) *along with* crs *as input and outputs* π*, and* V *receives an instance* x*,* crs*, and proof* π *as input and outputs a value in* $\{0, 1\}$*.*

Π *is a non-interactive* $(k-1)$*-to-*k*-unclonable zero-knowledge quantum protocol for language* $\mathcal{L}$ *if the following holds:*

- Π *is a quantum non-interactive zero-knowledge protocol for language* $\mathcal{L}$*.*

– $(k-1)$-*to-k*-**Unclonable with Extraction**: *There exists an oracle-aided polynomial-size quantum circuit* $\mathcal{E}$ *such that for every polynomial-size quantum circuit* $\mathcal{A}$*, for every tuple of* $k-1$ *instance-witness pairs* $(x_1,\omega_1),\ldots,(x_{k-1},\omega_{k-1}) \in \mathcal{R}$*, for every instance* x*, if there exists a polynomial* $p(\cdot)$ *such that*

$$\Pr_{\substack{(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Setup}(1^\lambda)\\ \forall \iota\in[k-1],\,\pi_\iota\leftarrow\mathsf{P}(\mathsf{crs},x_\iota,w_\iota)\\ \{\widetilde{x}_\iota,\widetilde{\pi}_\iota\}_{\iota\in[k]}\leftarrow\mathcal{A}(\mathsf{crs},\{x_\iota,\pi_\iota\}_{\iota\in[k-1]})}} \left[\begin{array}{c} \exists\ \mathcal{J}\subseteq\{j:\widetilde{x}_j=x\}\\ s.t.\ |\mathcal{J}|>|\{i:x_i=x\}|\\ and\ \forall\iota\in\mathcal{J},\mathsf{V}(\mathsf{crs},x,\widetilde{\pi}_\iota)=1\end{array}\right] \geq \frac{1}{p(\lambda)},$$

then there is also a polynomial $q(\cdot)$ *such that*

$$\Pr_{w\leftarrow\mathcal{E}^{\mathcal{A}}(x_1,\ldots,x_{k-1},x)}[(x,w)\in\mathcal{R}] \geq \frac{1}{q(\lambda)}.$$

We observe in Definition 5 that we can generically boost the extractor's success probability to $1-\mathsf{negl}(\lambda)$ with respect to a security parameter λ.

Definition 6 (**$(k-1)$-*to-k*-Unclonable Strong-Extractable NIZK).** *Let security parameter* $\lambda\in\mathbb{N}$ *and* NP *relation* $\mathcal{R}$ *with corresponding language* $\mathcal{L}$ *be given. Let* $\Pi=(\mathsf{Setup},\mathsf{P},\mathsf{V})$ *be given such that* $\mathsf{Setup},\mathsf{P}$ *and* V *are* $\mathsf{poly}(\lambda)$*-size quantum algorithms. We have that for any* $(x,w)\in\mathcal{R}$*,* $(\mathsf{crs},\mathsf{td})$ *is the output of* Setup *on input* 1^λ*,* P *receives an instance and witness pair* (x,w) *along with* crs *as input and outputs* π*, and* V *receives an instance* x*,* crs*, and proof* π *as input and outputs a value in* $\{0,1\}$*.*

Π *is a non-interactive* $(k-1)$*-to-*k*-unclonable zero-knowledge quantum protocol for language* $\mathcal{L}$ *if the following holds:*

– Π *is a quantum non-interactive zero-knowledge protocol for language* $\mathcal{L}$*.*
– $(k-1)$-*to-k*-**Unclonable with Strong-Extraction**: *There exists an oracle-aided polynomial-size quantum circuit* $\mathcal{E}$ *such that for every polynomial-size quantum circuit* $\mathcal{A}$ *with non-uniform quantum advice* aux*, for every tuple of* $k-1$ *instance-witness pairs* $(x_1,\omega_1),\ldots,(x_{k-1},\omega_{k-1})\in\mathcal{R}$*, for every instance* x *if there is a polynomial* $p(\cdot)$ *where*

$$\Pr_{\substack{(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Setup}(1^\lambda)\\ \forall \iota\in[k-1],\,\pi_\iota\leftarrow\mathsf{P}(\mathsf{crs},x_\iota,w_\iota)\\ \{\widetilde{x}_\iota,\widetilde{\pi}_\iota\}_{\iota\in[k]}\leftarrow\mathcal{A}(\mathsf{crs},\{x_\iota,\pi_\iota\}_{\iota\in[k-1]},\mathsf{aux})}} \left[\begin{array}{c} \exists\ \mathcal{J}\subseteq\{j:\widetilde{x}_j=x\}\\ s.t.\ |\mathcal{J}|>|\{i:x_i=x\}|\\ and\ \forall\iota\in\mathcal{J},\mathsf{V}(\mathsf{crs},x,\widetilde{\pi}_\iota)=1\end{array}\right] \geq \frac{1}{p(\lambda)},$$

then there is also a polynomial $\mathsf{poly}(\cdot)$ *and a negligible function* $\mathsf{negl}(\cdot)$ *such that*

$$\Pr_{w\leftarrow\mathcal{E}^{\mathcal{A}}(x_1,\ldots,x_{k-1},x,\mathsf{aux}^{\otimes\mathsf{poly}(\lambda)})}[(x,w)\in\mathcal{R}] \geq 1-\mathsf{negl}(\lambda).$$

We describe two useful lemmas to compare the above definitions.

Lemma 1. *Let* $\Pi = (\mathsf{Setup}, \mathsf{P}, \mathsf{V})$ *be a* 1*-to-*2*-unclonable with extraction, non-interactive zero-knowledge quantum protocol (Definition 5). Then,* Π *satisfies Definition 4.*

For a proof of Lemma 1, we refer to the full version [33].

Lemma 2. *Let* $\Pi = (\mathsf{Setup}, \mathsf{P}, \mathsf{V})$ *be a* $(k-1)$*-to-*k*-unclonable with extraction, non-interactive zero-knowledge quantum protocol (Definition 5). Then,* Π *satisfies Definition 6.*

For a proof of Lemma 2, we refer to the full version [33].

From the above lemmas, we conclude that Definition 5 is the strongest definition. In the following sections, we construct a protocol that satisfies Definition 5.

4.3 Unclonable NIZK Implies Public-Key Quantum Money Mini-scheme

Public-Key Quantum Money Mini-Scheme

Let $(\mathcal{X}, \mathcal{W})$ be a hard distribution over a language $\mathcal{L} \in \mathsf{NP}$. Let $\Pi = (\mathsf{Setup}, \mathsf{P}, \mathsf{V})$ be an unclonable non-interactive zero-knowledge protocol for $\mathcal{L}$.

$\underline{\textsc{Gen}}(1^\lambda)$: Sample a hard instance-witness pair $(x, w) \leftarrow (\mathcal{X}, \mathcal{Y})$, a common reference string $(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda, x)$, and a proof $\pi \leftarrow \mathsf{P}(\mathsf{crs}, x, w)$. Output $(\rho_\$ = \pi, s = (\mathsf{crs}, x))$.

$\underline{\textsc{Verify}}(\rho_\$, s)$: Parse $\rho_\$ = \pi$ and $s = (\mathsf{crs}, x)$. Output $\mathsf{V}(\mathsf{crs}, x, \pi)$.

Fig. 2. Public-Key Quantum Money Mini-Scheme from an Unclonable Non-Interactive Quantum Protocol

Theorem 11. *Let* $(\mathcal{X}, \mathcal{W})$ *be a hard distribution over a language* $\mathcal{L} \in \mathsf{NP}$*. Let* $\Pi = (\mathsf{Setup}, \mathsf{P}, \mathsf{V})$ *satisfy Definition 4. Then* $(\mathsf{Setup}, \mathsf{P}, \mathsf{V})$ *implies a public-key quantum money mini-scheme as described in Fig. 2.*

We defer the proof to the full version [33].

4.4 Construction and Analysis of Unclonable-Extractable NIZK in CRS Model

Unclonable Non-Interactive ZK for $\mathcal{L} \in \mathsf{NP}$

Let $\Pi = (\mathsf{Setup}, \mathsf{P}, \mathsf{V})$ be a non-interactive simulation-extractable, adaptively multi-theorem computationally zero-knowledge protocol for NP, Com be a post-quantum perfectly binding, computationally hiding commitment scheme, and $(\mathsf{NoteGen}, \mathsf{Ver})$ be a public-key quantum money scheme. Let $\mathcal{R}$ be the relation with respect to $\mathcal{L} \in \mathsf{NP}$.

$\textsc{Setup}(1^\lambda)$: Sample the common reference string $(\mathsf{crs}_\Pi, \mathsf{td}_\Pi) \leftarrow \Pi.\mathsf{Setup}(1^\lambda)$, and s^*, r^* uniformly at random. Define $c = \mathsf{Com}(s^*; r^*)$ and output $(\mathsf{crs} = (\mathsf{crs}_\Pi, c), \mathsf{td} = \mathsf{td}_\Pi)$.

$\textsc{Prove}(\mathsf{crs}, x, w)$:

- Compute a quantum note and associated serial number $(\rho_\$, s) \leftarrow \mathsf{NoteGen}$.
- Let $x_\Pi = (c, x, s)$ be an instance of the following language $\mathcal{L}_\Pi$:

$$\{(c, x, s) \ : \ \exists z \ : \ (x, z) \in \mathcal{R} \ \vee \ c = \mathsf{Com}(s; z)\}.$$

- Compute proof $\pi_\Pi \leftarrow \Pi.\mathsf{P}(\mathsf{crs}_\Pi, x_\Pi, w)$ for language $\mathcal{L}_\Pi$.
- Output $\pi = (\rho_\$, s, \pi_\Pi)$.

