A Concrete Treatment of Fiat-Shamir Signatures in the Quantum Random-Oracle Model

Eike Kiltz[1(✉)], Vadim Lyubashevsky[2], and Christian Schaffner[3]

[1] Ruhr Universität Bochum, Bochum, Germany
eike.kiltz@rub.de
[2] IBM Research – Zurich, Zurich, Switzerland
vad@zurich.ibm.com
[3] QuSoft and ILLC, University of Amsterdam, Amsterdam, The Netherlands
c.schaffner@uva.nl
http://www.qusoft.org/

Abstract. The Fiat-Shamir transform is a technique for combining a hash function and an identification scheme to produce a digital signature scheme. The resulting scheme is known to be secure in the random oracle model (ROM), which does not, however, imply security in the scenario where the adversary also has quantum access to the oracle. The goal of this current paper is to create a generic framework for constructing tight reductions in the QROM from underlying hard problems to Fiat-Shamir signatures.

Our generic reduction is composed of two results whose proofs, we believe, are simple and natural. We first consider a security notion (UF-NMA) in which the adversary obtains the public key and attempts to create a valid signature without accessing a signing oracle. We give a tight reduction showing that deterministic signatures (i.e., ones in which the randomness is derived from the message and the secret key) that are UF-NMA secure are also secure under the standard chosen message attack (UF-CMA) security definition. Our second result is showing that if the identification scheme is "lossy", as defined in (Abdalla et al. Eurocrypt 2012), then the security of the UF-NMA scheme is tightly based on the hardness of distinguishing regular and lossy public keys of the identification scheme. This latter distinguishing problem is normally exactly the definition of some presumably-hard mathematical problem. The combination of these components gives our main result.

As a concrete instantiation of our framework, we modify the recent lattice-based Dilithium digital signature scheme (Ducas et al., TCHES 2018) so that its underlying identification scheme admits lossy public keys. The original Dilithium scheme, which is proven secure in the classical ROM based on standard lattice assumptions, has 1.5 KB public keys and 2.7 KB signatures. The new scheme, which is tightly based on the hardness of the Module-LWE problem in the QROM using our generic reductions, has 7.7 KB public keys and 5.7 KB signatures for the same security level. Furthermore, due to our proof of equivalence between the UF-NMA and UF-CMA security notions of deterministic signature schemes, we can formu-

J. B. Nielsen and V. Rijmen (Eds.): EUROCRYPT 2018, LNCS 10822, pp. 552–586, 2018.
https://doi.org/10.1007/978-3-319-78372-7_18

late a new non-interactive assumption under which the original Dilithium signature scheme is also tightly secure in the QROM.

1 Introduction

Fiat-Shamir Signatures from Identification Protocols. A canonical identification scheme [2] is a three-move authentication protocol ID of a specific form. The prover (holding the secret-key) sends a commitment W to the verifier. The verifier (holding the public-key) returns a random challenge c. The prover sends a response Z. Finally, using the verification algorithm, the verifier accepts if the transcript (W, c, Z) is correct. The Fiat-Shamir transformation [2,20] combines a canonical identification scheme ID and a hash function H to obtain a digital signature scheme $\mathsf{FS} = \mathsf{FS}[\mathsf{ID}, \mathsf{H}]$. The signing algorithm first iteratively generates a transcript (W, c, Z), where the challenge c is derived via $c := \mathsf{H}(W \parallel M)$. Signature $\sigma = (W, Z)$ is valid if the transcript $(W, c := \mathsf{H}(W \parallel M), Z)$ makes the verification algorithm accept. Lyubashevsky [26] further generalized this to the "Fiat-Shamir with aborts" transformation to account for aborting provers.

Security of Fiat-Shamir Signatures in the ROM. Security of $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$ in the ROM can be proved in two steps. Firstly, if the underlying identification scheme has statistical Honest-Verifier Zero-Knowledge (HVZK), then UnForgeability against Chosen Message Attack (UF-CMA) and UnForgeability against No Message Attack (UF-NMA) are tightly equivalent (UF-NMA security means that the adversary is not allowed to make any signing queries). Secondly, the Forking Lemma [9,34] (based on a technique called "rewinding") is used to prove UF-NMA security in the random-oracle model (ROM) [11] from computational Special Soundness (SS). The latter part of the security reduction is non-tight and the loss in tightness is known to be inherent (e.g., [24,32]).

