Revocable Quantum Digital Signatures

Tomoyuki Morimae
Yukawa Institute for Theoretical Physics, Kyoto University, Japan

Alexander Poremba
Computing and Mathematical Sciences, Caltech, Pasadena, CA, USA
CSAIL and Department of Mathematics, MIT, Cambridge, MA, USA

Takashi Yamakawa
NTT Social Informatics Laboratories, Tokyo, Japan
NTT Research Center for Theoretical Quantum Information, Atsugi, Japan

Abstract

We study digital signatures with *revocation capabilities* and show two results. First, we define and construct digital signatures with revocable signing keys from the LWE assumption. In this primitive, the signing key is a quantum state which enables a user to sign many messages and yet, the quantum key is also *revocable*, i.e., it can be collapsed into a classical certificate which can later be verified. Once the key is successfully revoked, we require that the initial recipient of the key loses the ability to sign. We construct digital signatures with revocable signing keys from a newly introduced primitive which we call *two-tier one-shot signatures*, which may be of independent interest. This is a variant of one-shot signatures, where the verification of a signature for the message "0" is done publicly, whereas the verification for the message "1" is done in private. We give a construction of two-tier one-shot signatures from the LWE assumption. As a complementary result, we also construct digital signatures with *quantum* revocation from group actions, where the quantum signing key is simply "returned" and then verified as part of revocation.

Second, we define and construct digital signatures with revocable signatures from OWFs. In this primitive, the signer can produce quantum signatures which can later be revoked. Here, the security property requires that, once revocation is successful, the initial recipient of the signature loses the ability to find accepting inputs to the signature verification algorithm. We construct this primitive using a newly introduced *two-tier* variant of tokenized signatures. For the construction, we show a new lemma which we call the adaptive hardcore bit property for OWFs, which may enable further applications.

2012 ACM Subject Classification Theory of computation → Cryptographic protocols

Keywords and phrases Quantum cryptography, digital signatures, revocable cryptography

Digital Object Identifier 10.4230/LIPIcs.TQC.2024.5

Related Version *Full Version*: https://eprint.iacr.org/2023/1937

Funding *Tomoyuki Morimae*: JST CREST JPMJCR23I3, JST Moonshot R&D JPMJMS2061-5-1-1, JST FOREST, MEXT QLEAP, the Grant-in-Aid for Scientific Research (B) No. JP19H04066, the Grant-in Aid for Transformative Research Areas (A) 21H05183, and the Grant-in-Aid for Scientific Research (A) No. 22H00522.
Alexander Poremba: National Science Foundation (NSF) under Grant No. CCF-1729369.
Takashi Yamakawa: Supported by the NTT Corporation.

1 Introduction

1.1 Background

The exotic nature of quantum physics, such as quantum superposition, no-cloning, entanglement, and uncertainty relations, enables many new cryptographic applications which are impossible in a classical world. These include quantum money [43], copy-protection [1, 2],

19th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2024).
Editors: Frédéric Magniez and Alex Bredariol Grilo; Article No. 5; pp. 5:1–5:24
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

secure software leasing [5], unclonable encryption [20, 15], certified deletion [14], and more. Here, a common approach is to encode information into a quantum state which prevents it from being copied by the no-cloning principle. [42, 14, 23, 24, 6, 11, 9, 30, 35, 8, 7]

Following this line of research, Ananth, Poremba, and Vaikuntanathan [6] and Agrawal, Kitagawa, Nishimaki, Yamada, and Yamakawa [3] concurrently introduced the concept of key-revocable public key encryption (PKE),[1] which realizes the following functionality: a decryption capability is delegated to a user in the form of a quantum decryption key in such a way that, once the key is returned, the user loses the ability to decrypt. They constructed key-revocable PKE schemes based on standard assumptions, namely quantum hardness of the learning with errors problem (LWE assumption) [6] or even the mere existence of any PKE scheme [3]. They also extended the idea of revocable cryptography to pseudorandom functions [6] and encryption with advanced functionality such as attribute-based encryption and functional encryption [3]. However, neither of these works extended the idea to *digital signatures* despite their great importance in cryptography. This state of affairs raises the following question:

Is it possible to construct digital signature schemes with revocation capabilities?

The delegation of privileges is of central importance in cryptography, and the task of revoking privileges in the context of digital signatures and certificates, in particular, remains a fundamental challenge for cryptography [41, 39]. One simple solution is to use a limited-time delegatable signature scheme, where a certified signing key is generated together with an expiration date. Note that this requires that the expiration date is known ahead of time and that the clocks be synchronized. Moreover, issuing new keys (for example, each day) could potentially also be costly. Quantum digital signature schemes with revocation capabilities could potentially resolve these difficulties by leveraging the power of quantum information.

To illustrate the use of *revocable* digital signature schemes, consider the following scenarios. Suppose that an employee at a company, say Alice, takes a temporary leave of absence and wishes to authorize her colleague, say Bob, to sign a few important documents on her behalf. One thing Alice can do is to simply use a (classical) digital signature scheme and to share her signing keys with Bob. While this naïve approach would certainly allow Bob to produce valid signatures while Alice is gone, it also means that Bob continues to have access to the signing keys – long after Alice's return. This is because the signing key of a digital signature scheme is *classical*, and hence it can be copied at will. In particular, a malicious Bob could secretly sell Alice's signing key to a third party for a profit. A digital signature scheme with *revocable signing keys* can remedy this situation as it enables Alice to certify that Bob has lost access to the signing key once and for all.

As a second example, consider the following scenario. Suppose that a company or a governmental organization wishes to grant a new employee certain access privileges throughout their employment; for example to various buildings or office spaces. One solution is to use an *electronic* ID card through a mobile device, where a digital signature is used for identity management. Naturally, one would like to ensure that, once the employee's contract is terminated, their ID card is disabled in the system and no longer allows for further unauthorized access. However, if the signature corresponding to the employee's ID is a digital object, it is conceivable that the owner of the card manages to retain their ID card even after it is disabled. This threat especially concerns scenarios in which the verification of an ID

[1] Agrawal et al. [3] call it PKE with secure key leasing.

card is performed by a device which is not connected to the internet, or simply not updated frequently enough. A digital signature scheme with revocable signatures can remedy this situation as it enables *revocable quantum* ID cards; in particular, it allows one to certify that the initial access privileges have been revoked once and for all.

1.2 Our Results

In this paper, we show the following two results on revocable digital signatures.

Revocable signing keys. First, we define digital signatures with revocable *signing keys* (DSR-Key). In this primitive, a signing key is encoded in the form of a quantum state which enables the recipient to sign many messages. However, once the key is successfully revoked from a user, they no longer have the ability to generate valid signatures. Here, we consider *classical revocation*, i.e., a classical certificate is issued once the user destroys the quantum signing key with an appropriate measurement. In addition, the verification of the revocation certificate takes place in private, which means that the verification requires a private key which should be kept secret. We construct DSR-Key based solely on the quantum hardness of the LWE problem [38]. We remark that our scheme is inherently *stateful*, i.e., whenever a user generates a new signature, the user must update the singing key for the next invocation of the signing algorithm. Indeed, we believe that digital signatures with revocable signing keys must be inherently stateful since a user must keep the quantum signing key as a "state" for generating multiple signatures. An undesirable feature of our scheme is that the signing key and signature sizes grow with the number of signatures to be generated.

As complementary result, we also consider DSR-Key with *quantum* revocation. In this primitive, not a classical deletion certificate but the quantum signing key itself is returned for the revocation. In the full version of the paper, we construct the primitive from group actions with the one-wayness property [26]. The existence of group actions with the one-wayness property is incomparable with the LWE assumption.

Revocable signatures. Second, we define digital signatures with revocable *signatures* (DSR-Sign). In this primitive, signatures are encoded as quantum states which can later be revoked. The security property guarantees that, once revocation is successful, the initial recipient of the signature loses the ability to pass the signature verification. We construct digital signatures with revocable signatures based on the existence of (quantum-secure) one-way functions (OWFs). In our scheme, the revocation is classical and private, i.e., a user can issue a classical certificate of revocation, which is verified by using a private key.

1.3 Comparison with Existing Works

To our knowledge, there is no prior work that studies digital signatures with quantum signatures. On the other hand, there are several existing works that study digital signatures with quantum signing keys. We review them and compare them with our DSR-Key.

- **Tokenized signatures [12, 17].** In a tokenized signature scheme, the signing key corresponds to a quantum state which can be used to generate a signature on at most one message. At first sight, the security notion seems to imply the desired security guarantee for DSR-Key, since a signature for a dummy message may serve as the classical deletion certificate for the signing key.[2] However, the problem is that tokenized signatures do not achieve the correctness for DSR-Key; namely, in tokenized signatures, a user who receives a quantum signing key can generate only a single signature, whereas in DSR-Key, we require that a user can generate arbitrarily many signatures before the signing key is revoked. Thus, tokenized signatures are not sufficient for achieving our goal. A similar problem exists for semi-quantum tokenized signatures [40] and one-shot signatures [4] as well.

- **Copy-protection for digital signatures [31] (a.k.a. single-signer signatures [4].[3])** In this primitive, a signing key corresponds to a quantum state which cannot be copied. More precisely, suppose that a user is given one copy of the signing key and tries to split it into two signing keys. The security property requires that at most one of these two signing keys is capable at generating a valid signature on a random message. Amos, Georgiou, Kiayias, and Zhandry [4] constructed such a signature scheme based on one-shot signatures. However, the only known construction of one-shot signatures is relative to classical oracles, and there is no known construction without oracles. Liu, Liu, Qian, and Zhandry [31] constructed it based on indistinguishability obfuscation (iO) and OWFs. Intuitively, copy-protection for digital signatures implies DSR-Key, because checking whether a returned signing key succeeds at generating valid signatures on random messages can serve a means of verification for revocation.[4] Compared with this approach, our construction has the advantage that it is based on the standard assumption (namely the LWE assumption), whereas they require the very strong assumption of iO or ideal oracles. On the other hand, a disadvantage of our construction is that revocation requires private information, whereas theirs have the potential for public revocation. Another disadvantage is that the size of the signing key (and signatures) grows with the number of signatures, whereas this is kept constant in [31] (but not in [4]).

1.4 Technical Overview

Here we give intuitive explanations of our constructions.

Construction of DSR-Key. Our first scheme, DSR-Key, is constructed using *two-tier one-shot signatures* (2-OSS), which is a new primitive which we introduce in this paper.[5] 2-OSS are variants of one-shot signatures [4] for single-bit messages. The main difference with regard to one-shot signatures is that there are two verification algorithms, and a signature for the message “0” is verified by a public verification algorithm, whereas a signature for the massage “1” is verified by a *private* verification algorithm. We believe that the notion of 2-OSS may be of independent interest. Our construction of 2-OSS is conceptually similar to the construction of two-tier quantum lightning in [29], and can be based solely on the LWE assumption.

[2] Note, however, that tokenized signatures offer public verification of signatures, whereas certifying revocation in our DSR-Key scheme takes place in private.

[3] Technically speaking, [31] and [4] require slightly different security definitions, but high level ideas are the same.

[4] While this sounds plausible, there is a subtlety regarding the security definitions. Indeed, we believe that the security of copy-protection for digital signatures [31] or single-signer signatures [4] does not readily imply our security definition in Definition 4, though they do seem to imply some weaker but reasonable variants of security. See also Remark 5.

[5] The term “two-tier” is taken from [29] where they define two-tier quantum lightning, which is a similar variant of quantum lightning [44].

From 2-OSS, we then go on to construct $\mathsf{DSR\text{-}Key}$. We first construct $\mathsf{DSR\text{-}Key}$ for single-bit messages from 2-OSS as follows.[6] The signing key sigk of $\mathsf{DSR\text{-}Key}$ consists of a pair $(\mathsf{sigk}_0, \mathsf{sigk}_1)$ of signing keys of a 2-OSS scheme. To sign a single-bit message $m \in \{0,1\}$, the message "0" is signed with the signing algorithm of a 2-OSS scheme using the signing key sigk_m. Because the signature on m corresponds to a particular signature of "0" with respect to the 2-OSS scheme, it can be verified with the public verification algorithm of 2-OSS. To delete the signing key, the message "1" is signed with the signing algorithm of 2-OSS by using the signing key. The signature for the message "1" corresponds to the revocation certificate, and it can be verified using the private verification algorithm of 2-OSS.