$\textsc{Verify}(\mathsf{crs}, x, \pi)$:

- Check that $\mathsf{Ver}(\rho_\$, s)$ outputs 1 and that $\Pi.\mathsf{V}(\mathsf{crs}_\Pi, x_\Pi, \pi_\Pi)$ outputs 1.
- If both checks pass, output 1. Otherwise, output 0.

Fig. 3. Unclonable Non-Interactive Quantum Protocol for $\mathcal{L} \in \mathsf{NP}$

Theorem 12. *Let $k(\cdot)$ be a polynomial. Let NP relation $\mathcal{R}$ with corresponding language $\mathcal{L}$ be given.*

Let $(\mathsf{NoteGen}, \mathsf{Ver})$ be a public-key quantum money mini-scheme and Com be a post-quantum commitment scheme. Let $\Pi = (\mathsf{Setup}, \mathsf{P}, \mathsf{V})$ be a non-interactive post-quantum simulation-extractable, adaptive multi-theorem computational zero-knowledge protocol for NP.

$(\mathsf{Setup}, \mathsf{P}, \mathsf{V})$ as defined in Fig. 3 will be a non-interactive quantum simulation-extractable, adaptive multi-theorem computationally zero-knowledge, and $(k-1)$-to-k-unclonable argument with extraction protocol for $\mathcal{L}$ in the common reference string model (Definition 5).

Proof. Completeness follows from perfect correctness of the public key quantum money scheme, and perfect completeness of Π.

See the full version [33] for proofs of zero-knowledge and simulation extractability.

Let $\Pi.\mathsf{Sim} = (\Pi.\mathsf{Sim}_0, \Pi.\mathsf{Sim}_1)$ be the adaptive multi-theorem computationally zero-knowledge simulator of Π. We define Sim_0 with oracle access to $\Pi.\mathsf{Sim}_0$ as follows: *Input*: 1^λ.

(1) Send 1^λ to $\Pi.\mathsf{Sim}_0$. Receive $(\mathsf{crs}_\Pi, \mathsf{td}_\Pi)$ from $\Pi.\mathsf{Sim}_0$.
(2) Sample s^*, r^* uniformly at random. Define $c = \mathsf{Com}(s^*; r^*)$.
(3) Output $\mathsf{crs} = (\mathsf{crs}_\Pi, c)$ and $\mathsf{td} = \mathsf{td}_\Pi$.

We define Sim_1 with oracle access to $\Pi.\mathsf{Sim}_1$ as follows:
Input: $\mathsf{crs} = (\mathsf{crs}_\Pi, c)$, $\mathsf{td} = \mathsf{td}_\Pi$, x.

(1) Sample $(\rho_\$, s) \leftarrow \mathsf{NoteGen}(1^\lambda)$.
(2) Define $x_\Pi = (c, x, s)$. Send $(\mathsf{crs}_\Pi, \mathsf{td}_\Pi, x_\Pi)$ to $\Pi.\mathsf{Sim}_1$. Receive π_Π from $\Pi.\mathsf{Sim}_1$.
(3) Output $\pi = (\rho_\$, s, \pi_\Pi)$.

Claim (4.1). Let Ext be as defined earlier, in the current proof of simulation-extractability. There exists a negligible function $\mathsf{negl}(\cdot)$ such that for every polynomial-size quantum circuit $\mathcal{B}$,

$$\Pr_{\substack{(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Sim}_0(1^\lambda)\\ (x,\pi)\leftarrow\mathcal{B}^{\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},\cdot)}(\mathsf{crs})\\ w\leftarrow\mathsf{Ext}(\mathsf{crs},\mathsf{td},x,\pi)}} [\Pi.\mathsf{V}(\mathsf{crs}_\Pi, x_\Pi, \pi_\Pi) = 1 \wedge x_\Pi \notin Q_\Pi \wedge (x, w) \notin \mathcal{R}] \leq \mathsf{negl}(\lambda)$$

where Q_Π is the list of queries forwarded by Sim_1 to $\Pi.\mathsf{Sim}_1$.

See the full version [33] for proof of Claim 4.1.

Unclonable Extractability. Let $\Pi.\mathsf{Sim} = (\Pi.\mathsf{Sim}_0, \Pi.\mathsf{Sim}_1)$ be the adaptive multi-theorem computationally zero-knowledge simulator of Π. Let $\Pi.\mathsf{Ext}$ be the simulation-extraction extractor of Π with respect to $\Pi.\mathsf{Sim}$. Let $\mathsf{Sim} = (\mathsf{Sim}_0, \mathsf{Sim}_1)$ be the simulator, with oracle access to $\Pi.\mathsf{Sim}$, as defined in the proof that Fig. 3 is adaptive multi-theorem computational zero-knowledge. Let Ext be the extractor, based on Sim, as defined in the proof that Fig. 3 is simulation-extractable. We define $\mathcal{E}$ with oracle access to Sim, Ext, and some $\mathcal{A}$ as follows:
Hardwired: $x_1, \ldots, x_{k-1}$, x

(1) Send 1^λ to Sim_0. Receive $(\mathsf{crs}, \mathsf{td})$ from Sim_0.
(2) For $\iota \in [k-1]$: send $(\mathsf{crs}, \mathsf{td}, x_\iota)$ to Sim_1, and receive π_ι from Sim_1.
(3) Send $(\mathsf{crs}, \{x_\iota, \pi_\iota\}_{\iota\in[k-1]})$ to $\mathcal{A}$. Receive $\{\widetilde{x_\iota}, \widetilde{\pi_\iota}\}_{\iota\in[k]}$ from $\mathcal{A}$.
(4) Define j' uniformly at random from $[k]$.
(5) Output $\mathsf{Ext}(\mathsf{crs}, \mathsf{td}, x, \widetilde{\pi_{j'}})$ as w.

Let $\mathcal{A}$, $(x_1, w_1), \ldots, (x_{k-1}, w_{k-1}) \in \mathcal{R}$, x, polynomial $p(\cdot)$, and negligible function $\mathsf{negl}(\cdot)$ be given such that $\mathcal{A}$ outputs more accepting proofs for x than $\mathcal{A}$ received, and yet the extractor $\mathcal{E}$ is unable to extract a valid witness for x from $\mathcal{A}$. Restated more formally, that is that

$$\Pr_{\substack{(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Setup}(1^\lambda)\\ \forall\iota\in[k-1],\,\pi_\iota\leftarrow\mathsf{P}(\mathsf{crs},x_\iota,w_\iota)\\ \{\widetilde{x_\iota},\widetilde{\pi_\iota}\}_{\iota\in[k]}\leftarrow\mathcal{A}(\mathsf{crs},\{x_\iota,\pi_\iota\}_{\iota\in[k-1]})}} \left[\begin{array}{c} \exists\ \mathcal{J}\subseteq\{j : \widetilde{x}_j = x\} \\ \text{s.t. } |\mathcal{J}| > |\{i : x_i = x\}| \\ \text{and } \forall\iota\in\mathcal{J}, \mathsf{V}(\mathsf{crs}, x, \widetilde{\pi_\iota}) = 1 \end{array}\right] \geq \frac{1}{p(\lambda)}, \quad (1)$$

and for all polynomials $p'(\cdot)$ (there are infinitely many λ) such that

$$\Pr_{w \leftarrow \mathcal{E}^{\mathcal{A}}(x_1,\ldots,x_{k-1},x)}[(x,w) \in \mathcal{R}] \leq \frac{1}{p'(\lambda)}. \tag{2}$$

We parse the output of the adversary $\mathcal{A}$ as $\widetilde{\pi}_\iota = (\widetilde{\rho_{\$,\iota}}, \widetilde{s_\iota}, \widetilde{\pi_{\Pi,\iota}})$ for all $\iota \in [k]$.

Given Eq. (1), we may be in one of the two following cases: either $\mathcal{A}$ generates two accepting proofs which have the same serial number as an honestly generated proof (for an infinite set of λ), or $\mathcal{A}$ does not (for an infinite set of λ). We consider that either of these two scenarios occur with at least $1/(2p(\lambda))$ probability and show that each reaches a contradiction.

Scenario One

Say that (for an infinite set of λ) $\mathcal{A}$ generates two accepting proofs which have the same serial number as an honestly generated proof with at least $1/(2p(\lambda))$ probability. Symbolically,

$$\Pr_{\substack{(\mathsf{crs},\mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda) \\ \forall \iota \in [k-1],\, \pi_\iota \leftarrow \mathsf{P}(\mathsf{crs}, x_\iota, w_\iota) \\ \{\widetilde{x}_\iota, \widetilde{\pi}_\iota\}_{\iota \in [k]} \leftarrow \mathcal{A}(\mathsf{crs}, \{x_\iota, \pi_\iota\}_{\iota \in [k-1]})}} \left[\begin{array}{c} \exists\ \mathcal{J} \subseteq \{j : \widetilde{x}_j = x\} \\ \text{s.t. } |\mathcal{J}| > |\{i : x_i = x\}| \\ \text{and } \forall \iota \in \mathcal{J}, \mathsf{V}(\mathsf{crs}, x, \widetilde{\pi}_\iota) = 1 \\ \text{and } \exists i^* \in [k-1]\ \exists j^*, \ell^* \in \mathcal{J} \\ \text{s.t. } s_{i^*} = \widetilde{s_{j^*}} = \widetilde{s_{\ell^*}} \end{array} \right] \geq \frac{1}{2p(\lambda)}. \tag{3}$$

Through a hybrid argument, we can get a similar event with fixed indices i^*, j^*, and ℓ^* which belong to their respective sets with an advantage of $1/(2k^3p(\lambda))$. By using the advantage of $\mathcal{A}$ in this game, we can show a reduction that breaks the unforgeability of the quantum money scheme. We will now outline this reduction.

Reduction: to unforgeability of quantum money scheme given oracle access to $\mathcal{A}$.

Hardwired with: $(x_1, w_1), \ldots, (x_{k-1}, w_{k-1})$, x, i^*, j^*, ℓ^*.

(1) Compute $(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)$ where $\mathsf{crs} = (\mathsf{crs}_\Pi, c)$ and $\mathsf{td} = \mathsf{td}_\Pi$.
(2) Receive $(\rho_\$, s) \leftarrow \mathsf{NoteGen}$ from the challenger.
(3) Define $\rho_{\$,i^*} = \rho_\$$, $s_{i^*} = s$, and $x_\Pi = (c, x_{i^*}, s_{i^*})$.
Compute $\pi_{\Pi,\ell} \leftarrow \Pi.\mathsf{P}(\mathsf{crs}_\Pi, x_\Pi, w_{i^*})$. Define $\pi_{i^*} = (\rho_{\$,i^*}, s_{i^*}, \pi_{\Pi,i^*})$.
(4) Define $\pi_\iota \leftarrow \mathsf{P}(\mathsf{crs}, x_\iota, w_\iota)$ for $\iota \in [k-1] \setminus \{i^*\}$.
(5) Send $\{x_\iota, \pi_\iota\}_{\iota \in [k-1]}$ to $\mathcal{A}$.
(6) Receive $\{\widetilde{x}_\iota, \widetilde{\pi}_\iota\}_{\iota \in [k]}$ from $\mathcal{A}$.
(7) Parse $\widetilde{\pi_{j^*}} = (\widetilde{\rho_{\$,j^*}}, \widetilde{s_{j^*}}, \widetilde{\pi_{\Pi,j^*}})$ and $\widetilde{\pi_{\ell^*}} = (\widetilde{\rho_{\$,\ell^*}}, \widetilde{s_{\ell^*}}, \widetilde{\pi_{\Pi,\ell^*}})$.
(7) Send $(\widetilde{\rho_{\$,j^*}}, \widetilde{\rho_{\$,\ell^*}})$ to the challenger.

Given the event in Eq. (3) holds (for the afore mentioned fixed indices), then the reduction will return two quantum money states with the same serial number as the challenger sent. With advantage $1/(2k^3p(\lambda))$, the reduction will succeed at breaking unforgeability of the quantum money scheme, thus reaching a contradiction.

Scenario Two.

Alternatively, say that (for an infinite set of λ) $\mathcal{A}$ does not generate two accepting proofs which have the same serial number as an honestly generated

proof with at least $1/(2p(\lambda))$ probability. By the pigeon-hole principle, this means that $\mathcal{A}$ generates an accepting proof with a serial number which is not amongst the ones it received. In summary, we have that

$$\Pr_{\substack{(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Setup}(1^\lambda)\\ \forall \iota\in[k-1],\,\pi_\iota\leftarrow\mathsf{P}(\mathsf{crs},x_\iota,w_\iota)\\ \{\widetilde{x_\iota},\widetilde{\pi_\iota}\}_{\iota\in[k]}\leftarrow\mathcal{A}(\mathsf{crs},\{x_\iota,\pi_\iota\}_{\iota\in[k-1]})}}\left[\begin{array}{c}\exists\ \mathcal{J}\subseteq\{j:\widetilde{x}_j=x\}\\ \text{s.t. } |\mathcal{J}|>|\{i:x_i=x\}|\\ \text{and } \forall\iota\in\mathcal{J},\mathsf{V}(\mathsf{crs},x,\widetilde{\pi_\iota})=1\\ \text{and } \exists j^*\in\mathcal{J}\text{ s.t. }\widetilde{s_{j^*}}\notin\{s_\iota\}_{\iota\in[k-1]}\end{array}\right]\geq\frac{1}{2p(\lambda)}. \tag{4}$$

Through an averaging argument, we can get a similar event with a fixed index j^* that belongs to the event's set $\mathcal{J}$ with an advantage of $1/(2kp(\lambda))$. We will now switch to a hybrid where we provide $\mathcal{A}$ with simulated proofs.

Claim (Claim 4.2). There exists a polynomial $q(\cdot)$ such that

$$\Pr_{\substack{(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Sim}_0(1^\lambda)\\ \forall \iota\in[k-1],\,\pi_\iota\leftarrow\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},x_\iota)\\ \{\widetilde{x_\iota},\widetilde{\pi_\iota}\}_{\iota\in[k]}\leftarrow\mathcal{A}(\mathsf{crs},\{x_\iota,\pi_\iota\}_{\iota\in[k-1]})}}\left[\begin{array}{c}\exists\ \mathcal{J}\subseteq\{j:\widetilde{x}_j=x\}\\ \text{s.t. } |\mathcal{J}|>|\{i:x_i=x\}|\\ \text{and } \forall\iota\in\mathcal{J},\mathsf{V}(\mathsf{crs},x,\widetilde{\pi_\iota})=1\\ \text{and } j^*\in\mathcal{J}\\ \text{and } \widetilde{s_{j^*}}\notin\{s_\iota\}_{\iota\in[k-1]}\end{array}\right]\geq\frac{1}{q(\lambda)}. \tag{5}$$

We will later see a proof of Sect. 4.4. For now, assuming that this claim holds, by the definition of $\mathcal{E}$, Eq. (2), and Eq. (5), there exists a polynomial $q'(\cdot)$ such that

$$\Pr_{\substack{(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Sim}_0(1^\lambda)\\ \forall \iota\in[k-1],\,\pi_\iota\leftarrow\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},x_\iota)\\ \{\widetilde{x_\iota},\widetilde{\pi_\iota}\}_{\iota\in[k]}\leftarrow\mathcal{A}(\mathsf{crs},\{x_\iota,\pi_\iota\}_{\iota\in[k-1]})\\ j'\xleftarrow{\$}[k]\\ w\leftarrow\mathsf{Ext}(\mathsf{crs},\mathsf{td},x,\widetilde{\pi_{j'}})}}\left[\begin{array}{c}\exists\ \mathcal{J}\subseteq\{j:\widetilde{x}_j=x\}\\ \text{s.t. } |\mathcal{J}|>|\{i:x_i=x\}|\\ \text{and } \forall\iota\in\mathcal{J},\mathsf{V}(\mathsf{crs},x,\widetilde{\pi_\iota})=1\\ \text{and } j^*\in\mathcal{J}\\ \text{and } \widetilde{s_{j^*}}\notin\{s_\iota\}_{\iota\in[k-1]}\\ \text{and } (x,w)\notin\mathcal{R}\end{array}\right]\geq\frac{1}{q'(\lambda)}.$$

We will additionally have that $j'=j^*$ with advantage at least $1/(kq'(\lambda))$. Since V accepts $\widetilde{\pi_{j^*}}$ with respect to x, $\Pi.\mathsf{V}$ must accept $\widetilde{\pi_{\Pi,j^*}}$ with respect to $\widetilde{x_{\Pi,j^*}}=(c,x,\widetilde{s_{j^*}})$. Since $\widetilde{s_{j^*}}\notin\{s_\iota\}_{\iota\in[k-1]}$, we have that $\Pi.\mathsf{Sim}_1$, through Sim_1, has not previously received $\widetilde{x_{\Pi,j^*}}$ as a query. As such, we have that

$$\Pr_{\substack{(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Sim}_0(1^\lambda)\\ \forall \iota\in[k-1],\,\pi_\iota\leftarrow\mathsf{Sim}_1(\mathsf{crs},\mathsf{td},x_\iota)\\ \{\widetilde{x_\iota},\widetilde{\pi_\iota}\}_{\iota\in[k]}\leftarrow\mathcal{A}(\mathsf{crs},\{x_\iota,\pi_\iota\}_{\iota\in[k-1]})\\ w\leftarrow\mathsf{Ext}(\mathsf{crs},\mathsf{td},\widetilde{x_{j^*}},\widetilde{\pi_{j^*}})}}\left[\begin{array}{c}\Pi.\mathsf{V}(\mathsf{crs}_\Pi,(c,x,\widetilde{s_{j^*}}),\widetilde{\pi_{\Pi,j^*}})=1\\ \text{and } (c,x,\widetilde{s_{j^*}})\notin Q_\Pi\\ \text{and } (x,w)\notin\mathcal{R}\end{array}\right]\geq\frac{1}{kq'(\lambda)} \tag{6}$$

where Q_Π is the set of queries asked through Sim_1 to $\Pi.\mathsf{Sim}_1$. We now define $\mathcal{B}$ with oracle access to $\mathcal{A}$ and Sim_1[1]:

[1] Here, $\mathcal{B}$ is given oracle access to Sim_1 which has the terms $(\mathsf{crs},\mathsf{td})$ fixed by the output of Sim_0.

Hardwired: $x_1, \ldots, x_{k-1}$, x j^*
Input: $\mathsf{crs} = (\mathsf{crs}_\Pi, c)$

(1) For $\iota \in [k-1]$: send x_ι to Sim_1, and receive π_ι from Sim_1.
(2) Send $(\mathsf{crs}, \{x_\iota, \pi_\iota\}_{\iota \in [k-1]})$ to $\mathcal{A}$. Receive $\{\widetilde{x_\iota}, \widetilde{\pi_\iota}\}_{\iota \in [k]}$ from $\mathcal{A}$.
(3) Output $((c, x, \widetilde{s_{j^*}}), \widetilde{\pi_{j^*}})$.

Given that the event in Eq. (6) holds, then $\mathcal{B}$ contradicts Sect. 4.4. Thus, all that remains to be proven is Sect. 4.4.