Our aforementioned construction readily implies a *one-time version* of a $\mathsf{DSR\text{-}Key}$ scheme, namely, the correctness and security hold when the signing is used only once. We then upgrade it to the many-time version by using a similar chain-based construction of single-signer signatures from one-shot signatures as in [4]. That is, it works as follows. The signing key and verification key of the many-time scheme are those of the one-time scheme, respectively. We denote them by $(\mathsf{ot.sigk}_0, \mathsf{ot.vk}_0)$. When signing on the first message m_1, the signer first generates a new key pair $(\mathsf{ot.sigk}_1, \mathsf{ot.vk}_1)$ of the one-time scheme, uses $\mathsf{ot.sigk}_0$ to sign on the concatenation $m_1 \| \mathsf{ot.vk}_1$ of the message and the newly generated verification key to generate a signature $\mathsf{ot}.\sigma_1$ of the one-time scheme. Then it outputs $(m_1, \mathsf{ot.vk}_1, \mathsf{ot}.\sigma_1)$ as a signature of the many-time scheme.[7] Similarly, when signing on the k-th message m_k for $k \geq 2$, the signer generates a new key pair $(\mathsf{ot.sigk}_k, \mathsf{ot.vk}_k)$ and uses $\mathsf{ot.sigk}_{k-1}$ to sign on $m_k \| \mathsf{ot.vk}_k$ to generate a signature $\mathsf{ot}.\sigma_k$. Then the signature of the many-time scheme consists of $\{m_i, \mathsf{ot.vk}_i, \mathsf{ot}.\sigma_i\}_{i\in[k]}$. The verification algorithm of the many-time scheme verifies $\mathsf{ot}.\sigma_i$ for all $i \in [k]$ under the corresponding message and verification key, and accepts if all of these verification checks pass. To revoke a signing key, the signer generates revocation certificates for all of the signing keys of the one-time scheme which have previously been generated, and the verification of the revocation certificate simply verifies that all these revocation certificates are valid.[8] It is easy to reduce security of the above many-time scheme to that of the one-time scheme.

Construction of DSR-Sign. Our second scheme, $\mathsf{DSR\text{-}Sign}$, is constructed from what we call *two-tier tokenized signatures* (2-TS), which is a new primitive introduced in this paper. 2-TS are variants of tokenized signatures [12] for single-bit messages where two signature verification algorithms exist. One verification algorithm is used to verify signatures for the message "0", and it uses the public key. The other verification algorithm is used to verify signatures for the message "1", and it uses the *secret* key.

We construct 2-TS from OWFs by using a new lemma that we call the *adaptive hardcore bit property for OWFs*, inspired by a similar notion which was shown for a family of noisy trapdoor claw-free functions by Brakerski et al. [13]. We believe that our lemma may be of independent interest, and enable further applications down the line. The adaptive hardcore bit property for OWFs roughly states that given $|x_0\rangle + (-1)^c |x_1\rangle$ and $(f(x_0), f(x_1))$, no QPT adversary can output (x, d) such that $f(x) \in \{f(x_0), f(x_1)\}$ and $d \cdot (x_0 \oplus x_1) = c$, where f is a OWF, $x_0, x_1 \leftarrow \{0,1\}^\ell$, and $c \leftarrow \{0,1\}$.[9] The adaptive hardcore bit property for OWFs is shown by using a theorem which is implicit in a recent work [10].

[6] The scheme can be extended to the one for multi-bit messages by using the collision resistant hash functions.

[7] We include m_1 in the signature for notational convenience even though this is redundant.

[8] The ability to verify all previously generated signing keys (e.g., as part of a chain) may require secret *trapdoor information.*

[9] We actually need its amplified version, because in this case the adversary can win with probability 1/2 by measuring the state to get x_0 or x_1, and randomly choosing d.

From the adaptive hardcore bit property for OWFs, we construct 2-TS as follows: The quantum signing token is $|x_0\rangle + (-1)^c |x_1\rangle$ with random $x_0, x_1 \leftarrow \{0,1\}^\ell$ and $c \leftarrow \{0,1\}$.[10] The public key is $(f(x_0), f(x_1))$, where f is a OWF, and the secret key is (x_0, x_1, c). To sign the message "0", the token is measured in the computational basis to obtain either x_0 or x_1. To sign the message "1", the token is measured in the Hadamard basis to obtain a string d such that $d \cdot (x_0 \oplus x_1) = c$. The measurement result in the computational basis is then verified with the public key, whereas the measurement result in the Hadamard basis is verified with the secret key. Due to the adaptive hardcore bit property for OWFs (formally shown in Theorem 9), no QPT adversary can output both signatures at the same time.

Finally, we observe that DSR-Sign can be constructed from any 2-TS scheme by considering the quantum signature of DSR-Sign as a quantum signing token of 2-TS. To verify the quantum signature, we sign the message "0" by using the quantum token, and verify it. To delete the quantum signature, we sign the message "1" by using the quantum token. The verification of the revocation certificate requires one to check whether the deletion certificate is a valid signature for message "1" or not.

1.5 Related Works

We have already explained relations between our results and existing works on digital signatures with quantum signing keys. Here, we give a brief review on other related quantum cryptographic primitives.

Certified deletion and revocation. Unruh [42] first initiated the study of quantum revocable encryption. This allows the recipient of a quantum ciphertext to return the state, thereby losing all information about the encrypted message. Quantum encryption with certified deletion [23, 36, 8, 22, 7, 11], first introduced by Broadbent and Islam [14], enables the deletion of quantum ciphertexts, whereby a classical certificate is produced which can be verified. In particular, [8, 22, 24] study the certified everlasting security where the security is guaranteed even against unbounded adversary once a valid deletion certificate is issued. [30] and [10] recently showed a general conversion technique to convert the certified everlasting lemma by Bartusek and Kurana [8] for the private verification to the public one assuming only OWFs (or even weaker assumptions such as hard quantum planted problems for **NP** or the one-way states generators [33]).

The notion of certified deletion has also been used to revoke cryptographic keys [28, 3, 7, 6, 16]. Here, a key is delegated to a user in the form of a quantum state which can later be revoked. Once the key is destroyed and a valid certificate is issued, the functionality associated with the key is no longer available to the user.

Finally, we remark that the notion of revocation has also been considered in the context of more general programs. Ananth and La Placa [5] introduced the notion of secure software leasing. Here, the security guarantees that the functionality of a piece of quantum software is lost once it is returned and verified.

Copy-protection. Copy-protection, introduced by Aaronson [1], is a primitive which allows one to encode a functionality into a quantum state in such a way that it cannot be cloned. [2] showed that any unlearnable functionality can be copy-protected with a classical

[10] Again, we actually consider its amplified version so that the winning probability of the adversary is negligibly small.

oracle. [18] constructed copy-protection schemes for (multi-bit) point functions as well as compute-and-compare programs in the quantum random oracle model. [17] constructed unclonable decryption schemes from iO and compute-and-compare obfuscation for the class of unpredictable distributions, which were previously constructed with classical oracle in [19]. [17] also constructed a copy-protection scheme for pseudorandom functions assuming iO, OWFs, and compute-and-compare obfuscation for the class of unpredictable distributions. [31] constructed bounded collusion-resistant copy-protection for various functionalities (copy-protection of decryption, digital signatures and PRFs) with iO and LWE.

2 Preliminaries

2.1 Basic Notation

We use the standard notations of quantum computing and cryptography. We use λ as the security parameter. For any set S, $x \leftarrow S$ means that an element x is sampled uniformly at random from the set S. We write negl to mean a negligible function. PPT stands for (classical) probabilistic polynomial-time and QPT stands for quantum polynomial-time. For an algorithm A, $y \leftarrow A(x)$ means that the algorithm A outputs y on input x. For two bit strings x and y, $x\|y$ means the concatenation of them. For simplicity, we sometimes omit the normalization factor of a quantum state. (For example, we write $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_1\rangle)$ just as $|x_0\rangle + |x_1\rangle$.) $I \coloneqq |0\rangle\langle 0| + |1\rangle\langle 1|$ is the two-dimensional identity operator. For the notational simplicity, we sometimes write $I^{\otimes n}$ just as I when the dimension is clear from the context. For two density matrices ρ and σ, the trace distance is defined as

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

where $\|\cdot\|_1$ is the trace norm. We also make use of the following result.

▶ **Theorem 1** (Holevo-Helstrom, [25, 21]). *Consider an experiment in which one of two quantum states, either ρ or σ, is sent to a distinguisher with probability $1/2$. Then, any measurement which seeks to discriminate between ρ and σ has success probability p_{succ} at most $p_{succ} \leq \frac{1}{2} + \frac{1}{2}\|\rho - \sigma\|_{\mathrm{tr}}$.*

3 Two-Tier One-Shot Signatures

In this section, we define two-tier one-shot signatures (2-OSS), and construct it from the LWE assumption [38]. Broadly speaking, this cryptographic primitive is a variant of one-shot signatures [4], where the verification of a signature for the message "0" is done publicly, whereas that for the message "1" is done only privately.

3.1 Definition

The formal definition of 2-OSS is as follows.

▶ **Definition 2** (Two-Tier One-Shot Signatures (2-OSS)). *A two-tier one-shot signature scheme is a set* $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Ver}_0, \mathsf{Ver}_1)$ *of algorithms such that*

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{pp}, \mathsf{sk})$: *on input the security parameter λ, it outputs a classical parameter* pp *and a classical secret key* sk.
- $\mathsf{KeyGen}(\mathsf{pp}) \to (\mathsf{sigk}, \mathsf{vk})$: *on input* pp, *it outputs a quantum signing key* sigk *and a classical verification key* vk.

- $\mathsf{Sign}(\mathsf{sigk}, m) \to \sigma$: *on input* sigk *and a single-bit message* $m \in \{0,1\}$*, it outputs a classical signature* σ*.*
- $\mathsf{Ver}_0(\mathsf{pp}, \mathsf{vk}, \sigma) \to \top/\bot$: *on input* pp, vk*, and* σ*, it outputs* $\top/\bot$*.*
- $\mathsf{Ver}_1(\mathsf{pp}, \mathsf{sk}, \mathsf{vk}, \sigma) \to \top/\bot$: *on input* pp, sk*, and* σ*, it outputs* $\top/\bot$*.*

We require the following properties.

Correctness:

$$\Pr\left[\top \leftarrow \mathsf{Ver}_0(\mathsf{pp}, \mathsf{vk}, \sigma) : \begin{array}{r} (\mathsf{sk}, \mathsf{pp}) \leftarrow \mathsf{Setup}(1^\lambda) \\ (\mathsf{sigk}, \mathsf{vk}) \leftarrow \mathsf{KeyGen}(\mathsf{pp}) \\ \sigma \leftarrow \mathsf{Sign}(\mathsf{sigk}, 0) \end{array}\right] \geq 1 - \mathsf{negl}(\lambda) \tag{1}$$

and

$$\Pr\left[\top \leftarrow \mathsf{Ver}_1(\mathsf{pp}, \mathsf{sk}, \mathsf{vk}, \sigma) : \begin{array}{r} (\mathsf{sk}, \mathsf{pp}) \leftarrow \mathsf{Setup}(1^\lambda) \\ (\mathsf{sigk}, \mathsf{vk}) \leftarrow \mathsf{KeyGen}(\mathsf{pp}) \\ \sigma \leftarrow \mathsf{Sign}(\mathsf{sigk}, 1) \end{array}\right] \geq 1 - \mathsf{negl}(\lambda). \tag{2}$$

Security: *For any QPT adversary* $\mathcal{A}$*,*

$$\Pr\left[\top \leftarrow \mathsf{Ver}_0(\mathsf{pp}, \mathsf{vk}, \sigma_0) \wedge \top \leftarrow \mathsf{Ver}_1(\mathsf{pp}, \mathsf{sk}, \mathsf{vk}, \sigma_1) : \begin{array}{r} (\mathsf{sk}, \mathsf{pp}) \leftarrow \mathsf{Setup}(1^\lambda) \\ (\mathsf{vk}, \sigma_0, \sigma_1) \leftarrow \mathcal{A}(\mathsf{pp}) \end{array}\right] \leq \mathsf{negl}(\lambda). \tag{3}$$

3.2 Construction

We show that 2-OSS can be constructed from the LWE assumption [38]. Specifically, we make use of *noisy trapdoor claw-free function* (NTCF) families which allow us to generate quantum states that have a nice structure in both the computational basis, as well as the Hadamard basis. For a detailed definition of NTCF families, we refer to [13].

Our 2-OSS scheme is based on the two-tier quantum lightning scheme in [29] and leverages this structure to sign messages: to sign the message "0", we output a measurement outcome in the computational basis, whereas if we wish to sign "1", we output a measurement outcome in the Hadamard basis. Crucially, the so-called adaptive hardcore-bit property ensures that it is computationally difficult to produce the two outcomes simultaneously. In this context, we use the amplified adaptive hardcore bit property which was shown in [37, 29].

In the full version of the paper, we show the following result.

▶ **Theorem 3.** *Assuming the quantum hardness of the LWE problem, there exists two-tier one-shot signatures.*

4 Digital Signatures with Revocable Signing Keys

In this section, we define digital signatures with revocable signing keys (DSR-Key) and give its construction from 2-OSS.

4.1 Definition

Let us now present a formal definition of DSR-Key. Note that we consider the *stateful* setting which requires that the signer keep a *state* of all previously signed messages and keys.

▶ **Definition 4** ((Stateful) Digital Signatures with Revocable Signing Keys (DSR-Key)). *A (stateful) digital signature scheme with revocable signing keys is the following set of algorithms* (Setup, KeyGen, Sign, Ver, Del, Cert) *consisting of:*

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{ck}, \mathsf{pp})$: *on input the security parameter λ, it outputs a classical key* ck *and a classical parameter* pp.
- $\mathsf{KeyGen}(\mathsf{pp}) \to (\mathsf{sigk}_0, \mathsf{vk})$: *on input* pp*, it outputs a quantum signing key* sigk_0 *and a classical verification key* vk.
- $\mathsf{Sign}(\mathsf{pp}, \mathsf{sigk}_i, m) \to (\mathsf{sigk}_{i+1}, \sigma)$: *on input* pp*, a message m and a signing key* sigk_i*, it outputs a subsequent signing key* sigk_{i+1} *and a classical signature σ.*
- $\mathsf{Ver}(\mathsf{pp}, \mathsf{vk}, m, \sigma) \to \top/\bot$: *on input* pp*,* vk*, m, and σ, it outputs $\top/\bot$.*
- $\mathsf{Del}(\mathsf{sigk}_i) \to \mathsf{cert}$: *on input* sigk_i*, it outputs a classical certificate* cert.
- $\mathsf{Cert}(\mathsf{pp}, \mathsf{vk}, \mathsf{ck}, \mathsf{cert}, S) \to \top/\bot$: *on input* pp*,* vk*,* ck*,* cert*, and a set S consisting of messages, it outputs $\top/\bot$.*

We require the following properties.

Many-time correctness: *For any polynomial $p = p(\lambda)$, and any messages $(m_1, m_2, ..., m_p)$,*

$$\Pr\left[\bigwedge_{i\in[p]} \top \leftarrow \mathsf{Ver}(\mathsf{pp}, \mathsf{vk}, m_i, \sigma_i) : \begin{array}{r} (\mathsf{pp}, \mathsf{ck}) \leftarrow \mathsf{Setup}(1^\lambda) \\ (\mathsf{sigk}_0, \mathsf{vk}) \leftarrow \mathsf{KeyGen}(\mathsf{pp}) \\ (\mathsf{sigk}_1, \sigma_1) \leftarrow \mathsf{Sign}(\mathsf{pp}, \mathsf{sigk}_0, m_1) \\ (\mathsf{sigk}_2, \sigma_2) \leftarrow \mathsf{Sign}(\mathsf{pp}, \mathsf{sigk}_1, m_2) \\ \dots \\ (\mathsf{sigk}_p, \sigma_p) \leftarrow \mathsf{Sign}(\mathsf{pp}, \mathsf{sigk}_{p-1}, m_p) \end{array}\right] \geq 1 - \mathsf{negl}(\lambda). \quad (4)$$

We say that the scheme satisfies one-time correctness if the above is satisfied for $p = 1$.

EUF-CMA security: *For any QPT adversary $\mathcal{A}$,*

$$\Pr\left[\top \leftarrow \mathsf{Ver}(\mathsf{pp}, \mathsf{vk}, m^*, \sigma^*) : \begin{array}{r} (\mathsf{pp}, \mathsf{ck}) \leftarrow \mathsf{Setup}(1^\lambda) \\ (\mathsf{sigk}_0, \mathsf{vk}) \leftarrow \mathsf{KeyGen}(\mathsf{pp}) \\ (m^*, \sigma^*) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{Sign}}}(\mathsf{vk}) \end{array}\right] \leq \mathsf{negl}(\lambda), \quad (5)$$

where $\mathcal{O}_{\mathsf{Sign}}$ is a stateful signing oracle defined below and $\mathcal{A}$ is not allowed to query the oracle on m^*:

$\mathcal{O}_{\mathsf{Sign}}$*: Its initial state is set to be* $(\mathsf{pp}, \mathsf{sigk}_0)$*. When a message m is queried, it proceeds as follows:*

- *Parse its state as* $(\mathsf{pp}, \mathsf{sigk}_i)$.
- *Run* $(\mathsf{sigk}_{i+1}, \sigma) \leftarrow \mathsf{Sign}(\mathsf{pp}, \mathsf{sigk}_i, m)$.
- *Return σ to $\mathcal{A}$ and update its state to* $(\mathsf{pp}, \mathsf{sigk}_{i+1})$.

We say that the scheme satisfies one-time EUF-CMA security if Equation (5) holds for any $\mathcal{A}$ that submits at most one query to the oracle.

Many-time deletion correctness: *For any polynomial $p = p(\lambda)$, and any messages $(m_1, m_2, ..., m_p)$, the quantity*

$$\Pr\left[\top \leftarrow \mathsf{Cert}(\mathsf{pp}, \mathsf{vk}, \mathsf{ck}, \mathsf{cert}, \{m_1, m_2, ..., m_p\}) : \begin{array}{r} (\mathsf{pp}, \mathsf{ck}) \leftarrow \mathsf{Setup}(1^\lambda) \\ (\mathsf{sigk}_0, \mathsf{vk}) \leftarrow \mathsf{KeyGen}(\mathsf{pp}) \\ (\mathsf{sigk}_1, \sigma_1) \leftarrow \mathsf{Sign}(\mathsf{pp}, \mathsf{sigk}_0, m_1) \\ (\mathsf{sigk}_2, \sigma_2) \leftarrow \mathsf{Sign}(\mathsf{pp}, \mathsf{sigk}_1, m_2) \\ \dots \\ (\mathsf{sigk}_p, \sigma_p) \leftarrow \mathsf{Sign}(\mathsf{pp}, \mathsf{sigk}_{p-1}, m_p) \\ \mathsf{cert} \leftarrow \mathsf{Del}(\mathsf{sigk}_p) \end{array}\right] \quad (6)$$

is at least $1 - \mathsf{negl}(\lambda)$. We remark that we require the above to also hold for the case of $p = 0$, in which case the fifth component of the input of Cert *is the empty set $\emptyset$. We say that the scheme satisfies one-time deletion correctness if the above property is satisfied for $p \leq 1$.*

Many-time deletion security: *For any QPT adversary $\mathcal{A}$,*

$$\Pr\left[\begin{array}{l} \top \leftarrow \mathsf{Cert}(\mathsf{pp}, \mathsf{vk}, \mathsf{ck}, \mathsf{cert}, S) \\ \wedge\ m^* \notin S \\ \wedge\ \top \leftarrow \mathsf{Ver}(\mathsf{pp}, \mathsf{vk}, m^*, \sigma^*) \end{array} : \begin{array}{r} (\mathsf{pp}, \mathsf{ck}) \leftarrow \mathsf{Setup}(1^\lambda) \\ (\mathsf{vk}, \mathsf{cert}, S, m^*, \sigma^*) \leftarrow \mathcal{A}(\mathsf{pp}) \end{array}\right] \leq \mathsf{negl}(\lambda). \tag{7}$$

We say that the scheme satisfies one-time deletion security if the above property is satisfied if we additionally require $|S| \leq 1$.

▶ Remark 5. Following the definition of single signer security in [4] or copy-protection security in [31], it is also reasonable to define deletion security as follows:

For any pair $(\mathcal{A}_1, \mathcal{A}_2)$ of QPT adversaries and any distribution $\mathcal{D}$ with super-logarithmic min-entropy over the message space, the following probability is negligible in λ:

$$\Pr\left[\top \leftarrow \mathsf{Cert}(\mathsf{pp}, \mathsf{vk}, \mathsf{ck}, \mathsf{cert}, S) \wedge \top \leftarrow \mathsf{Ver}(\mathsf{pp}, \mathsf{vk}, m, \sigma) : \begin{array}{r} (\mathsf{pp}, \mathsf{ck}) \leftarrow \mathsf{Setup}(1^\lambda) \\ (\mathsf{vk}, \mathsf{cert}, S, \mathsf{st}) \leftarrow \mathcal{A}_1(\mathsf{pp}) \\ m \leftarrow \mathcal{D} \\ \sigma \leftarrow \mathcal{A}_2(m, \mathsf{st}) \end{array}\right]. \tag{8}$$

It is easy to see that our definition implies the above, but the converse is unlikely. This is why we define deletion security as in Definition 4.

4.2 One-Time Construction for Single-Bit Messages

In the full version of the paper, we construct one-time DSR-Key for single-bit messages from 2-OSS in a black-box way.

▶ **Theorem 6.** *If two-tier one-shot signatures exist, then digital signatures with revocable signing keys with the message space $\{0,1\}$ that satisfy one-time variants of correctness, EUF-CMA security, deletion correctness, and deletion security in Definition 4 exist.*

4.3 From Single-Bit to Multi-Bit Messages

In the full version of the paper, we also show the following theorem which says that we can expand the message space to $\{0,1\}^*$ using collision-resistant hashes.

▶ **Theorem 7.** *If collision-resistant hash functions and digital signatures with revocable signing keys with the message space $\{0,1\}$ that satisfy one-time variants of correctness, EUF-CMA security, deletion correctness, and deletion security in Definition 4 exist, then a similar scheme with the message space $\{0,1\}^*$ exists.*

The proof of correctness is immediate and the proof of one-time EUF-CMA security follows from standard techniques which allow conventional signature schemes to handle messages of arbitrarily length, see [27] for example. Therefore, it suffices to show that the scheme Σ' satisfies the one-time variants of deletion correctness and deletion security. We show this in the full version.

4.4 From One-Time Schemes to Many-Time Schemes

In this section, we show how to extend any one-time scheme into a proper many-time scheme as in Definition 4. The transformation is inspired by the chain-based approach for constructing many-time digital signatures, see [27] for example.[11]

Let $\mathsf{OT} = (\mathsf{OT.Setup}, \mathsf{OT.KeyGen}, \mathsf{OT.Sign}, \mathsf{OT.Ver}, \mathsf{OT.Del}, \mathsf{OT.Cert})$ be a scheme which satisfies the one-time variants of correctness, EUF-CMA security, deletion correctness, and deletion security according to in Definition 4, and has the message space $\{0,1\}^*$. Then, we construct $\mathsf{MT} = (\mathsf{MT.Setup}, \mathsf{MT.KeyGen}, \mathsf{MT.Sign}, \mathsf{MT.Ver}, \mathsf{MT.Del}, \mathsf{MT.Cert})$ with the message space $\{0,1\}^n$ as follows:

- $\mathsf{MT.Setup}(1^\lambda) \to (\mathsf{ck}, \mathsf{pp})$: This is the same as $\mathsf{OT.Setup}$.
- $\mathsf{MT.KeyGen}(\mathsf{pp}) \to (\mathsf{sigk}, \mathsf{vk})$: run $(\mathsf{ot.sigk}_0, \mathsf{ot.vk}_0) \leftarrow \mathsf{OT.KeyGen}(\mathsf{pp})$ and output $\mathsf{sigk} := \mathsf{ot.sigk}_0$ as the quantum signing key and $\mathsf{vk} := \mathsf{ot.vk}_0$ as the classical verification key.
- $\mathsf{MT.Sign}(\mathsf{pp}, \mathsf{sigk}_i, m) \to (\mathsf{sigk}_{i+1}, \sigma)$: on input the public parameter pp, a quantum signing key sigk_i, and a message $m \in \{0,1\}^n$ proceed as follows:
  1. Parse sigk_i as $(\mathsf{ot.sigk}_i, \{\mathsf{ot.sigk}'_j\}_{j\in\{0,1,\dots,i-1\}}, \{m_j, \mathsf{ot.vk}_j, \mathsf{ot.}\sigma_j\}_{j\in[i]})$
  2. Generate $(\mathsf{ot.sigk}_{i+1}, \mathsf{ot.vk}_{i+1}) \leftarrow \mathsf{OT.KeyGen}(\mathsf{pp})$.
  3. Run
  $$(\mathsf{ot.sigk}'_i, \mathsf{ot.}\sigma_{i+1}) \leftarrow \mathsf{OT.Sign}(\mathsf{pp}, \mathsf{ot.sigk}_i, m \| \mathsf{ot.vk}_{i+1}).$$
  4. Set $m_{i+1} := m$ and output a subsequent signing key
  $$\mathsf{sigk}_{i+1} := (\mathsf{ot.sigk}_{i+1}, \{\mathsf{ot.sigk}'_j\}_{j\in\{0,1,\dots,i\}}, \{m_j, \mathsf{ot.vk}_j, \mathsf{ot.}\sigma_j\}_{j\in[i+1]})$$
  and a signature
  $$\sigma := \{m_j, \mathsf{ot.vk}_j, \mathsf{ot.}\sigma_j\}_{j\in[i+1]}.$$
- $\mathsf{MT.Ver}(\mathsf{pp}, \mathsf{vk}, m, \sigma) \to \top/\bot$: on input pp, a key vk, a message m, and signature σ, proceed as follows.
  1. Parse σ as $\{m_j, \mathsf{ot.vk}_j, \mathsf{ot.}\sigma_j\}_{j\in[i]}$ and let $\mathsf{ot.vk}_0 = \mathsf{vk}$.
  2. Output $\top$ if $m = m_i$ and $\mathsf{OT.Ver}(\mathsf{pp}, \mathsf{ot.vk}_{j-1}, m_j \| \mathsf{ot.vk}_j, \mathsf{ot.}\sigma_j) = \top$ for every $j \in [i]$.
- $\mathsf{MT.Del}(\mathsf{sigk}_i) \to \mathsf{cert}$: on input sigk, proceed as follows:
  1. Parse sigk_i as $(\mathsf{ot.sigk}_i, \{\mathsf{ot.sigk}'_j\}_{j\in\{0,1,\dots,i-1\}}, \{m_j, \mathsf{ot.vk}_j, \mathsf{ot.}\sigma_j\}_{j\in[i]})$.
  2. For $j \in \{0, 1, \dots, i-1\}$, run $\mathsf{ot.cert}_j \leftarrow \mathsf{OT.Del}(\mathsf{ot.sigk}'_j)$.
  3. Run $\mathsf{ot.cert}_i \leftarrow \mathsf{OT.Del}(\mathsf{ot.sigk}_i)$.
  4. Output $\mathsf{cert} := \{\mathsf{ot.cert}_j, m_j, \mathsf{ot.vk}_j, \mathsf{ot.}\sigma_j\}_{j\in[i]}$.
- $\mathsf{MT.Cert}(\mathsf{pp}, \mathsf{vk}, \mathsf{ck}, \mathsf{cert}, S) \to \top/\bot$: on input $\mathsf{pp}, \mathsf{vk}, \mathsf{ck}$, cert, and S, parse the certificate cert as a tuple $\{\mathsf{ot.cert}_j, m_j, \mathsf{ot.vk}_j, \mathsf{ot.}\sigma_j\}_{j\in[i]}$, let $\mathsf{ot.vk}_0 = \mathsf{vk}$, and output $\top$ if the following holds:
  - $S = \{m_1, m_2, \dots, m_i\}$,
  - $\mathsf{OT.Cert}(\mathsf{ot.vk}_{j-1}, \mathsf{ck}, \mathsf{ot.cert}_{j-1}, \{m_j \| \mathsf{ot.vk}_j\}) = \top$ for every $j \in [i]$, and
  - $\mathsf{OT.Cert}(\mathsf{ot.vk}_i, \mathsf{ck}, \mathsf{ot.cert}_i, \emptyset) = \top$.

In the full version of the paper, we prove the following theorem.

[11] We could also use the tree-based construction [32], which has a shorter (logarithmic) signature length. We describe the chain-based construction here for ease of presentation.

▶ **Theorem 8.** *Suppose that* $(\mathsf{OT.Setup}, \mathsf{OT.KeyGen}, \mathsf{OT.Sign}, \mathsf{OT.Ver}, \mathsf{OT.Del}, \mathsf{OT.Cert})$ *satisfies the one-time variants of correctness, EUF-CMA security, deletion correctness, and deletion security in Definition 4. Then, the "many-time scheme" which consists of the tuple* $(\mathsf{MT.Setup}, \mathsf{MT.KeyGen}, \mathsf{MT.Sign}, \mathsf{MT.Ver}, \mathsf{MT.Del}, \mathsf{MT.Cert})$ *satisfies many-time variants of each of the properties.*

5 Adaptive Hardcore Bit Property for OWFs

In this section, we introduce a new concept, which we call *adaptive hardcore bit property for OWFs*, and show it from the existence of OWFs. This property is inspired by the adaptive hardcore bit property which was shown for a family of noisy trapdoor claw-free functions by Brakerski et al. [13]. Our notion of the adaptive hardcore bit property for OWFs will be used to construct two-tier tokenized signatures.

5.1 Statements

The formal statement of the adaptive hardcore bit property for OWFs is given as follows. (Its proof is given later.)

▶ **Theorem 9** (Adaptive Hardcore Bit Property for OWFs). *Let* $\lambda \in \mathbb{N}$ *be the security parameter and let* $\ell(\lambda), \kappa(\lambda) \in \mathbb{N}$ *be polynomials. Let* $f : \{0,1\}^{\ell(\lambda)} \to \{0,1\}^{\kappa(\lambda)}$ *be a (quantumly-secure) OWF. Then, for any QPT adversary* $\{\mathcal{A}_\lambda\}_{\lambda \in \mathbb{N}}$*, it holds that*

$$\Pr\left[\begin{array}{c} f(x) \in \{f(x_0), f(x_1)\} \\ \bigwedge \\ d \cdot (x_0 \oplus x_1) = c \end{array} : \begin{array}{l} x_0 \leftarrow \{0,1\}^{\ell(\lambda)},\ x_1 \leftarrow \{0,1\}^{\ell(\lambda)} \\ c \leftarrow \{0,1\} \\ (x,d) \leftarrow \mathcal{A}_\lambda\left(\frac{|x_0\rangle + (-1)^c |x_1\rangle}{\sqrt{2}}, f(x_0), f(x_1)\right) \end{array}\right] \le \frac{1}{2} + \mathsf{negl}(\lambda). \tag{9}$$

We actually use its amplified version, which is given as follows. (Its proof is given later.)

▶ **Theorem 10** (Amplified Adaptive Hardcore Bit Property for OWFs). *Let* $\lambda \in \mathbb{N}$ *be the security parameter and let* $\ell(\lambda), \kappa(\lambda), n(\lambda) \in \mathbb{N}$ *be polynomials. Let* $f : \{0,1\}^{\ell(\lambda)} \to \{0,1\}^{\kappa(\lambda)}$ *be a (quantumly-secure) OWF. Then, for any QPT adversary* $\{\mathcal{A}_\lambda\}_{\lambda \in \mathbb{N}}$*, it holds that*

$$\Pr\left[\begin{array}{c} \wedge_{i \in [n]} f(x_i) \in \{f(x_i^0), f(x_i^1)\} \\ \bigwedge \\ \wedge_{i \in [n]} d_i \cdot (x_i^0 \oplus x_i^1) = c_i \end{array} : \begin{array}{l} \forall i \in [n] \,:\, x_i^0 \leftarrow \{0,1\}^{\ell(\lambda)},\ x_i^1 \leftarrow \{0,1\}^{\ell(\lambda)} \\ \forall i \in [n] \,:\, c_i \leftarrow \{0,1\} \\ \{x_i, d_i\}_{i \in [n]} \leftarrow \mathcal{A}_\lambda\left(\bigotimes_{i=1}^n \frac{|x_i^0\rangle + (-1)^{c_i} |x_i^1\rangle}{\sqrt{2}}, \{f(x_i^b)\}_{i,b}\right) \end{array}\right] \tag{10}$$

is at most negligible in λ.

5.2 Theorem of [10]

In order to show adaptive hardcore bit property for OWFs, we use the following theorem which is implicit in [10, Theorem 3.1]. The only difference is that we additionally reveal both pre-images as part of the distribution $\left\{\widetilde{\mathcal{Z}}_\lambda^{\mathcal{A}_\lambda}(b)\right\}_{\lambda \in \mathbb{N}, b \in \{0,1\}}$. We remark that the proof is the same.

▶ **Theorem 11** (Implicit in [10], Theorem 3.1). *Let* $\lambda \in \mathbb{N}$ *be the security parameter, and let* $\ell(\lambda), \kappa(\lambda) \in \mathbb{N}$ *be polynomials. Let* $f : \{0,1\}^{\ell(\lambda)} \to \{0,1\}^{\kappa(\lambda)}$ *be a OWF secure against QPT adversaries. Let* $\{\mathcal{Z}_\lambda(\cdot,\cdot,\cdot,\cdot)\}_{\lambda \in \mathbb{N}}$ *be a quantum operation with four arguments: an* $\ell(\lambda)$*-bit* *string z, two $\kappa(\lambda)$-bit strings y_0, y_1, and an $\ell(\lambda)$-qubit quantum state $|\psi\rangle$. Suppose that for any QPT adversary $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$, $z \in \{0,1\}^{\ell(\lambda)}, y_0, y_1 \in \{0,1\}^{\kappa(\lambda)}$, and $\ell(\lambda)$-qubit state $|\psi\rangle$,*

$$\left|\Pr\left[\mathcal{A}_\lambda(\mathcal{Z}_\lambda(z, y_0, y_1, |\psi\rangle)) = 1\right] - \Pr\left[\mathcal{A}_\lambda(\mathcal{Z}_\lambda(0^{\ell(\lambda)}, y_0, y_1, |\psi\rangle)) = 1\right]\right| = \mathsf{negl}(\lambda).$$

That is, $\mathcal{Z}_\lambda$ is semantically-secure with respect to its first input. Now, for any QPT adversary $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$, consider the distribution $\left\{\widetilde{\mathcal{Z}}_\lambda^{\mathcal{A}_\lambda}(b)\right\}_{\lambda\in\mathbb{N}, b\in\{0,1\}}$ over quantum states, obtained by running $\mathcal{A}_\lambda$ as follows.

- *Sample $x_0, x_1 \leftarrow \{0,1\}^{\ell(\lambda)}$, define $y_0 = f(x_0), y_1 = f(x_1)$ and initialize $\mathcal{A}_\lambda$ with*
$$\mathcal{Z}_\lambda\left(x_0 \oplus x_1, y_0, y_1, \frac{|x_0\rangle + (-1)^b |x_1\rangle}{\sqrt{2}}\right).$$
- *$\mathcal{A}_\lambda$'s output is parsed as a string $x' \in \{0,1\}^{\ell(\lambda)}$ and a residual state on register A'.*
- *If $f(x') \in \{y_0, y_1\}$, then output (x_0, x_1, A'), and otherwise output $\bot$.*

Then, it holds that

$$\left\|\widetilde{\mathcal{Z}}_\lambda^{\mathcal{A}_\lambda}(0) - \widetilde{\mathcal{Z}}_\lambda^{\mathcal{A}_\lambda}(1)\right\|_{\mathrm{tr}} \leq \mathsf{negl}(\lambda). \tag{11}$$

We can show the following parallel version. (It can be shown by the standard hybrid argument. A detailed proof is given in the full version of the paper.)

▶ **Theorem 12** (Parallel version of Theorem 11)**.** *Let $\lambda \in \mathbb{N}$ be the security parameter. Let $\ell(\lambda), \kappa(\lambda), n(\lambda) \in \mathbb{N}$ be polynomials. Let $f : \{0,1\}^{\ell(\lambda)} \to \{0,1\}^{\kappa(\lambda)}$ be a OWF secure against QPT adversaries. Let $\{\mathcal{Z}_\lambda(\cdot,\cdot,\cdot,\cdot)\}_{\lambda\in\mathbb{N}}$ be a quantum operation with four arguments: an $\ell(\lambda)$-bit string z, two $\kappa(\lambda)$-bit strings y_0, y_1, and an $\ell(\lambda)$-qubit quantum state $|\psi\rangle$. Suppose that for any QPT adversary $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$, $z \in \{0,1\}^{\ell(\lambda)}, y_0, y_1 \in \{0,1\}^{\kappa(\lambda)}$, and $\ell(\lambda)$-qubit state $|\psi\rangle$,*

$$\left|\Pr\left[\mathcal{A}_\lambda(\mathcal{Z}_\lambda(z, y_0, y_1, |\psi\rangle)) = 1\right] - \Pr\left[\mathcal{A}_\lambda(\mathcal{Z}_\lambda(0^{\ell(\lambda)}, y_0, y_1, |\psi\rangle)) = 1\right]\right| = \mathsf{negl}(\lambda).$$

That is, $\mathcal{Z}_\lambda$ is semantically-secure with respect to its first input. Now, for any QPT adversary $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$, consider the distribution $\left\{\widetilde{\mathcal{Z}}_\lambda^{\mathcal{A}_\lambda}(b_1, ..., b_{n(\lambda)})\right\}_{\lambda\in\mathbb{N}, b_i\in\{0,1\}}$ over quantum states, obtained by running $\mathcal{A}_\lambda$ as follows.