See the full version [33] for a proof of Claim 4.2.

By completing the proofs of our claim, we have concluding the proof of our theorem statement.

Corollary 3. *Assuming the polynomial quantum hardness of LWE, injective one-way functions exist, and post-quantum iO exists, there exists a non-interactive adaptive argument of knowledge, adaptive computationally zero-knowledge, and* $(k-1)$*-to-k-unclonable argument with extraction protocol for* NP *in the common reference string model (Definition 5).*

Proof. This follows from Theorem 5, Corollary 2, Theorem 9, and Theorem 12.

We have thus shown that Fig. 3 is an unclonable NIZK AoK in the CRS model as defined according to our proposed unclonability definition, Definition 5.

In the upcoming sections, we will consider unclonable proof systems in the QROM.

5 Unclonable NIZK in the Quantum Random Oracle Model

5.1 A Modified Sigma Protocol

We will begin by introducing a slightly modified sigma protocol. In the coming sections, our construction will involve applying Fiat-Shamir to this modified protocol.

Theorem 13. *Let a post-quantum sigma protocol with unpredictable commitments* Π *be given. Let* $\mathcal{R}_\Pi$ *be an* NP *relation. Let* $\mathcal{R} = \{((x, \mathcal{S}), w) : (x, w) \in \mathcal{R}_\Pi \wedge \mathcal{S} \neq \emptyset\}$*. We argue that the following protocol will be a post-quantum sigma protocol with unpredictable commitments:*

- $\mathsf{P.Com}(1^\lambda, (x, \mathcal{S}), w)$*: Sends* (x, α, s) *to* V *where* $(\alpha, \mathsf{st}) \leftarrow \Pi.\mathsf{P.Com}(1^\lambda, x, w)$ *and* s *is sampled from* $\mathcal{S}$*.*
- $\mathsf{V.Ch}(1^\lambda, (x, \mathcal{S}), (x, \alpha, s))$*: Sends* β *to* P *where* $\beta \leftarrow \Pi.\mathsf{V.Ch}(1^\lambda, x, \alpha)$*.*
- $\mathsf{P.Com}(1^\lambda, (x, \mathcal{S}), w, \mathsf{st}, \beta)$*: Sends* γ *to* V *where* $\gamma \leftarrow \Pi.\mathsf{P.Prove}(1^\lambda, x, w, \mathsf{st}, \beta)$*.*
- $\mathsf{V.Ver}(1^\lambda, (x, \mathcal{S}), (x, \alpha, s), \beta, \gamma)$*: 1 iff* $s \in \mathsf{Support}(\mathcal{S})$ *and* $\Pi.\mathsf{V.Ver}(1^\lambda, x, \alpha, \beta, \gamma) = 1$*.*

See the full version [33] for the proof of Theorem 13.

Corollary 4. *The Fiat-Shamir transform applied to the post-quantum sigma protocol defined in Theorem 13 yields a classical post-quantum NIZKAoK* Π' *in the QROM.*

Proof. This follows by Theorem 13 and Theorem 8.

5.2 Unclonability Definitions

Unclonable NIZKs in the quantum random oracle model are defined analogously to the CRS model – we repeat these definitions in the QRO model for completeness in the full version [33].

5.3 Unclonable NIZK Implies Public-Key Quantum Money Mini-Scheme in QROM

We defer the construction and proof to the full version [33]; below we state our results.

Theorem 14. *Let* $\mathcal{O}$ *be a quantum random oracle. Let* $(\mathcal{X}, \mathcal{W})$ *be a hard distribution over a language* $\mathcal{L} \in \mathsf{NP}$*. Let* $\Pi = (\mathsf{P}, \mathsf{V})$ *be a* 1*-to-*2 *unclonable non-interactive perfectly complete, computationally zero-knowledge protocol for* $\mathcal{L}$ *in the QRO model.*

Then (P, V) *implies a public-key quantum money mini-scheme in the QRO model.*

5.4 Construction and Analysis of Unclonable-Extractable NIZK in QROM

We now introduce our construction in Fig. 4 and prove the main theorem of this section.

Theorem 15. *Let* $k(\cdot)$ *be a polynomial. Let* NP *relation* $\mathcal{R}$ *with corresponding language* $\mathcal{L}$ *be given.*

Let $(\mathsf{NoteGen}, \mathsf{Ver})$ *be a public-key quantum money mini-scheme and* $\Pi = (\mathsf{P}, \mathsf{V})$ *be a post-quantum sigma protocol.*

(P, V) *as defined in Fig. 4 will be a non-interactive knowledge sound, computationally zero-knowledge, and* $(k-1)$*-to-*k*-unclonable argument with extraction protocol for* $\mathcal{L}$ *in the quantum random oracle model.*

Proof. Let the parameters and primitives be as given in the theorem statement. We argue that completeness follows from the protocol construction in Fig. 4, and we prove the remaining properties below.

See the full version [33] for complete proofs of argument of knowledge and zero-knowledge properties.

Unclonable NIZK for NP in the QROM

Let $\mathcal{O}$ be a random oracle. Let $\Pi = (\mathsf{P} = (\mathsf{P.Com}, \mathsf{P.Prove}), \mathsf{V} = (\mathsf{V.Ch}, \mathsf{V.Ver}))$ be a post-quantum sigma protocol with unpredictable commitments, and $(\mathsf{NoteGen}, \mathsf{Ver})$ be a public-key quantum money mini-scheme. Let $\mathcal{R}$ be the relation with respect to $\mathcal{L} \in \mathsf{NP}$.

$\textsc{Prove}^{\mathcal{O}}(x, \omega)$:

- Compute a quantum note and associated serial number $(\rho_\$, s) \leftarrow \mathsf{NoteGen}(1^\lambda)$.
- Compute $(\alpha, \zeta) \leftarrow \mathsf{P.Com}(x, \omega)$.
- Query $\mathcal{O}$ at (x, α, s) to get β.
- Compute $\gamma \leftarrow \mathsf{P.Prove}(x, \omega, \beta, \zeta)$.
- Output $\pi = (\rho_\$, s, \alpha, \beta, \gamma)$.

$\textsc{Verify}^{\mathcal{O}}(x, \pi)$:

- Check that $\mathsf{Ver}(\rho_\$, s)$ outputs 1.
- Check that $\mathcal{O}$ outputs β when queried at (x, α, s).
- Output the result of $\mathsf{V.Ver}(x, \alpha, \beta, \gamma)$.

Fig. 4. Unclonable Non-Interactive Quantum Protocol for $\mathcal{L} \in \mathsf{NP}$ in the Quantum Random Oracle Model

Let $\mathcal{S}$ be the distribution of serial numbers as output by $\mathsf{NoteGen}(1^\lambda)$. We define Ext[2] with oracle-access to Ext_{FS}, $\mathcal{O}$, and some $\mathcal{A}$ as follows:
Hardwired with: $\mathcal{S}$.
Input: x.

(1) Given an oracle-query (x, α, s) from $\mathcal{A}$: send (x, α, s) to $\mathcal{O}$, receive β from $\mathcal{O}$, and send β to $\mathcal{A}$.
(2) Upon receiving $\pi = (\rho_\$, s, \alpha, \beta, \gamma)$ from $\mathcal{A}$: send $\pi_{FS} = ((x, \alpha, s), \beta, \gamma)$ to Ext_{FS}.
(3) Output the result of Ext_{FS} as w.

Let Sim_{FS} be the simulator for Π' in Corollary 4 (where Π instantiates Theorem 13). Let $\mathcal{R}_{FS}$ be the relation for Π' with respect to $\mathcal{R}$. We define Sim with oracle-access to Sim_{FS} and program access to some random oracle $\mathcal{O}$ as follows:
Input: x (ignores any witnesses it may receive).

(1) Sample $(\rho_\$, s) \leftarrow \mathsf{NoteGen}(1^\lambda)$.
(2) Let $\mathcal{S}$ be the distribution where all probability mass is on s.
(3) Compute $((x, \alpha, s), \beta, \gamma) \leftarrow \Pi.\mathsf{Sim}(x, \mathcal{S})$. Allow $\Pi.\mathsf{Sim}$ to program $\mathcal{O}$ at (x, α, s) to return β.
(5) Output $\pi = (\rho_\$, s, \alpha, \beta, \gamma)$.

[2] An extractor whose local code is implementable as a simple unitary which allows for straightforward rewinding.

Unclonable Extractability. Let Ext be the quantum circuit of the extractor we defined earlier (in our proof that Fig. 4 is an argument of knowledge). Let Sim be the quantum circuit of the simulator that we defined earlier (in our proof that Fig. 4 is a zero-knowledge protocol). We define a simulator for our extractor, SimExt, which interacts with some $\mathcal{A}$ and has oracle-access to $\mathcal{O}$ as follows:
Hardwired with: $x_1, \ldots, x_{k-1}$, x

(1) Compute $\pi_\iota \leftarrow \mathsf{Sim}(x_\iota)$ for $\iota \in [k-1]$ where we store all points Sim would program into a list $\mathcal{P}$.
(2) Send $\{x_\iota, \pi_\iota\}_{\iota \in [k-1]}$ to $\mathcal{A}$.
(3) For every query from $\mathcal{A}$, if the query is in $\mathcal{P}$, then reply with the answer from $\mathcal{P}$. Else, forward the query to $\mathcal{O}$ and send the answer back to $\mathcal{A}$.

We now define our extractor $\mathcal{E}$ with oracle-access to some $\mathcal{A}$ as follows:
Hardwired with: some choice of $x_1, \ldots, x_{k-1}$, x.

(1) Instantiates a simulatable and extractable random oracle $\mathcal{O}$. Runs Ext on $\mathcal{O}$ throughout the interaction with $\mathcal{A}$ (which may involve rewinding, in which case we would rewind $\mathcal{A}$ and repeat the following steps).
(2) Run $\mathsf{SimExt}^{\mathcal{O}}(x_1, \ldots, x_{k-1}, x)$ which interacts with $\mathcal{A}$.
(3) Receive $\{\widetilde{x_\iota}, \widetilde{\pi_\iota}\}_{\iota \in [k]}$ from $\mathcal{A}$.
(4) Samples $\ell \in [k]$ uniformly at random. Send $\widetilde{\pi_\ell}$ to Ext.
(5) Outputs the result of Ext as w.

Let $\mathcal{A}$, $(x_1, w_1), \ldots, (x_{k-1}, w_{k-1}) \in \mathcal{R}$, x, polynomial $p(\cdot)$, and negligible function $\mathsf{negl}(\cdot)$ be given such that $\mathcal{A}$ outputs more accepting proofs for x than $\mathcal{A}$ received, and yet the extractor $\mathcal{E}$ is unable to extract a valid witness for x from $\mathcal{A}$. Restated more formally, that is that

$$\Pr_{\substack{\mathcal{O} \\ \forall \iota \in [k-1],\, \pi_\iota \leftarrow \mathsf{P}^{\mathcal{O}}(x_\iota, w_\iota) \\ \{\widetilde{x_\iota}, \widetilde{\pi_\iota}\}_{\iota \in [k]} \leftarrow \mathcal{A}^{\mathcal{O}}(\{x_\iota, \pi_\iota\}_{\iota \in [k-1]})}} \left[\begin{array}{c} \exists\, \mathcal{J} \subseteq \{j : \widetilde{x}_j = x\} \\ \text{s.t. } |\mathcal{J}| > |\{i : x_i = x\}| \\ \text{and } \forall \iota \in \mathcal{J}, \mathsf{V}^{\mathcal{O}}(x, \widetilde{\pi_\iota}) = 1 \end{array} \right] \geq \frac{1}{p(\lambda)}, \quad (7)$$

and for all polynomials $p'(\cdot)$ (there are infinitely many λ) such that

$$\Pr_{w \leftarrow \mathcal{E}^{\mathcal{A}}(x_1, \ldots, x_{k-1}, x)} [(x, w) \in \mathcal{R}] \leq \frac{1}{p'(\lambda)}. \quad (8)$$

We parse the output of the adversary $\mathcal{A}$ as $\widetilde{\pi_\iota} = (\widetilde{\rho_{\$,\iota}}, \widetilde{s_\iota}, \widetilde{\alpha_\iota}, \widetilde{\beta_\iota}, \widetilde{\gamma_\iota})$ for all $\iota \in [k]$.

Given Eq. (7), we may be in one of the two following cases: either $\mathcal{A}$ generates two accepting proofs which have the same serial number as a honestly generated proof (for an infinite set of λ), or $\mathcal{A}$ does not (for an infinite set of λ). We consider that either of these two scenarios occur with at least $1/(2p(\lambda))$ probability and show that each reaches a contradiction.

Scenario One.
Say that (for an infinite set of λ) $\mathcal{A}$ generates two accepting proofs which have the same serial number as an honestly generated proof with at least $1/(2p(\lambda))$ probability. Symbolically,

$$\Pr_{\substack{\mathcal{O} \\ \forall \iota \in [k-1],\, \pi_\iota \leftarrow \mathsf{P}^{\mathcal{O}}(x_\iota, w_\iota) \\ \{\widetilde{x_\iota}, \widetilde{\pi_\iota}\}_{\iota \in [k]} \leftarrow \mathcal{A}^{\mathcal{O}}(\{x_\iota, \pi_\iota\}_{\iota \in [k-1]})}} \left[\begin{array}{c} \exists\, \mathcal{J} \subseteq \{j : \widetilde{x}_j = x\} \\ \text{s.t. } |\mathcal{J}| > |\{i : x_i = x\}| \\ \text{and } \forall \iota \in \mathcal{J}, \mathsf{V}^{\mathcal{O}}(x, \widetilde{\pi}_\iota) = 1 \\ \text{and } \exists i^* \in [k-1]\ \exists j^*, \ell^* \in \mathcal{J} \\ \text{s.t. } s_{i^*} = \widetilde{s_{j^*}} = \widetilde{s_{\ell^*}} \end{array} \right] \geq \frac{1}{2p(\lambda)}. \quad (9)$$

Through a hybrid argument, we can get a similar event with fixed indices i^*, j^*, and ℓ^* which belong to their respective sets with an advantage of $1/(2k^3p(\lambda))$. By using the advantage of $\mathcal{A}$ in this game, we can show a reduction that breaks the unforgeability of the quantum money scheme. We will now outline this reduction.
Reduction: to unforgeability of quantum money scheme given oracle access to $\mathcal{A}$ and $\mathcal{O}$.
Hardwired with: $(x_1, w_1), \ldots, (x_{k-1}, w_{k-1})$, x, i^*, j^*, ℓ^*.

(1) Receive $(\rho_\$, s)$ from the challenger.
(2) Define $\rho_{\$,i^*} = \rho_\$$ and $s_{i^*} = s$. Sample $(\rho_{\$,\iota}, s_\iota) \leftarrow \mathsf{NoteGen}(1^\lambda)$ for $\iota \in [k-1] \setminus \{i^*\}$. Compute $(\alpha_\iota, \zeta_\iota) \leftarrow \Pi.\mathsf{P}.\mathsf{Com}(x_\iota, w_\iota)$, query $\mathcal{O}$ at $(x_\iota, \alpha_\iota, s_\iota)$ to get β_ι, compute $\gamma_\iota \leftarrow \Pi.\mathsf{P}.\mathsf{Prove}(x_\iota, w_\iota, \beta_\iota, \zeta_\iota)$, and define $\pi_\iota = (\rho_{\$,\iota}, s_\iota, \alpha_\iota, \beta_\iota, \gamma_\iota)$ for $\iota \in [k-1]$.
(3) Send $\{x_\iota, \pi_\iota\}_{\iota \in [k-1]}$ to $\mathcal{A}$.
(4) Receive $\{\widetilde{\pi}_\iota\}_{\iota \in [k]}$ from $\mathcal{A}$.
(5) Send $(\widetilde{\rho}_{\$_{j^*}}, \widetilde{\rho}_{\$_{\ell^*}})$ to the challenger.

Given the event in Eq. (9) holds (for the afore mentioned fixed indices), then the reduction will return two quantum money states with the same serial number as the challenger sent. With advantage $1/(2k^3p(\lambda))$, the reduction will succeed at breaking unforgeability of the quantum money scheme, thus reaching a contradiction.
Scenario Two.

Alternatively, say that (for an infinite set of λ) $\mathcal{A}$ does not generate two accepting proofs which have the same serial number as an honestly generated proof with at least $1/(2p(\lambda))$ probability. By the pigeon-hole principle, this means that $\mathcal{A}$ generates an accepting proof with a serial number which is not amongst the ones it received. In summary, we have that

$$\Pr_{\substack{\mathcal{O} \\ \forall \iota \in [k-1],\, \pi_\iota \leftarrow \mathsf{P}^{\mathcal{O}}(x_\iota, w_\iota) \\ \{\widetilde{x_\iota}, \widetilde{\pi_\iota}\}_{\iota \in [k]} \leftarrow \mathcal{A}^{\mathcal{O}}(\{x_\iota, \pi_\iota\}_{\iota \in [k-1]})}} \left[\begin{array}{c} \exists\, \mathcal{J} \subseteq \{j : \widetilde{x}_j = x\} \\ \text{s.t. } |\mathcal{J}| > |\{i : x_i = x\}| \\ \text{and } \forall \iota \in \mathcal{J}, \mathsf{V}^{\mathcal{O}}(x, \widetilde{\pi}_\iota) = 1 \\ \text{and } \exists j^* \in \mathcal{J} \text{ s.t. } \widetilde{s_{j^*}} \notin \{s_\iota\}_{\iota \in [k-1]} \end{array} \right] \geq \frac{1}{2p(\lambda)}. \quad (10)$$

Through an averaging argument, we can get a similar event with a fixed index j^* that belongs to the event's set $\mathcal{J}$ with an advantage of $1/(2kp(\lambda))$. We will now switch to a hybrid where we provide $\mathcal{A}$ with simulated proofs.

Claim (5.1). There exists a polynomial $q(\cdot)$ such that

$$\Pr_{\substack{\mathcal{O} \\ \{\pi_\iota\}_{\iota\in[k-1]}\leftarrow \mathsf{SimExt}^{\mathcal{O}}(x_1,\ldots,x_{k-1}) \\ \{\widetilde{x_\iota},\widetilde{\pi_\iota}\}_{\iota\in[k]}\leftarrow \mathcal{A}^{\mathsf{SimExt}^{\mathcal{O}}}(\{x_\iota,\pi_\iota\}_{\iota\in[k-1]})}} \left[\begin{array}{c} \exists\ \mathcal{J}\subseteq\{j:\widetilde{x}_j=x\} \\ \text{s.t. } |\mathcal{J}|>|\{i:x_i=x\}| \\ \text{and } \forall \iota\in\mathcal{J}, \mathsf{V}^{\mathsf{SimExt}^{\mathcal{O}}}(x,\widetilde{\pi}_\iota)=1 \\ \text{and } j^*\in\mathcal{J} \\ \text{and } \widetilde{s_{j^*}}\notin\{s_\iota\}_{\iota\in[k-1]} \end{array}\right] \geq \frac{1}{q(\lambda)}. \tag{11}$$

We will later see a proof of Sect. 5.4. For now, assuming that this claim holds, we can define an adversary from which Ext can extract a valid witness for x.