- *Sample $x_i^0, x_i^1 \leftarrow \{0,1\}^{\ell(\lambda)}$ for each $i \in [n(\lambda)]$, define $y_i^0 = f(x_i^0), y_i^1 = f(x_i^1)$ and initialize $\mathcal{A}_\lambda$ with*
$$\bigotimes_{i\in[n(\lambda)]} \mathcal{Z}_\lambda\left(x_i^0 \oplus x_i^1, y_i^0, y_i^1, \frac{|x_i^0\rangle + (-1)^{b_i} |x_i^1\rangle}{\sqrt{2}}\right). \tag{12}$$
- *$\mathcal{A}_\lambda$'s output is parsed as strings $x_i' \in \{0,1\}^{\ell(\lambda)}$ for $i \in [n(\lambda)]$ and a residual state on register A'.*
- *If $f(x_i') \in \{y_i^0, y_i^1\}$ for all $i \in [n(\lambda)]$, output $(\{x_i^0\}_{i\in[n(\lambda)]}, \{x_i^1\}_{i\in[n(\lambda)]}, \mathsf{A}')$, and otherwise output $\bot$.*

Then, there exists a negligible function $\mathsf{negl}(\lambda)$ such that for any $b_1, ..., b_{n(\lambda)} \in \{0,1\}$,

$$\left\|\widetilde{\mathcal{Z}}_\lambda^{\mathcal{A}_\lambda}(b_1, ..., b_{n(\lambda)}) - \widetilde{\mathcal{Z}}_\lambda^{\mathcal{A}_\lambda}(0, ..., 0)\right\|_{\mathrm{tr}} \leq \mathsf{negl}(\lambda). \tag{13}$$

5.3 Proof of Theorem 9

By using Theorem 11, we can show Theorem 9 as follows. Here, we leverage the fact that any algorithm that simultaneously produces both a valid pre-image of the OWF, as well as a string which leaks information about the relative phase between the respective pre-images, must necessarily violate Theorem 11.

Proof of Theorem 9. Let $\ell(\lambda), \kappa(\lambda) \in \mathbb{N}$ be polynomials, and let $f : \{0,1\}^{\ell(\lambda)} \to \{0,1\}^{\kappa(\lambda)}$ be a (quantumly-secure) OWF. Suppose there exist a QPT algorithm $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$ and a polynomial $p(\lambda)$ such that, for random $x_0, x_1 \leftarrow \{0,1\}^\ell$ and $c \leftarrow \{0,1\}$, it holds that

$$\Pr\left[\bigwedge_{d\cdot(x_0\oplus x_1)=c}^{f(x)\in\{f(x_0),f(x_1)\}} : (x,d) \leftarrow \mathcal{A}_\lambda\left(\frac{|x_0\rangle + (-1)^c|x_1\rangle}{\sqrt{2}}, f(x_0), f(x_1)\right)\right] \geq \frac{1}{2} + \frac{1}{p(\lambda)} \quad (14)$$

for infinitely many λ. We now show how to construct an algorithm that violates Theorem 11. For simplicity, we define the quantum operation $\{\mathcal{Z}_\lambda(\cdot,\cdot,\cdot,\cdot)\}_{\lambda\in\mathbb{N}}$ in Theorem 11 as

$$\mathcal{Z}_\lambda\left(x_0 \oplus x_1, f(x_0), f(x_1), \frac{|x_0\rangle + (-1)^c|x_1\rangle}{\sqrt{2}}\right) := \left(f(x_0), f(x_1), \frac{|x_0\rangle + (-1)^c|x_1\rangle}{\sqrt{2}}\right).$$

Evidently, our choice of $\mathcal{Z}_\lambda$ is trivially semantically secure with respect to the first argument. Consider the following QPT algorithm $\mathcal{B}_\lambda$:

1. On input $\left(f(x_0), f(x_1), \frac{|x_0\rangle+(-1)^c|x_1\rangle}{\sqrt{2}}\right)$, run
$$(x, d_c) \leftarrow \mathcal{A}_\lambda\left(\frac{|x_0\rangle + (-1)^c|x_1\rangle}{\sqrt{2}}, f(x_0), f(x_1)\right).$$
2. Output x and assign $|d_c\rangle\langle d_c|$ as the residual state.[12]

Adopting the notation from Theorem 11, we define $\widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(c)$.[13] Consider the following distinguisher that distinguishes $\widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(c)$ for $c \in \{0,1\}$:

1. Get $\widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(c)$ as input.
2. If it is $\perp$, output $\perp$ and abort.
3. Output $d_c \cdot (x_0 \oplus x_1) \pmod 2$.

From Equation (14), there exists a polynomial $p(\lambda)$ such that both $f(x) \in \{f(x_0), f(x_1)\}$ and $d_c \cdot (x_0 \oplus x_1) = c \pmod 2$ occur with probability at least $\frac{1}{2} + \frac{1}{p(\lambda)}$. Thus, the distinguisher can distinguish $\widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(0)$ and $\widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(1)$ with probability at least $\frac{1}{2} + \frac{1}{p(\lambda)}$, but this means

$$\left\|\widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(0) - \widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(1)\right\|_{\mathrm{tr}} \geq \frac{2}{p(\lambda)}.$$

from Theorem 1. This violates Theorem 11. ◀

5.4 Proof of Theorem 10

In this subsection, we show Theorem 10 by using Theorem 12.

[12] Note that we can think of d_c as a classical mixture (i.e., density matrix) over the randomness of $x_0, x_1 \leftarrow \{0,1\}^\ell$, $c \leftarrow \{0,1\}$ and the internal randomness of the algorithm $\mathcal{A}_\lambda$.

[13] It is, roughly speaking, $|x_0\rangle\langle x_0| \otimes |x_1\rangle\langle x_1| \otimes |d_c\rangle\langle d_c|$ for $c \in \{0,1\}$ when $f(x) \in \{f(x_0), f(x_1)\}$, and is $\perp$ when $f(x) \notin \{f(x_0), f(x_1)\}$.

Proof of Theorem 10. For the sake of contradiction, assume that there is a QPT adversary $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$ such that the following quantity

$$\Pr\left[\begin{array}{c}\wedge_{i\in[n]} f(x_i)\in\{f(x_i^0),f(x_i^1)\}\\ \bigwedge\\ \wedge_{i\in[n]} d_i\cdot(x_i^0\oplus x_i^1)=c_i\end{array} : \begin{array}{l}\forall i\in[n]:\ x_i^0\leftarrow\{0,1\}^\ell,\ x_i^1\leftarrow\{0,1\}^\ell, c_i\leftarrow\{0,1\}\\ \{x_i,d_i\}_{i\in[n]}\leftarrow\mathcal{A}_\lambda\left(\bigotimes_{i=1}^n\frac{|x_i^0\rangle+(-1)^{c_i}|x_i^1\rangle}{\sqrt{2}},\{f(x_i^b)\}_{i,b}\right)\end{array}\right] \tag{15}$$

is at least $1/\mathrm{poly}(\lambda)$ for infinitely many λ. We consider the quantum operation $\{\mathcal{Z}_\lambda(\cdot,\cdot,\cdot,\cdot)\}_{\lambda\in\mathbb{N}}$ in Theorem 12 as

$$\mathcal{Z}_\lambda\left(x_0\oplus x_1, f(x_0), f(x_1), \frac{|x_0\rangle+(-1)^c|x_1\rangle}{\sqrt{2}}\right) := \left(f(x_0), f(x_1), \frac{|x_0\rangle+(-1)^c|x_1\rangle}{\sqrt{2}}\right), \tag{16}$$

which is trivially semantically secure with respect to the first argument. From such $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$ and $\{\mathcal{Z}_\lambda\}_{\lambda\in\mathbb{N}}$, we construct the following QPT adversary $\{\mathcal{B}_\lambda\}_{\lambda\in\mathbb{N}}$ for fixed each $(c_1,...,c_n)\in\{0,1\}^n$:

1. Get $\{f(x_i^b)\}_{i\in[n],b\in\{0,1\}}$ and $\bigotimes_{i\in[n]}\frac{|x_i^0\rangle+(-1)^{c_i}|x_i^1\rangle}{\sqrt{2}}$ as input.
2. Run $(\{x_i\}_{i\in[n]},\{d_i\}_{i\in[n]})\leftarrow\mathcal{A}_\lambda\left(\bigotimes_{i=1}^n\frac{|x_i^0\rangle+(-1)^{c_i}|x_i^1\rangle}{\sqrt{2}},\{f(x_i^b)\}_{i\in[n],b\in\{0,1\}}\right)$.
3. Output $\{x_i\}_{i\in[n]}$. Set its residual state as $\bigotimes_{i\in[n]}|d_i\rangle\langle d_i|$.

Then, by using the notation of Theorem 12, we define $\widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(c_1,...,c_n)$.[14] Let us consider the following QPT distinguisher $\{\mathcal{D}_\lambda\}_{\lambda\in\mathbb{N}}$:

1. Get $\widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(c_1,...,c_n)$ as input.
2. If it is $\perp$, output $\perp$. Otherwise, parse it as $\left(\bigotimes_{i\in[n],b\in\{0,1\}}|x_i^b\rangle\langle x_i^b|\right)\otimes\left(\bigotimes_{i\in[n]}|d_i\rangle\langle d_i|\right)$.
3. Compute $c_i' := d_i\cdot(x_i^0\oplus x_i^1)$ for each $i\in[n]$. Output $\{c_i'\}_{i\in[n]}$.

Then, from Equation (15),

$$\frac{1}{2^n}\sum_{(c_1,...,c_n)\in\{0,1\}^n}\Pr[(c_1,...,c_n)\leftarrow\mathcal{D}(\widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(c_1,...,c_n))]\geq\frac{1}{\mathrm{poly}(\lambda)} \tag{17}$$

for infinitely many λ. Now we show that it contradicts Theorem 12.

If Theorem 12 is correct, there exists a negligible function negl such that

$$\left\|\widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(c_1,...,c_n)-\widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(0,...,0)\right\|_{\mathrm{tr}}\leq\mathsf{negl}(\lambda) \tag{18}$$

for all $(c_1,...,c_n)\in\{0,1\}^n$. However, in that case, there exists a negligible function negl such that

$$\left|\Pr\left[(c_1,...,c_n)\leftarrow\mathcal{D}(\widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(c_1,...,c_n))\right]-\Pr\left[(c_1,...,c_n)\leftarrow\mathcal{D}(\widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(0,...,0))\right]\right|\leq\mathsf{negl}(\lambda) \tag{19}$$

for all $(c_1,...,c_n)\in\{0,1\}^n$. Then we have

[14] Roughly speaking, it is $\left(\bigotimes_{i\in[n],b\in\{0,1\}}|x_i^b\rangle\langle x_i^b|\right)\otimes\left(\bigotimes_{i\in[n]}|d_i\rangle\langle d_i|\right)$ if $f(x_i)\in\{f(x_i^0),f(x_i^1)\}$ for all $i\in[n]$, and it is $\perp$ otherwise.

$$\frac{1}{\mathrm{poly}(\lambda)} \leq \frac{1}{2^n}\sum_{(c_1,...,c_n)\in\{0,1\}^n} \Pr[(c_1,...,c_n)\leftarrow \mathcal{D}(\widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(c_1,...,c_n))] \tag{20}$$

$$\leq \frac{1}{2^n}\sum_{(c_1,...,c_n)\in\{0,1\}^n} \Big(\Pr[(c_1,...,c_n)\leftarrow \mathcal{D}(\widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(0,...,0))] + \mathsf{negl}(\lambda)\Big) \tag{21}$$

$$\leq \frac{1}{2^n}\sum_{(c_1,...,c_n)\in\{0,1\}^n} \Pr[(c_1,...,c_n)\leftarrow \mathcal{D}(\widetilde{\mathcal{Z}}_\lambda^{\mathcal{B}_\lambda}(0,...,0))] + \mathsf{negl}(\lambda) \tag{22}$$

$$\leq \frac{1}{2^n} + \mathsf{negl}(\lambda) \tag{23}$$

for infinitely many λ, which yields a contradiction. Here, the first inequality is from Equation (17), the second inequality is from Equation (19), and the last inequality is from the fact that $\sum_{(c_1,...,c_n)\in\{0,1\}^n}\Pr[(c_1,...,c_n)\leftarrow\mathcal{A}] = 1$ for any algorithm $\mathcal{A}$. ◀

6 Two-Tier Tokenized Signatures

In this section, we will first give the formal definition of two-tier tokenized signatures (2-TS), and then show that they can be constructed from OWFs. For the construction, we use the (amplified) adaptive hardcore bit property for OWFs (Theorem 10).