Claim (5.2). There exists a polynomial $q'(\cdot)$ such that

$$\Pr_{w\leftarrow\mathcal{E}^{\mathcal{A}}(x_1,\ldots,x_{k-1},x)}[(x,w)\in\mathcal{R}] \geq \frac{1}{q'(\lambda)}. \tag{12}$$

We will soon see a proof for Sect. 5.4. Meanwhile, if this claim is true, then we will have a direct contradiction with Eq. (8). Thus, all that remains to be proven are the two claims.

See proof of Claim 5.1 and Claim 5.2 in the full version [33].

By completing the proofs of our claims, we have concluding the proof of our theorem statement.

Corollary 5. *Assuming the injective one-way functions exist, and post-quantum iO exists, there exists a non-interactive knowledge sound, computationally zero-knowledge, and $(k-1)$-to-k-unclonable with extraction protocol for* NP *in the quantum random oracle model.*

Proof. This follows from Theorem 9 and Theorem 15.

We have thus shown that Fig. 4 is an unclonable NIZK AoK in the ROM model as defined according to our unclonability definition.

6 Applications

6.1 Unclonable Signatures of Knowledge

Definition 7 (Unclonable Extractable SimExt-secure Signatures of Knowledge). *Let* NP *relation $\mathcal{R}$ with corresponding language $\mathcal{L}$ be given such that they can be indexed by a security parameter $\lambda\in\mathbb{N}$. Let a message space $\mathcal{M}$ be given such that it can be indexed by a security parameter $\lambda\in\mathbb{N}$.*

$(\mathsf{Setup},\mathsf{Sign},\mathsf{Verify})$ *is an unclonable signature of knowledge of a witness with respect to $\mathcal{L}$ and $\mathcal{M}$ if it has the following properties:*

– $(\mathsf{Setup},\mathsf{Sign},\mathsf{Verify})$ *is a quantum Sim-Ext signature of knowledge.*

– $(k-1)$-*to-*k**-Unclonable with Extraction**: *There exists an oracle-aided polynomial-size quantum circuit* $\mathcal{E}$ *such that for every polynomial-size quantum circuit* $\mathcal{A}$*, for every tuple of* $k-1$ *instance-witness pairs* $(x_1,\omega_1),\ldots,(x_{k-1},\omega_{k-1}) \in \mathcal{R}$*, every* $\{m_\iota \in \mathcal{M}_\lambda\}_{\iota\in[k-1]}$*, for every* (x,m)*, if there is a polynomial* $p(\cdot)$ *where*

$$\Pr_{\substack{(\mathsf{crs},\mathsf{td})\leftarrow\mathsf{Setup}(1^\lambda)\\ \forall\iota\in[k-1],\,\sigma_\iota\leftarrow\mathsf{Sign}(\mathsf{crs},x_\iota,\omega_\iota,m_\iota)\\ \{\widetilde{\sigma_\iota}\}_{\iota\in[k]}\leftarrow\mathcal{A}(\mathsf{crs},\{x_\iota,m_\iota,\sigma_\iota\}_{\iota\in[k-1]})}}\left[\begin{array}{c}\exists\ \mathcal{J}\subseteq\{j:(\widetilde{x}_j,\widetilde{m}_j)=(x,m)\}\\ s.t.\ |\mathcal{J}|>|\{i:(x_i,m_i)=(x,m)\}|\\ and\ \forall\iota\in\mathcal{J},\mathsf{Verify}(\mathsf{crs},x,m,\widetilde{\sigma_\iota})=1\end{array}\right]\geq\frac{1}{p(\lambda)},$$

then there is also a polynomial $q(\cdot)$ *such that*

$$\Pr_{w\leftarrow\mathcal{E}^{\mathcal{A}}(\{x_\iota,m_\iota\}_{\iota\in[k-1]},x,m)}[(x,w)\in\mathcal{R}]\geq\frac{1}{q(\lambda)}.$$

Unclonable Signature of Knowledge with CRS

Let $(\mathsf{Setup},\mathsf{P},\mathsf{V})$ be non-interactive simulation-extractable, adaptive multi-theorem computational zero-knowledge, unclonable-extractable protocol for NP. Let $\mathcal{R}$ be the relation with respect to $\mathcal{L}\in\mathsf{NP}$.

$\underline{\textsc{Setup}}(1^\lambda)$: $(\mathsf{crs},\mathsf{td})\leftarrow\Pi.\mathsf{Setup}(1^\lambda)$.

$\underline{\textsc{Sign}}(\mathsf{crs},x,w,m)$:

– Let $x_\Pi=(x,m)$ be an instance and $w_\Pi=w$ be its corresponding witness for the following language $\mathcal{L}_\Pi$:

$$\{(x,m)\ :\ \exists w\ \ :\ \ (x,w)\in\mathcal{R}\}.$$

– Compute $\pi_\Pi\leftarrow\Pi.\mathsf{P}(\mathsf{crs},x_\Pi,w_\Pi)$.
– Output $\sigma=\pi_\Pi$.

$\underline{\textsc{Verify}}(\mathsf{crs},x,m,\sigma)$: Output $\Pi.\mathsf{V}(\mathsf{crs},(x,m),\pi_\Pi)$.

Fig. 5. Unclonable Signature of Knowledge in CRS model

Theorem 16. *Let* $\Pi=(\mathsf{Setup},\mathsf{P},\mathsf{V})$ *be a non-interactive simulation-extractable, adaptive multi-theorem computational zero-knowledge, unclonable-extractable protocol for* NP *(Definition 5).*

$(\mathsf{Setup},\mathsf{Sign},\mathsf{Verify})$ *in Fig. 5 is an unclonable-extractable SimExt-secure signature of knowledge (Definition 7).*

Corollary 6. *Assuming the polynomial quantum hardness of LWE, injective one-way functions exist, post-quantum iO exists, there exists an unclonable SimExt-secure signature of knowledge (Definition 7).*

Proof. This follows from Corollary 3 and Theorem 16.

6.2 Revocable Anonymous Credentials

Definition 8 (Revocable Anonymous Credentials). $(\mathsf{IssuerKeyGen}, \mathsf{Issue}, \mathsf{VerifyCred}, \mathsf{Revoke}, \mathsf{Prove}, \mathsf{VerRevoke})$ *is a revocable anonymous credentials scheme with respect to some set of accesses* $\{\mathcal{S}_\lambda\}_{\lambda\in\mathbb{N}}$ *if it has the following properties:*

- **Correctness***: For every sufficiently large* $\lambda \in \mathbb{N}$*, and every* $\mathsf{access} \in \mathcal{S}_\lambda$*,*

$$\Pr_{\substack{(\mathsf{nym},\mathsf{sk})\leftarrow\mathsf{IssuerKeyGen}(1^\lambda)\\ \mathsf{cred}\leftarrow\mathsf{Issue}(1^\lambda,\mathsf{nym},\mathsf{sk},\mathsf{access})}}[\mathsf{VerifyCred}(1^\lambda,\mathsf{nym},\mathsf{access},\mathsf{cred})=1]=1$$

  and

$$\Pr_{\substack{(\mathsf{nym},\mathsf{sk})\leftarrow\mathsf{IssuerKeyGen}(1^\lambda)\\ \mathsf{cred}\leftarrow\mathsf{Issue}(1^\lambda,\mathsf{nym},\mathsf{sk},\mathsf{access})\\ \mathsf{revnotice}\leftarrow\mathsf{Revoke}(1^\lambda,\mathsf{nym},\mathsf{sk},\mathsf{access})\\ \pi\leftarrow\mathsf{Prove}(1^\lambda,\mathsf{nym},\mathsf{revnotice},\mathsf{cred})}}[\mathsf{VerRevoke}(\mathsf{nym},\mathsf{sk},\mathsf{access},\mathsf{revnotice},\pi)=1]=1.$$

- **Revocation***: For every polynomial-size quantum circuit* $\mathcal{A}$*, there exists a negligible function* $\mathsf{negl}(\cdot)$ *such that for sufficiently large* $\lambda \in \mathbb{N}$*, and every* $\mathsf{access} \in \mathcal{M}_\lambda$

$$\Pr_{\substack{(\mathsf{nym},\mathsf{sk})\leftarrow\mathsf{IssuerKeyGen}(1^\lambda)\\ \mathsf{cred}\leftarrow\mathsf{Issue}(1^\lambda,\mathsf{nym},\mathsf{sk},\mathsf{access})\\ \mathsf{revnotice}\leftarrow\mathsf{Revoke}(1^\lambda,\mathsf{nym},\mathsf{sk},\mathsf{access})\\ \pi,\mathsf{cred}'\leftarrow\mathcal{A}(1^\lambda,\mathsf{nym},\mathsf{revnotice},\mathsf{cred})}}\left[\begin{array}{c}\mathsf{VerRevoke}(1^\lambda,\mathsf{nym},\mathsf{sk},\mathsf{access},\mathsf{revnotice},\pi)=1\\ \wedge\,\mathsf{VerifyCred}(1^\lambda,\mathsf{nym},\mathsf{access},\mathsf{cred}')=1\end{array}\right]\leq\mathsf{negl}(\lambda).$$

We now introduce a construction based on unclonable signatures of knowledge.

Theorem 17. *Let* $(\mathcal{X},\mathcal{W})$ *be a hard-distribution of instance and witness pairs for some* NP *relation. Let* $\{\mathcal{S}_\lambda\}_{\lambda\in\mathbb{N}}$ *be some set of accesses. Let* $(\mathsf{Setup},\mathsf{Sign},\mathsf{Verify})$ *be an unclonable-extractable SimExt-secure signature of knowledge for message space* $\{\mathcal{S}_\lambda\}_{\lambda\in\mathbb{N}}$ *(Definition 7).*

$(\mathsf{IssuerKeyGen},\mathsf{Issue},\mathsf{VerifyCred},\mathsf{Revoke},\mathsf{Prove},\mathsf{VerRevoke})$ *defined in Fig. 6 is a revocable anonymous credentials scheme (Definition 8).*

Proof (Proof Sketch of Theorem 17). The correctness of this revocable anonymous credentials scheme follows from the correctness of the unclonable signature of knowledge scheme.

We will now sketch the proof of revocation. Say that there exists an adversary $\mathcal{A}$, access access, and polynomial $p(\cdot)$ such that, with probability at least $1/p(\lambda)$: (1) π passes the revocation check, and (2) cred' passes the credential check. This means that both π and cred' are valid signatures with respect to the same crs, x, and access that the signature cred was issued under. This satisfies the "if" condition of the unclonability property of the unclonable signature of knowledge.

Revocable Anonymous Credentials

Let $(\mathcal{X}, \mathcal{W})$ be a hard-distribution of instance and witness pairs for some NP relation. Let $\{\mathcal{S}_\lambda\}_{\lambda\in\mathbb{N}}$ be some set of accesses. Let $(\mathsf{Setup}, \mathsf{Sign}, \mathsf{Verify})$ be an unclonable-extractable SimExt-secure signature of knowledge for message space $\{\mathcal{S}_\lambda\}_{\lambda\in\mathbb{N}}$ (Definition 7).

$\underline{\textsc{IssuerKeyGen}}(1^\lambda)$: $(\mathsf{crs}, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)$; $(x, w) \leftarrow (\mathcal{X}, \mathcal{W})$; Output $\mathsf{nym} = (\mathsf{crs}, x)$ and $\mathsf{sk} = (\mathsf{td}, w)$.

$\underline{\textsc{Issue}}(\mathsf{nym}, \mathsf{sk}, \mathsf{access})$: $\sigma \leftarrow \mathsf{Sign}(\mathsf{crs}, x, w, \mathsf{access})$; Output $\mathsf{cred} = \sigma$.

$\underline{\textsc{VerifyCred}}(\mathsf{nym}, \mathsf{access}, \mathsf{cred})$: Output $\mathsf{Verify}(\mathsf{crs}, x, \mathsf{access}, \mathsf{cred})$.

$\underline{\textsc{Revoke}}(\mathsf{nym}, \mathsf{sk}, \mathsf{access})$: Output $\mathsf{revnotice} = \mathsf{access}$.

$\underline{\textsc{Prove}}(\mathsf{nym}, \mathsf{revnotice}, \mathsf{cred})$: Output $\mathsf{revnotice} = \mathsf{access}$.

$\underline{\textsc{VerifyRevoke}}(\mathsf{nym}, \mathsf{sk}, \mathsf{access}, \mathsf{revnotice}, \pi)$:
Output $\mathsf{VerifyCred}(\mathsf{nym}, \mathsf{access}, \pi)$.

Fig. 6. Revocable Anonymous Credentials

As such, there exists a polynomial $q(\cdot)$ such that the unclonable signature of knowledge's extractor can produce a witness w for x with probability at least $1/q(\lambda)$. However, this contradicts the hardness of the distribution $(\mathcal{X}, \mathcal{W})$. Hence, our protocol must have the revocation property.

Corollary 7. *Assuming the polynomial quantum hardness of LWE, injective one-way functions exist, post-quantum iO exists, and the hardness of* NP*, there exists a revocable anonymous credentials scheme (Definition 8).*

Proof. This follows from Corollary 6 and Theorem 17.

6.3 Unclonable Anonymous Credentials

We will show that our revocable anonymous credentials construction in Fig. 6 also satisfies a definition of unclonable anonymous credentials. We defer the definitions and proofs to the full version [33].

Theorem 18. *Let* $(\mathcal{X}, \mathcal{W})$ *be a hard-distribution of instance and witness pairs for some* NP *relation. Let* $\{\mathcal{S}_\lambda\}_{\lambda\in\mathbb{N}}$ *be some set of accesses. Let* $(\mathsf{Setup}, \mathsf{Sign}, \mathsf{Verify})$ *be an unclonable-extractable SimExt-secure signature of knowledge for message space* $\{\mathcal{S}_\lambda\}_{\lambda\in\mathbb{N}}$ *(Definition 7).*

$(\mathsf{IssuerKeyGen}, \mathsf{Issue}, \mathsf{VerifyCred})$ *defined in Fig. 6 is an unclonable anonymous credentials scheme.*

Corollary 8. *Assuming the polynomial quantum hardness of LWE, injective one-way functions exist, post-quantum iO exists, and the hardness of* NP*, there exists an unclonable anonymous credentials scheme.*

Acknowledgments. The authors were supported in part by DARPA SIEVE, NSF QIS-2112890, NSF CAREER CNS-2238718, and NSF CNS-2247727. This material is based on work supported by DARPA under Contract No. HR001120C0024. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Government or DARPA.

References

1. Aaronson, S.: Quantum copy-protection and quantum money. In: Proceedings of the 24th Annual IEEE Conference on Computational Complexity, CCC 2009, Paris, France, 15-18 July 2009. pp. 229–242. IEEE Computer Society (2009). https://doi.org/10.1109/CCC.2009.42, https://doi.org/10.1109/CCC.2009.42
2. Aaronson, S., Christiano, P.F.: Quantum money from hidden subspaces. Theory Comput. **9**, 349–401 (2013). https://doi.org/10.4086/toc.2013.v009a009, https://doi.org/10.4086/toc.2013.v009a009
3. Aaronson, S., Liu, J., Liu, Q., Zhandry, M., Zhang, R.: New approaches for quantum copy-protection. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12825, pp. 526–555. Springer (2021). https://doi.org/10.1007/978-3-030-84242-0_19, https://doi.org/10.1007/978-3-030-84242-0_19
4. Acar, T., Nguyen, L.: Revocation for delegatable anonymous credentials. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings. Lecture Notes in Computer Science, vol. 6571, pp. 423–440. Springer (2011). https://doi.org/10.1007/978-3-642-19379-8_26, https://doi.org/10.1007/978-3-642-19379-8_26
5. Amos, R., Georgiou, M., Kiayias, A., Zhandry, M.: One-shot signatures and applications to hybrid quantum/classical authentication. In: Makarychev, K., Makarychev, Y., Tulsiani, M., Kamath, G., Chuzhoy, J. (eds.) Proccedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2020, Chicago, IL, USA, June 22-26, 2020. pp. 255–268. ACM (2020). https://doi.org/10.1145/3357713.3384304, https://doi.org/10.1145/3357713.3384304
6. Ananth, P., Kaleoglu, F.: Unclonable encryption, revisited. In: Nissim, K., Waters, B. (eds.) Theory of Cryptography - 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 13042, pp. 299–329. Springer (2021). https://doi.org/10.1007/978-3-030-90459-3_11, https://doi.org/10.1007/978-3-030-90459-3_11
7. Ananth, P., Kaleoglu, F., Li, X., Liu, Q., Zhandry, M.: On the feasibility of unclonable encryption, and more. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II. Lecture Notes in Computer Science, vol. 13508, pp. 212–241. Springer (2022). https://doi.org/10.1007/978-3-031-15979-4_8, https://doi.org/10.1007/978-3-031-15979-4_8
8. Ananth, P., Placa, R.L.L.: Secure software leasing. In: Canteaut, A., Standaert, F. (eds.) Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb,

Croatia, October 17-21, 2021, Proceedings, Part II. Lecture Notes in Computer Science, vol. 12697, pp. 501–530. Springer (2021). https://doi.org/10.1007/978-3-030-77886-6_17, https://doi.org/10.1007/978-3-030-77886-6_17
9. Ananth, P., Poremba, A., Vaikuntanathan, V.: Revocable cryptography from learning with errors. In: Rothblum, G.N., Wee, H. (eds.) Theory of Cryptography - 21st International Conference, TCC 2023, Taipei, Taiwan, November 29 - December 2, 2023, Proceedings, Part IV. Lecture Notes in Computer Science, vol. 14372, pp. 93–122. Springer (2023). https://doi.org/10.1007/978-3-031-48624-1_4, https://doi.org/10.1007/978-3-031-48624-1_4
10. Barhoush, M., Salvail, L.: How to sign quantum messages (2023)
11. Barhoush, M., Salvail, L.: Powerful primitives in the bounded quantum storage model (2023)
12. Bartusek, J., Garg, S., Goyal, V., Khurana, D., Malavolta, G., Raizes, J., Roberts, B.: Obfuscation and outsourced computation with certified deletion. Cryptology ePrint Archive, Paper 2023/265 (2023), https://eprint.iacr.org/2023/265
13. Bartusek, J., Khurana, D.: Cryptography with certified deletion. In: Crypto 2023 (to appear) (2023)
14. Bartusek, J., Khurana, D., Poremba, A.: Publicly-verifiable deletion via target-collapsing functions. In: Crypto 2023 (to appear) (2023)
15. Belenkiy, M., Camenisch, J., Chase, M., Kohlweiss, M., Lysyanskaya, A., Shacham, H.: Randomizable proofs and delegatable anonymous credentials. In: Halevi, S. (ed.) Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings. Lecture Notes in Computer Science, vol. 5677, pp. 108–125. Springer (2009). https://doi.org/10.1007/978-3-642-03356-8_7, https://doi.org/10.1007/978-3-642-03356-8_7
16. Ben-David, S., Sattath, O.: Quantum tokens for digital signatures. CoRR **abs/1609.09047** (2016), http://arxiv.org/abs/1609.09047
17. Ben-David, S., Sattath, O.: Quantum tokens for digital signatures. IACR Cryptol. ePrint Arch. p. 94 (2017), http://eprint.iacr.org/2017/094
18. Broadbent, A., Islam, R.: Quantum encryption with certified deletion. In: Pass, R., Pietrzak, K. (eds.) Theory of Cryptography. pp. 92–122. Springer International Publishing, Cham (2020)
19. Broadbent, A., Lord, S.: Uncloneable quantum encryption via oracles. In: Flammia, S.T. (ed.) 15th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2020, June 9-12, 2020, Riga, Latvia. LIPIcs, vol. 158, pp. 4:1–4:22. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2020). https://doi.org/10.4230/LIPIcs.TQC.2020.4, https://doi.org/10.4230/LIPIcs.TQC.2020.4
20. Camenisch, J., Kohlweiss, M., Soriente, C.: Solving revocation with efficient update of anonymous credentials. In: Garay, J.A., Prisco, R.D. (eds.) Security and Cryptography for Networks, 7th International Conference, SCN 2010, Amalfi, Italy, September 13-15, 2010. Proceedings. Lecture Notes in Computer Science, vol. 6280, pp. 454–471. Springer (2010). https://doi.org/10.1007/978-3-642-15317-4_28, https://doi.org/10.1007/978-3-642-15317-4_28
21. Chase, M., Lysyanskaya, A.: On signatures of knowledge. In: Dwork, C. (ed.) Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings. Lecture Notes in Computer Science, vol. 4117, pp. 78–96. Springer (2006). https://doi.org/10.1007/11818175_5, https://doi.org/10.1007/11818175_5