6.1 Definition

The formal definition is as follows.

▶ **Definition 13** (Two-Tier Tokenized Signatures (2-TS)). *A two-tier tokenized signature scheme is a tuple* $(\mathsf{KeyGen},\mathsf{StateGen},\mathsf{Sign},\mathsf{Ver}_0,\mathsf{Ver}_1)$ *of algorithms such that*

- $\mathsf{KeyGen}(1^\lambda)\to(\mathsf{sk},\mathsf{pk})$: *It is a QPT algorithm that, on input the security parameter λ, outputs a classical secret key* sk *and a classical public key* pk.
- $\mathsf{StateGen}(\mathsf{sk})\to\psi$: *It is a QPT algorithm that, on input* sk*, outputs a quantum state ψ.*
- $\mathsf{Sign}(\psi,m)\to\sigma$: *It is a QPT algorithm that, on input ψ and a message $m\in\{0,1\}$, outputs a classical signature σ.*
- $\mathsf{Ver}_0(\mathsf{pk},\sigma)\to\top/\bot$: *It is a QPT algorithm that, on input* pk *and σ, outputs $\top/\bot$.*
- $\mathsf{Ver}_1(\mathsf{sk},\sigma)\to\top/\bot$: *It is a QPT algorithm that, on input* sk *and σ, outputs $\top/\bot$.*

We require the following properties.

Correctness:

$$\Pr\left[\top\leftarrow\mathsf{Ver}_0(\mathsf{pk},\sigma):\begin{array}{r}(\mathsf{sk},\mathsf{pk})\leftarrow\mathsf{KeyGen}(1^\lambda)\\ \psi\leftarrow\mathsf{StateGen}(\mathsf{sk})\\ \sigma\leftarrow\mathsf{Sign}(\psi,0)\end{array}\right]\geq 1-\mathsf{negl}(\lambda) \tag{24}$$

and

$$\Pr\left[\top\leftarrow\mathsf{Ver}_1(\mathsf{sk},\sigma):\begin{array}{r}(\mathsf{sk},\mathsf{pk})\leftarrow\mathsf{KeyGen}(1^\lambda)\\ \psi\leftarrow\mathsf{StateGen}(\mathsf{sk})\\ \sigma\leftarrow\mathsf{Sign}(\psi,1)\end{array}\right]\geq 1-\mathsf{negl}(\lambda). \tag{25}$$

Security: *For any QPT adversary $\mathcal{A}$,*

$$\Pr\left[\top\leftarrow\mathsf{Ver}_0(\mathsf{pk},\sigma_0)\wedge\top\leftarrow\mathsf{Ver}_1(\mathsf{sk},\sigma_1):\begin{array}{r}(\mathsf{sk},\mathsf{pk})\leftarrow\mathsf{KeyGen}(1^\lambda)\\ \psi\leftarrow\mathsf{StateGen}(\mathsf{sk})\\ (\sigma_0,\sigma_1)\leftarrow\mathcal{A}(\psi,\mathsf{pk})\end{array}\right]\leq\mathsf{negl}(\lambda). \tag{26}$$

We can show that the following type of security, which we call *one-wayness*, is also satisfied by two-tier tokenized signatures.

▶ **Lemma 14** (One-wayness of two-tier tokenized signatures). *For any QPT adversary $\mathcal{A}$,*

$$\Pr\left[\top \leftarrow \mathsf{Ver}_0(\mathsf{pk},\sigma) : \begin{array}{r} (\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda) \\ \psi \leftarrow \mathcal{A}(\mathsf{pk}) \\ \sigma \leftarrow \mathsf{Sign}(\psi, 0) \end{array}\right] \leq \mathsf{negl}(\lambda). \tag{27}$$

Proof. Assume that there exists a QPT adversary $\mathcal{A}$ such that

$$\Pr\left[\top \leftarrow \mathsf{Ver}_0(\mathsf{pk},\sigma) : \begin{array}{r} (\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda) \\ \psi \leftarrow \mathcal{A}(\mathsf{pk}) \\ \sigma \leftarrow \mathsf{Sign}(\psi, 0) \end{array}\right] \geq \frac{1}{\mathrm{poly}(\lambda)} \tag{28}$$

for infinitely many λ. Then, from such $\mathcal{A}$, we can construct a QPT adversary $\mathcal{B}$ that breaks the security of the two-tier tokenized signature scheme as follows:

1. Get ψ and pk as input.
2. Run $\psi' \leftarrow \mathcal{A}(\mathsf{pk})$.
3. Run $\sigma_0 \leftarrow \mathsf{Sign}(\psi', 0)$ and $\sigma_1 \leftarrow \mathsf{Sign}(\psi, 1)$.
4. Output (σ_0, σ_1).

It is clear that $\mathcal{B}$ breaks the security of the two-tier tokenized signature scheme. ◀

6.2 Construction

We show that 2-TS can be constructed from OWFs.

▶ **Theorem 15.** *If OWFs exist, then two-tier tokenized signatures exist.*

Proof. Let f be a OWF. From it, we construct a two-tier tokenized signature scheme as follows:

- $\mathsf{KeyGen}(1^\lambda) \to (\mathsf{sk},\mathsf{pk})$: Choose $x_i^0, x_i^1 \leftarrow \{0,1\}^\ell$ for each $i \in [n]$. Choose $c_i \leftarrow \{0,1\}$ for each $i \in [n]$. Output $\mathsf{sk} := \{c_i, x_i^0, x_i^1\}_{i\in[n]}$ and $\mathsf{pk} := \{f(x_i^0), f(x_i^1)\}_{i\in[n]}$.
- $\mathsf{StateGen}(\mathsf{sk}) \to \psi$: Parse $\mathsf{sk} = \{c_i, x_i^0, x_i^1\}_{i\in[n]}$. Output $\psi := \bigotimes_{i\in[n]} \frac{|x_i^0\rangle + (-1)^{c_i}|x_i^1\rangle}{\sqrt{2}}$.
- $\mathsf{Sign}(\psi, m) \to \sigma$: If $m = 0$, measure ψ in the computational basis to get the result $\{z_i\}_{i\in[n]}$ (where $z_i \in \{0,1\}^\ell$ for each $i \in [n]$), and output it as σ. If $m = 1$, measure ψ in the Hadamard basis to get the result $\{d_i\}_{i\in[n]}$ (where $d_i \in \{0,1\}^\ell$ for each $i \in [n]$), and output it as σ.
- $\mathsf{Ver}_0(\mathsf{pk},\sigma) \to \top/\bot$: Parse $\mathsf{pk} = \{f(x_i^0), f(x_i^1)\}_{i\in[n]}$ and $\sigma = \{z_i\}_{i\in[n]}$. If $f(z_i) \in \{f(x_i^0), f(x_i^1)\}$ for all $i \in [n]$, output $\top$. Otherwise, output $\bot$.
- $\mathsf{Ver}_1(\mathsf{sk},\sigma) \to \top/\bot$: Parse $\mathsf{sk} = \{c_i, x_i^0, x_i^1\}_{i\in[n]}$ and $\sigma = \{d_i\}_{i\in[n]}$. If $d_i \cdot (x_i^0 \oplus x_i^1) = c_i$ for all $i \in [n]$, output $\top$. Otherwise, output $\bot$.

The correctness is clear. The security is also clear from Theorem 10. ◀

7 Digital Signatures with Revocable Signatures

In this section, we define digital signatures with revocable signatures (DSR-Sign). We also show that it can be constructed from 2-TS, and therefore from OWFs.

7.1 Definition

We first give its formal definition as follows.

▶ **Definition 16** (Digital Signatures with Revocable Signatures (DSR-Sign)). *A digital signature scheme with revocable signatures is a set* $(\mathsf{KeyGen},\mathsf{Sign},\mathsf{Ver},\mathsf{Del},\mathsf{Cert})$ *of algorithms that satisfy the following.*

- $\mathsf{KeyGen}(1^\lambda)\to(\mathsf{sigk},\mathsf{vk})$: *It is a QPT algorithm that, on input the security parameter* λ*, outputs a classical signing key* sigk *and a classical public verification key* vk*.*
- $\mathsf{Sign}(\mathsf{sigk},m)\to(\psi,\mathsf{ck})$: *It is a QPT algorithm that, on input a message* m *and* sigk*, outputs a quantum signature* ψ *and a classical check key* ck*.*
- $\mathsf{Ver}(\mathsf{vk},\psi,m)\to\top/\bot$: *It is a QPT algorithm that, on input* vk*,* m*, and* ψ*, outputs* $\top/\bot$*.*
- $\mathsf{Del}(\psi)\to\mathsf{cert}$: *It is a QPT algorithm that, on input* ψ*, outputs a classical certificate* cert*.*
- $\mathsf{Cert}(\mathsf{ck},\mathsf{cert})\to\top/\bot$: *It is a QPT algorithm that, on input* ck *and* cert*, outputs* $\top/\bot$*.*

We require the following properties.

Correctness: *For any message* m*,*

$$\Pr\left[\top\leftarrow\mathsf{Ver}(\mathsf{vk},\psi,m):\begin{array}{r}(\mathsf{sigk},\mathsf{vk})\leftarrow\mathsf{KeyGen}(1^\lambda)\\(\psi,\mathsf{ck})\leftarrow\mathsf{Sign}(\mathsf{sigk},m)\end{array}\right]\geq1-\mathsf{negl}(\lambda).\tag{29}$$

Deletion correctness: *For any message* m*,*

$$\Pr\left[\top\leftarrow\mathsf{Cert}(\mathsf{ck},\mathsf{cert}):\begin{array}{r}(\mathsf{sigk},\mathsf{vk})\leftarrow\mathsf{KeyGen}(1^\lambda)\\(\psi,\mathsf{ck})\leftarrow\mathsf{Sign}(\mathsf{sigk},m)\\\mathsf{cert}\leftarrow\mathsf{Del}(\psi)\end{array}\right]\geq1-\mathsf{negl}(\lambda).\tag{30}$$

Many-time deletion security: *For any adversary* $\mathcal{A}$ *consisting of a pair of QPT algorithms* $(\mathcal{A}_1,\mathcal{A}_2)$*:*

$$\Pr\left[\top\leftarrow\mathsf{Cert}(\mathsf{ck}^*,\mathsf{cert})\wedge\top\leftarrow\mathsf{Ver}(\mathsf{vk},\psi,m^*):\begin{array}{r}(\mathsf{sigk},\mathsf{vk})\leftarrow\mathsf{KeyGen}(1^\lambda)\\(m^*,\mathsf{st})\leftarrow\mathcal{A}_1^{\mathsf{Sign}(\mathsf{sigk},\cdot)}(\mathsf{vk})\\(\psi^*,\mathsf{ck}^*)\leftarrow\mathsf{Sign}(\mathsf{sigk},m^*)\\(\mathsf{cert},\psi)\leftarrow\mathcal{A}_2^{\mathsf{Sign}(\mathsf{sigk},\cdot)}(\mathsf{st},\psi^*)\end{array}\right]\leq\mathsf{negl}(\lambda),\tag{31}$$

where $\mathcal{A}$ *is not allowed to query* m^* *to the signing oracle.*

▶ Remark 17. The above definition does not capture the situation where the adversary gets more than one signatures on m^* but deleted all of them. Actually, our construction seems to also satisfy security in such a setting. However, we choose to not formalize it for simplicity.

▶ Remark 18. We can define the standard EUF-CMA security as follows, but it is trivially implied by many-time deletion security, and therefore we do not include EUF-CMA security in the definition of digital signatures with revocable signatures.

▶ Definition 19 (EUF-CMA Security). *For any QPT adversary* $\mathcal{A}$*,*

$$\Pr\left[\top\leftarrow\mathsf{Ver}(\mathsf{vk},\psi^*,m^*):\begin{array}{r}(\mathsf{sigk},\mathsf{vk})\leftarrow\mathsf{KeyGen}(1^\lambda)\\(m^*,\psi^*)\leftarrow\mathcal{A}^{\mathsf{Sign}(\mathsf{sigk},\cdot)}(\mathsf{vk})\end{array}\right]\leq\mathsf{negl}(\lambda),\tag{32}$$

where $\mathcal{A}$ *is not allowed to query* m^* *to the signing oracle.*

We define a weaker version of many-time deletion security, which we call no-query deletion security as follows.

▶ **Definition 20** (No-Query Deletion Security). *It is the same as many-time deletion security, Equation* (31)*, except that $\mathcal{A}$ cannot query the signing oracle.*

The no-query security notion actually implies the many-time case:

▶ **Lemma 21** (Many-Time Deletion Security from No-Query Deletion Security). *Assume that EUF-CMA secure digital signature schemes exist. Then following holds: if there exists a digital signature scheme with revocable signatures which satisfies no-query deletion security, then there is a scheme that satisfies many-time deletion security.*

Proof. Let $(\mathsf{NQ.KeyGen}, \mathsf{NQ.Sign}, \mathsf{NQ.Ver}, \mathsf{NQ.Del}, \mathsf{NQ.Cert})$ be a digital signature scheme with revocable signatures that satisfies no-query deletion security. Let $(\mathsf{MT.KeyGen}, \mathsf{MT.Sign}, \mathsf{MT.Ver})$ be a plain EUF-CMA secure digital signature scheme. From them, we can construct a digital signature scheme $\Sigma := (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Ver}, \mathsf{Del}, \mathsf{Cert})$ with revocable signatures that satisfies many-time deletion security as follows.

- $\mathsf{KeyGen}(1^\lambda) \to (\mathsf{sigk}, \mathsf{vk})$: Run $(\mathsf{mt.sigk}, \mathsf{mt.vk}) \leftarrow \mathsf{MT.KeyGen}(1^\lambda)$. Output $\mathsf{sigk} := \mathsf{mt.sigk}$ and $\mathsf{vk} := \mathsf{mt.vk}$.
- $\mathsf{Sign}(\mathsf{sigk}, m) \to (\psi, \mathsf{ck})$: Parse $\mathsf{sigk} = \mathsf{mt.sigk}$. Run $(\mathsf{nq.sigk}, \mathsf{nq.vk}) \leftarrow \mathsf{NQ.KeyGen}(1^\lambda)$. Run $(\phi, \mathsf{nq.ck}) \leftarrow \mathsf{NQ.Sign}(\mathsf{nq.sigk}, m)$. Run $\sigma \leftarrow \mathsf{MT.Sign}(\mathsf{mt.sigk}, \mathsf{nq.vk}\|m)$. Output $\psi := (\phi, \sigma, \mathsf{nq.vk})$ and $\mathsf{ck} := \mathsf{nq.ck}$.
- $\mathsf{Ver}(\mathsf{vk}, \psi, m) \to \top/\bot$: Parse $\mathsf{vk} = \mathsf{mt.vk}$ and $\psi = (\phi, \sigma, \mathsf{nq.vk})$. Run $\mathsf{MT.Ver}(\mathsf{mt.vk}, \sigma, \mathsf{nq.vk}\|m)$. If the output is $\bot$, output $\bot$ and abort. Run $\mathsf{NQ.Ver}(\mathsf{nq.vk}, \phi, m)$. If the output is $\top$, output $\top$. Otherwise, output $\bot$.
- $\mathsf{Del}(\psi) \to \mathsf{cert}$: Parse $\psi = (\phi, \sigma, \mathsf{nq.vk})$. Run $\mathsf{cert}' \leftarrow \mathsf{NQ.Del}(\phi)$. Output $\mathsf{cert} := \mathsf{cert}'$.
- $\mathsf{Cert}(\mathsf{ck}, \mathsf{cert}) \to \top/\bot$: Parse $\mathsf{ck} = \mathsf{nq.ck}$. Run $\mathsf{NQ.Cert}(\mathsf{nq.ck}, \mathsf{cert})$, and output its output.

We show that Σ satisfies many-time deletion security. In other words, we show that if the many-time deletion security of Σ is broken, then either the no-query deletion security of the digital signature scheme NQ is broken or the EUF-CMA security of the digital signature scheme MT is broken. Assume that there exists a pair of QPT algorithms $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2)$ such that

$$\Pr\left[\top \leftarrow \mathsf{Cert}(\mathsf{ck}^*, \mathsf{cert}) \wedge \top \leftarrow \mathsf{Ver}(\mathsf{vk}, \psi, m^*) : \begin{array}{r} (\mathsf{sigk}, \mathsf{vk}) \leftarrow \mathsf{KeyGen}(1^\lambda) \\ (m^*, \mathsf{st}) \leftarrow \mathcal{A}_1^{\mathsf{Sign}(\mathsf{sigk}, \cdot)}(\mathsf{vk}) \\ (\psi^*, \mathsf{ck}^*) \leftarrow \mathsf{Sign}(\mathsf{sigk}, m^*) \\ (\mathsf{cert}, \psi) \leftarrow \mathcal{A}_2^{\mathsf{Sign}(\mathsf{sigk}, \cdot)}(\mathsf{st}, \psi^*) \end{array}\right] \geq \frac{1}{\mathrm{poly}(\lambda)} \tag{33}$$

for infinitely many λ, where $\mathcal{A}$ is not allowed to query m^* to the signing oracle. From such $\mathcal{A}$, we construct a QPT adversary $\mathcal{B}$ that breaks the no-query deletion security of the scheme NQ as follows: Let $\mathcal{C}$ be the challenger of the security game of the no-query deletion security.

1. $\mathcal{C}$ runs $(\mathsf{nq.sigk}^*, \mathsf{nq.vk}^*) \leftarrow \mathsf{NQ.KeyGen}(1^\lambda)$.
2. $\mathcal{C}$ sends $\mathsf{nq.vk}^*$ to $\mathcal{B}$.
3. $\mathcal{B}$ runs $(\mathsf{mt.sigk}, \mathsf{mt.vk}) \leftarrow \mathsf{MT.KeyGen}(1^\lambda)$.
4. $\mathcal{B}$ runs $(m^*, \mathsf{st}) \leftarrow \mathcal{A}_1^{\mathsf{Sign}(\mathsf{sigk}, \cdot)}(\mathsf{mt.vk})$. When $\mathcal{A}_1$ queries m to the signing oracle, $\mathcal{B}$ simulates it as follows:
   a. Run $(\mathsf{nq.sigk}, \mathsf{nq.vk}) \leftarrow \mathsf{NQ.KeyGen}(1^\lambda)$.
   b. Run $(\phi, \mathsf{nq.ck}) \leftarrow \mathsf{NQ.Sign}(\mathsf{nq.sigk}, m)$.
   c. Run $\sigma \leftarrow \mathsf{MT.Sign}(\mathsf{mt.sigk}, \mathsf{nq.vk}\|m)$.
   d. Output $\psi := (\phi, \sigma, \mathsf{nq.vk})$ and $\mathsf{ck} := \mathsf{nq.ck}$.
5. $\mathcal{B}$ sends m^* to $\mathcal{C}$.
6. $\mathcal{C}$ runs $(\phi^*, \mathsf{nq.ck}^*) \leftarrow \mathsf{NQ.Sign}(\mathsf{nq.sigk}^*, m^*)$, and sends ϕ^* to $\mathcal{B}$.

7. $\mathcal{B}$ runs $\sigma^* \leftarrow \mathsf{MT.Sign}(\mathsf{mt.sigk}, \mathsf{nq.vk}^* \| m^*)$.
8. $\mathcal{B}$ runs $(\mathsf{cert}, \psi) \leftarrow \mathcal{A}_2^{\mathsf{Sign}(\mathsf{sigk},\cdot)}((\phi^*, \sigma^*, \mathsf{nq.vk}^*))$. When $\mathcal{A}_2$ queries m to the signing oracle, $\mathcal{B}$ simulates it as follows:
   a. Run $(\mathsf{nq.sigk}, \mathsf{nq.vk}) \leftarrow \mathsf{NQ.KeyGen}(1^\lambda)$.
   b. Run $(\phi, \mathsf{nq.ck}) \leftarrow \mathsf{NQ.Sign}(\mathsf{nq.sigk}, m)$.
   c. Run $\sigma \leftarrow \mathsf{MT.Sign}(\mathsf{mt.sigk}, \mathsf{nq.vk} \| m)$.
   d. Output $\psi := (\phi, \sigma, \mathsf{nq.vk})$ and $\mathsf{ck} := \mathsf{nq.ck}$.
9. Parse $\psi = (\phi, \sigma, \eta)$. $\mathcal{B}$ outputs cert and ϕ.

Due to the EUF-CMA security of the scheme MT, $\top \leftarrow \mathsf{MT.Ver}(\mathsf{mt.vk}, \sigma, \eta \| m^*)$ occurs only when $\eta = \mathsf{nq.vk}^*$ except for a negligible probability. Therefore, Equation (33) means that both $\Pr[\top \leftarrow \mathsf{NQ.Ver}(\mathsf{nq.vk}^*, \phi, m^*)]$ and $\Pr[\top \leftarrow \mathsf{NQ.Cert}(\mathsf{nq.ck}^*, \mathsf{cert})]$ are non-negligible for the above $\mathcal{B}$, which breaks the no-query deletion security of the scheme NQ. ◀

7.2 Construction

Here we show the following result.

▶ **Theorem 22.** *If two-tier tokenized signatures exist, then digital signatures with revocable signatures that satisfy no-query deletion security exist.*

From Lemma 21, it also means the following:

▶ **Corollary 23.** *Digital signatures with revocable signatures (that satisfy many-time deletion security) exist if two-tier tokenized signatures and EUF-CMA secure digital signatures exist.*

Proof of Theorem 22. Here, we construct the scheme for the single-bit message space. It is clear that this can be extended to any fixed multi-bit message space case by the parallel execution of the protocol. Moreover, by using universal one-way hash functions, it can be extended to unbounded poly-length message space case [34].

Let $(\mathsf{TS.KeyGen}, \mathsf{TS.StateGen}, \mathsf{TS.Sign}, \mathsf{TS.Ver}_0, \mathsf{TS.Ver}_1)$ be a two-tier tokenized signature scheme. From it, we construct a digital signature scheme with revocable signatures $\Sigma := (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Ver}, \mathsf{Del}, \mathsf{Cert})$ that satisfies no-query deletion security for the single bit message space as follows.

- $\mathsf{KeyGen}(1^\lambda) \to (\mathsf{sigk}, \mathsf{vk})$: Run $(\mathsf{sk}_0, \mathsf{pk}_0) \leftarrow \mathsf{TS.KeyGen}(1^\lambda)$. Run $(\mathsf{sk}_1, \mathsf{pk}_1) \leftarrow \mathsf{TS.KeyGen}(1^\lambda)$. Output $\mathsf{sigk} := (\mathsf{sk}_0, \mathsf{sk}_1)$ and $\mathsf{vk} := (\mathsf{pk}_0, \mathsf{pk}_1)$.
- $\mathsf{Sign}(\mathsf{sigk}, m) \to (\psi, \mathsf{ck})$: Parse $\mathsf{sigk} = (\mathsf{sk}_0, \mathsf{sk}_1)$. Run $\psi' \leftarrow \mathsf{TS.StateGen}(\mathsf{sk}_m)$. Output $\psi := \psi'$ and $\mathsf{ck} := \mathsf{sk}_m$.
- $\mathsf{Ver}(\mathsf{vk}, \psi, m) \to \top/\bot$: Parse $\mathsf{vk} := (\mathsf{pk}_0, \mathsf{pk}_1)$. Run $\sigma \leftarrow \mathsf{TS.Sign}(\psi, 0)$. Run $\mathsf{TS.Ver}_0(\mathsf{pk}_m, \sigma)$, and output its output.[15]
- $\mathsf{Del}(\psi) \to \mathsf{cert}$: Run $\sigma \leftarrow \mathsf{TS.Sign}(\psi, 1)$, and output $\mathsf{cert} := \sigma$.
- $\mathsf{Cert}(\mathsf{ck}, \mathsf{cert}) \to \top/\bot$: Parse $\mathsf{ck} = \mathsf{sk}_m$. Run $\mathsf{TS.Ver}_1(\mathsf{sk}_m, \mathsf{cert})$, and output its output.