22. Coiteux-Roy, X., Wolf, S.: Proving erasure. In: IEEE International Symposium on Information Theory, ISIT 2019, Paris, France, July 7-12, 2019. pp. 832–836 (2019). https://doi.org/10.1109/ISIT.2019.8849661, https://doi.org/10.1109/ISIT.2019.8849661
23. Coladangelo, A., Liu, J., Liu, Q., Zhandry, M.: Hidden cosets and applications to unclonable cryptography. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12825, pp. 556–584. Springer (2021). https://doi.org/10.1007/978-3-030-84242-0_20, https://doi.org/10.1007/978-3-030-84242-0_20
24. Farhi, E., Gosset, D., Hassidim, A., Lutomirski, A., Shor, P.W.: Quantum money from knots. In: Goldwasser, S. (ed.) Innovations in Theoretical Computer Science 2012, Cambridge, MA, USA, January 8-10, 2012. pp. 276–289. ACM (2012). https://doi.org/10.1145/2090236.2090260, https://doi.org/10.1145/2090236.2090260
25. Fu, H., Miller, C.A.: Local randomness: Examples and application. Phys. Rev. A **97**, 032324 (Mar 2018). https://doi.org/10.1103/PhysRevA.97.032324, https://link.aps.org/doi/10.1103/PhysRevA.97.032324
26. Georgiou, M., Zhandry, M.: Unclonable decryption keys. IACR Cryptol. ePrint Arch. p. 877 (2020), https://eprint.iacr.org/2020/877
27. Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof systems. SIAM J. Comput. **18**(1), 186–208 (1989). https://doi.org/10.1137/0218012, https://doi.org/10.1137/0218012
28. Gottesman, D.: Uncloneable encryption. Quantum Inf. Comput. **3**(6), 581–602 (2003). https://doi.org/10.26421/QIC3.6-2, https://doi.org/10.26421/QIC3.6-2
29. Goyal, V., Malavolta, G., Raizes, J.: Unclonable commitments and proofs. IACR Cryptol. ePrint Arch. p. 1538 (2023), https://eprint.iacr.org/2023/1538
30. Hiroka, T., Morimae, T., Nishimaki, R., Yamakawa, T.: Quantum encryption with certified deletion, revisited: Public key, attribute-based, and classical communication. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2021. pp. 606–636. Springer International Publishing, Cham (2021)
31. Hiroka, T., Morimae, T., Nishimaki, R., Yamakawa, T.: Certified everlasting zero-knowledge proof for QMA. CRYPTO (2022), https://ia.cr/2021/1315
32. IBM: Cost of a data breach report 2023. Tech. rep., IBM (2023)
33. Jawale, R., Khurana, D.: Unclonable non-interactive zero-knowledge. IACR Cryptol. ePrint Arch. p. 1532 (2023), https://eprint.iacr.org/2023/1532
34. Kane, D.M.: Quantum money from modular forms. CoRR **abs/1809.05925** (2018), http://arxiv.org/abs/1809.05925
35. Kitagawa, F., Nishimaki, R.: One-out-of-many unclonable cryptography: Definitions, constructions, and more. IACR Cryptol. ePrint Arch. p. 229 (2023), https://eprint.iacr.org/2023/229
36. Kundu, S., Tan, E.Y.Z.: Composably secure device-independent encryption with certified deletion (2020). https://doi.org/10.48550/ARXIV.2011.12704, https://arxiv.org/abs/2011.12704
37. Liu, Q., Zhandry, M.: Revisiting post-quantum fiat-shamir. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II. Lecture Notes in Computer Science, vol. 11693, pp. 326–355. Springer (2019). https://doi.org/10.1007/978-3-030-26951-7_12, https://doi.org/10.1007/978-3-030-26951-7_12

38. Lombardi, A., Schaeffer, L.: A note on key agreement and non-interactive commitments. Cryptology ePrint Archive, Paper 2019/279 (2019), https://eprint.iacr.org/2019/279, https://eprint.iacr.org/2019/279
39. Majenz, C., Schaffner, C., Tahmasbi, M.: Limitations on uncloneable encryption and simultaneous one-way-to-hiding. IACR Cryptol. ePrint Arch. p. 408 (2021), https://eprint.iacr.org/2021/408
40. Peikert, C., Shiehian, S.: Noninteractive zero knowledge for NP from (plain) learning with errors. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part I. Lecture Notes in Computer Science, vol. 11692, pp. 89–114. Springer (2019). https://doi.org/10.1007/978-3-030-26948-7_4, https://doi.org/10.1007/978-3-030-26948-7_4
41. Poremba, A.: Quantum proofs of deletion for learning with errors. Cryptology ePrint Archive, Report 2022/295 (2022), https://ia.cr/2022/295
42. Sahai, A.: Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In: 40th Annual Symposium on Foundations of Computer Science, FOCS '99, 17-18 October, 1999, New York, NY, USA. pp. 543–553. IEEE Computer Society (1999). https://doi.org/10.1109/SFFCS.1999.814628, https://doi.org/10.1109/SFFCS.1999.814628
43. Santis, A.D., Crescenzo, G.D., Ostrovsky, R., Persiano, G., Sahai, A.: Robust non-interactive zero knowledge. In: Kilian, J. (ed.) Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings. Lecture Notes in Computer Science, vol. 2139, pp. 566–598. Springer (2001). https://doi.org/10.1007/3-540-44647-8_33, https://doi.org/10.1007/3-540-44647-8_33
44. Santis, A.D., Crescenzo, G.D., Persiano, G.: Necessary and sufficient assumptions for non-iterative zero-knowledge proofs of knowledge for all NP relations. In: Montanari, U., Rolim, J.D.P., Welzl, E. (eds.) Automata, Languages and Programming, 27th International Colloquium, ICALP 2000, Geneva, Switzerland, July 9-15, 2000, Proceedings. Lecture Notes in Computer Science, vol. 1853, pp. 451–462. Springer (2000). https://doi.org/10.1007/3-540-45022-X_38, https://doi.org/10.1007/3-540-45022-X_38
45. Santis, A.D., Persiano, G.: Zero-knowledge proofs of knowledge without interaction (extended abstract). In: 33rd Annual Symposium on Foundations of Computer Science, Pittsburgh, Pennsylvania, USA, 24-27 October 1992. pp. 427–436. IEEE Computer Society (1992). https://doi.org/10.1109/SFCS.1992.267809, https://doi.org/10.1109/SFCS.1992.267809
46. Unruh, D.: Revocable quantum timed-release encryption. In: Nguyen, P.Q., Oswald, E. (eds.) Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings. Lecture Notes in Computer Science, vol. 8441, pp. 129–146. Springer (2014). https://doi.org/10.1007/978-3-642-55220-5_8, https://doi.org/10.1007/978-3-642-55220-5_8
47. Unruh, D.: Post-quantum security of fiat-shamir. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I. Lecture Notes in Computer Science, vol. 10624, pp. 65–95. Springer (2017). https://doi.org/10.1007/978-3-319-70694-8_3, https://doi.org/10.1007/978-3-319-70694-8_3

48. Wiesner, S.: Conjugate coding. SIGACT News **15**(1), 78–88 (1983). https://doi.org/10.1145/1008908.1008920, https://doi.org/10.1145/1008908.1008920
49. Zhandry, M.: How to record quantum queries, and applications to quantum indifferentiability. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II. Lecture Notes in Computer Science, vol. 11693, pp. 239–268. Springer (2019). https://doi.org/10.1007/978-3-030-26951-7_9, https://doi.org/10.1007/978-3-030-26951-7_9
50. Zhandry, M.: Quantum lightning never strikes the same state twice. In: Ishai, Y., Rijmen, V. (eds.) Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III. Lecture Notes in Computer Science, vol. 11478, pp. 408–438. Springer (2019). https://doi.org/10.1007/978-3-030-17659-4_14, https://doi.org/10.1007/978-3-030-17659-4_14