Correctness and the deletion correctness are clear. Let us show the no-query deletion security. Assume that there is a pair of QPT algorithms $(\mathcal{A}_1, \mathcal{A}_2)$ such that

$$\Pr\left[\top \leftarrow \mathsf{Cert}(\mathsf{ck}^*, \mathsf{cert}) \wedge \top \leftarrow \mathsf{Ver}(\mathsf{vk}, \psi, m^*) : \begin{array}{r} (\mathsf{sigk}, \mathsf{vk}) \leftarrow \mathsf{KeyGen}(1^\lambda) \\ (m^*, \mathsf{st}) \leftarrow \mathcal{A}_1(\mathsf{vk}) \\ (\psi^*, \mathsf{ck}^*) \leftarrow \mathsf{Sign}(\mathsf{sigk}, m^*) \\ (\mathsf{cert}, \psi) \leftarrow \mathcal{A}_2(\mathsf{st}, \psi^*) \end{array}\right] \geq \frac{1}{\mathrm{poly}(\lambda)} \quad (34)$$

[15] The verification algorithm destroys the signature, but it can be done in a non-destructive way by coherently applying this procedure and then doing the uncomputation.

for infinitely many λ. From $\mathcal{A}$, we can construct a QPT adversary $\mathcal{B}$ that breaks the original two-tier tokenized signature scheme as follows:

1. Get ψ^* and pk as input.
2. Run $(\mathsf{sk}', \mathsf{pk}') \leftarrow \mathsf{TS.KeyGen}(1^\lambda)$. Choose $r \leftarrow \{0,1\}$. If $r = 0$, set $\mathsf{vk} := (\mathsf{pk}, \mathsf{pk}')$. If $r = 1$, set $\mathsf{vk} := (\mathsf{pk}', \mathsf{pk})$.
3. Run $(m^*, \mathsf{st}) \leftarrow \mathcal{A}_1(\mathsf{vk})$. If $r \neq m^*$, output $\perp$ and abort.
4. Run $(\mathsf{cert}, \psi) \leftarrow \mathcal{A}_2(\mathsf{st}, \psi^*)$.
5. Run $\sigma_0 \leftarrow \mathsf{TS.Sign}(\psi, 0)$. Define $\sigma_1 := \mathsf{cert}$.
6. Output (σ_0, σ_1).

It is clear that $\Pr[\mathcal{B}$ breaks the two-tier tokenized signature scheme$] \geq \frac{1}{2}\Pr[\mathcal{A}$ breaks $\Sigma]$. Therefore, from Equation (34), $\mathcal{B}$ breaks the two-tier tokenized signature scheme. ◀

References

1 Scott Aaronson. 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*, pages 229–242. IEEE Computer Society, 2009. doi:10.1109/CCC.2009.42.

2 Scott Aaronson, Jiahui Liu, Qipeng Liu, Mark Zhandry, and Ruizhe Zhang. New approaches for quantum copy-protection. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021, Part I*, volume 12825 of *Lecture Notes in Computer Science*, pages 526–555, Virtual Event, August 16–20 2021. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-84242-0_19.

3 Shweta Agrawal, Fuyuki Kitagawa, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa. Public key encryption with secure key leasing. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023, Part I*, volume 14004 of *Lecture Notes in Computer Science*, pages 581–610, Lyon, France, April 23–27 2023. Springer, Heidelberg, Germany. doi:10.1007/978-3-031-30545-0_20.

4 Ryan Amos, Marios Georgiou, Aggelos Kiayias, and Mark Zhandry. One-shot signatures and applications to hybrid quantum/classical authentication. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *52nd Annual ACM Symposium on Theory of Computing*, pages 255–268, Chicago, IL, USA, June 22–26 2020. ACM Press. doi:10.1145/3357713.3384304.

5 Prabhanjan Ananth and Rolando L. La Placa. Secure software leasing. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021, Part II*, volume 12697 of *Lecture Notes in Computer Science*, pages 501–530, Zagreb, Croatia, October 17–21 2021. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-77886-6_17.

6 Prabhanjan Ananth, Alexander Poremba, and Vinod Vaikuntanathan. Revocable cryptography from learning with errors. In Guy Rothblum and Hoeteck Wee, editors, *Theory of Cryptography*, pages 93–122, Cham, 2023. Springer Nature Switzerland.

7 James Bartusek, Sanjam Garg, Vipul Goyal, Dakshita Khurana, Giulio Malavolta, Justin Raizes, and Bhaskar Roberts. Obfuscation and outsourced computation with certified deletion. Cryptology ePrint Archive, Paper 2023/265, 2023. URL: https://eprint.iacr.org/2023/265.

8 James Bartusek and Dakshita Khurana. Cryptography with certified deletion. Cryptology ePrint Archive, Paper 2022/1178, 2022. URL: https://eprint.iacr.org/2022/1178.

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

10 James Bartusek, Dakshita Khurana, Giulio Malavolta, Alexander Poremba, and Michael Walter. Weakening assumptions for publicly-verifiable deletion. In *Theory of Cryptography: 21st International Conference, TCC 2023, Taipei, Taiwan, November 29–December 2, 2023, Proceedings, Part IV*, pages 183–197, Berlin, Heidelberg, 2023. Springer-Verlag. doi:10.1007/978-3-031-48624-1_7.

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

12 Shalev Ben-David and Or Sattath. Quantum tokens for digital signatures. *Quantum*, 2023.

13 Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. *Journal of the ACM*, 68(5):31:1–31:47, 2021.

14 Anne Broadbent and Rabib Islam. Quantum encryption with certified deletion. In Rafael Pass and Krzysztof Pietrzak, editors, *TCC 2020: 18th Theory of Cryptography Conference, Part III*, volume 12552 of *Lecture Notes in Computer Science*, pages 92–122, Durham, NC, USA, November 16–19 2020. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-64381-2_4.

15 Anne Broadbent and Sébastien Lord. Uncloneable quantum encryption via oracles. In Steven T. Flammia, editor, *15th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2020, June 9-12, 2020, Riga, Latvia*, volume 158 of *LIPIcs*, pages 4:1–4:22. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020. doi:10.4230/LIPIcs.TQC.2020.4.

16 Orestis Chardouvelis, Vipul Goyal, Aayush Jain, and Jiahui Liu. Quantum key leasing for pke and fhe with a classical lessor. Cryptology ePrint Archive, Paper 2023/1640, 2023. URL: https://eprint.iacr.org/2023/1640.

17 Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021, Part I*, volume 12825 of *Lecture Notes in Computer Science*, pages 556–584, Virtual Event, August 16–20 2021. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-84242-0_20.

18 Andrea Coladangelo, Christian Majenz, and Alexander Poremba. Quantum copy-protection of compute-and-compare programs in the quantum random oracle model. Cryptology ePrint Archive, Paper 2020/1194, 2020. URL: https://eprint.iacr.org/2020/1194.

19 Marios Georgiou and Mark Zhandry. Unclonable decryption keys. Cryptology ePrint Archive, Paper 2020/877, 2020. URL: https://eprint.iacr.org/2020/877.

20 Daniel Gottesman. Unclonable encryption, 2002. arXiv:0210062.

21 Carl W. Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1:231–252, 1969.

22 Taiga Hiroka, Fuyuki Kitagawa, Tomoyuki Morimae, Ryo Nishimaki, Tapas Pal, and Takashi Yamakawa. Certified everlasting secure collusion-resistant functional encryption, and more. Cryptology ePrint Archive, Paper 2023/236, 2023. URL: https://eprint.iacr.org/2023/236.

23 Taiga Hiroka, Tomoyuki Morimae, Ryo Nishimaki, and Takashi Yamakawa. Quantum encryption with certified deletion, revisited: Public key, attribute-based, and classical communication. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2021, Part I*, volume 13090 of *Lecture Notes in Computer Science*, pages 606–636, Singapore, December 6–10 2021. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-92062-3_21.

24 Taiga Hiroka, Tomoyuki Morimae, Ryo Nishimaki, and Takashi Yamakawa. Certified everlasting zero-knowledge proof for QMA. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022, Part I*, volume 13507 of *Lecture Notes in Computer Science*, pages 239–268, Santa Barbara, CA, USA, August 15–18 2022. Springer, Heidelberg, Germany. doi:10.1007/978-3-031-15802-5_9.

25 A.S Holevo. Statistical decision theory for quantum systems. *Journal of Multivariate Analysis*, 3(4):337–394, 1973. doi:10.1016/0047-259X(73)90028-6.

26 Zhengfeng Ji, Youming Qiao, Fang Song, and Aaram Yun. General linear group action on tensors: A candidate for post-quantum cryptography. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019: 17th Theory of Cryptography Conference, Part I*, volume 11891 of *Lecture Notes in Computer Science*, pages 251–281, Nuremberg, Germany, December 1–5 2019. Springer, Heidelberg, Germany. `doi:10.1007/978-3-030-36030-6_11`.

27 Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC Press, 2007. URL: `http://www.cs.umd.edu/~jkatz/imc.html`.

28 Fuyuki Kitagawa and Ryo Nishimaki. Functional encryption with secure key leasing. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology – ASIACRYPT 2022, Part IV*, volume 13794 of *Lecture Notes in Computer Science*, pages 569–598, Taipei, Taiwan, December 5–9 2022. Springer, Heidelberg, Germany. `doi:10.1007/978-3-031-22972-5_20`.

29 Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Secure software leasing from standard assumptions. In Kobbi Nissim and Brent Waters, editors, *TCC 2021: 19th Theory of Cryptography Conference, Part I*, volume 13042 of *Lecture Notes in Computer Science*, pages 31–61, Raleigh, NC, USA, November 8–11 2021. Springer, Heidelberg, Germany. `doi:10.1007/978-3-030-90459-3_2`.

30 Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Publicly verifiable deletion from minimal assumptions. Cryptology ePrint Archive, Paper 2023/538, 2023. URL: `https://eprint.iacr.org/2023/538`.

31 Jiahui Liu, Qipeng Liu, Luowen Qian, and Mark Zhandry. Collusion resistant copy-protection for watermarkable functionalities. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022: 20th Theory of Cryptography Conference, Part I*, volume 13747 of *Lecture Notes in Computer Science*, pages 294–323, Chicago, IL, USA, November 7–10 2022. Springer, Heidelberg, Germany. `doi:10.1007/978-3-031-22318-1_11`.

32 Ralph C. Merkle. A digital signature based on a conventional encryption function. In Carl Pomerance, editor, *Advances in Cryptology – CRYPTO'87*, volume 293 of *Lecture Notes in Computer Science*, pages 369–378, Santa Barbara, CA, USA, August 16–20 1988. Springer, Heidelberg, Germany. `doi:10.1007/3-540-48184-2_32`.

33 Tomoyuki Morimae and Takashi Yamakawa. Classically verifiable NIZK for QMA with preprocessing. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology – ASIACRYPT 2022, Part IV*, volume 13794 of *Lecture Notes in Computer Science*, pages 599–627, Taipei, Taiwan, December 5–9 2022. Springer, Heidelberg, Germany. `doi:10.1007/978-3-031-22972-5_21`.

34 Moni Naor and Moti Yung. Universal one-way hash functions and their cryptographic applications. In *21st Annual ACM Symposium on Theory of Computing*, pages 33–43, Seattle, WA, USA, May 15–17 1989. ACM Press. `doi:10.1145/73007.73011`.

35 Alexander Poremba. Quantum proofs of deletion for learning with errors. Cryptology ePrint Archive, Paper 2022/295, 2022. URL: `https://eprint.iacr.org/2022/295`.

36 Alexander Poremba. Quantum Proofs of Deletion for Learning with Errors. In Yael Tauman Kalai, editor, *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*, volume 251 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 90:1–90:14, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. `doi:10.4230/LIPIcs.ITCS.2023.90`.

37 Roy Radian and Or Sattath. Semi-quantum money. *arXiv/1908.08889*, 2019. `arXiv:1908.08889`.

38 Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC*, pages 84–93. ACM Press, 2005.

39 Ronald L. Rivest. Can we eliminate certificate revocation lists? In Rafael Hirschfeld, editor, *Proceedings Financial Cryptography '98*, volume 1465 of *Lecture Notes in Computer Science*, pages 178–183. Springer, 1998. `doi:10.1007/BFb0055482`.

40 Omri Shmueli. Semi-quantum tokenized signatures. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022, Part I*, volume 13507 of *Lecture Notes in Computer Science*, pages 296–319, Santa Barbara, CA, USA, August 15–18 2022. Springer, Heidelberg, Germany. doi:10.1007/978-3-031-15802-5_11.

41 S. Stubblebine. Recent-secure authentication: enforcing revocation in distributed systems. In *2012 IEEE Symposium on Security and Privacy*, page 0224, Los Alamitos, CA, USA, May 1995. IEEE Computer Society.

42 Dominique Unruh. Revocable quantum timed-release encryption. *J. ACM*, 62(6):49:1–49:76, 2015.

43 Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.

44 Mark Zhandry. Quantum lightning never strikes the same state twice. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 408–438, Darmstadt, Germany, May 19–23 2019. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-17659-4_14.