Lossy Identification schemes. With the goal of constructing signature schemes with a tight security reduction and generalizing a signature scheme by Katz and Wang [22], AFLT [3] introduced the new concept of lossy identification schemes and proved that Fiat-Shamir transformed signatures have a tight security reduction in the ROM. A lossy identification scheme comes with an additional lossy key generator that produces a lossy public key, computationally indistinguishable from a honestly generated public key. Further, relative to

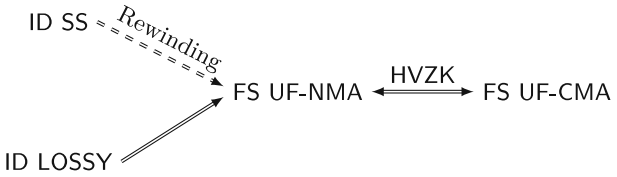

Fig. 1. Known security results of Fiat-Shamir signatures $\mathsf{FS} = \mathsf{FS}[\mathsf{ID}, \mathsf{H}]$ in the ROM. Solid arrows denote tight reductions, dashed arrows non-tight reductions.

a lossy public key the identification scheme has *statistical soundness*, i.e., not even an unbounded adversary can successfully impersonate a prover. Figure 1 summarizes the known security results of Fiat-Shamir signatures in the ROM.

Quantum Random-Oracle Model. Recently, NIST announced a competition with the goal to standardize new asymmetric encryption and signature schemes [1] with security against quantum adversaries, i.e., adversaries equipped with a quantum computer. There exists a number of (sometimes only implicitly defined) canonical identification schemes (e.g., [3,5,7,16,23,26]) whose security relies on the hardness of certain problems over lattices and codes, which are generally believed to resist quantum adversaries. Quantum computers may execute all "offline primitives" such as the hash function on arbitrary superpositions, which motivated the introduction of the quantum (accessible) random-oracle model (QROM) [13]. That is, in the UF-CMA security experiment for signatures in the QROM, an adversary has quantum access to a perfect hash function H and classical access to the signing oracle. Aiding in the construction of UF-CMA secure signatures with provable (post-quantum) security in the QROM is the main motivation of this paper.

Security of Fiat-Shamir signatures in the QROM. A number of recent works considered the security of Fiat-Shamir transformed signatures in the QROM. [13] proved a general result showing that if a reduction in the classical ROM is *history-free*, then it can also be carried out in the QROM. History-free reductions basically determine random oracle answers independently of the history of previous queries. For reductions that are not history-free, adaptive re-programming of the quantum random oracle is required which is problematic in the QROM: with one single quantum query to all inputs in superposition, an adversary might learn a superposition of all possible random oracle values which essentially means the reduction has to provide plausible values for the whole random oracle at this point. Hence, adaptive reprogramming in the QROM is difficult (but not impossible e.g., [12,18,36]).

Unfortunately, the known random-oracle proofs of Fiat-Shamir signatures [3,24,34] are not history-free. Beyond the general problem of adaptive re-programming, the classical proof [34] uses rewinding and the Forking Lemma, a technique that we currently do not know how to extend to the quantum setting. Even worse, Ambanis et al. [6] proved that Fiat-Shamir signatures cannot be proven secure in a black-box way by just assuming computational special soundness and HVZK (these two conditions are, on the other hand, sufficient for a proof in the classical ROM).

To circumvent the above negative result, Unruh [36] proposed an alternative Fiat-Shamir transformation with provable QROM security but the resulting signatures are considerably less efficient as they require multiple executions of the underlying identification scheme.

Alkim et al. [5] gave a concrete tight security reduction for a signature scheme, TESLA, in the QROM. TESLA is a concrete lattice-based digital signature scheme implicitly derived via the Fiat-Shamir transformation. Their QROM

proof from the learning with errors (LWE) assumption adaptively re-programs the quantum random oracle using a technique from [12] and seems tailored to their particular identification protocol. As described in [5], the intuition behind the QROM security proof for TESLA comes from the fact that the underlying identification scheme is lossy. They leave it as an open problem to prove Fiat-Shamir signatures generically secure from lossy identification schemes.

Unruh [37] could prove (among other things) that identification schemes with HVZK and statistical soundness yield UF-CMA secure Fiat-Shamir signatures in the QROM when additionally assuming a "dual-mode hard instance generator" for generating key pairs of the identification scheme. The latter dual mode hard instance generator is very similar to lossy identification schemes. Whereas the original publication [37] only contains asymptotic proofs, a recently updated version of the full version [38] also provides concrete security bounds. Below, in Sect. 1.2, we will compare them with our bounds.

1.1 Our Results

This work contains a simple and modular security analysis in the QROM of signatures $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$ obtained via the Fiat-Shamir transform with aborts [26] from any lossy identification scheme ID. We also consider the security of a deterministic variant $\mathsf{DFS}[\mathsf{ID}, \mathsf{H}, \mathsf{PRF}]$ with better tightness. DFS derives the randomness for signing deterministically using a pseudo-random function PRF. Our main security statements are summarized in Fig. 2. Most importantly, if ID is a lossy identification scheme and has HVZK, then $\mathsf{DFS}[\mathsf{ID}, \mathsf{H}, \mathsf{PRF}]$ is tightly UF-CMA secure and $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$ is (non-tightly) UF-CMA secure in the QROM. Our results suggest to prefer $\mathsf{DFS}[\mathsf{ID}, \mathsf{H}, \mathsf{PRF}]$ over $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$.

The main component of our proof is a tweak to the AFLT Fiat-Shamir proof [3] that makes it history-free. Together with the general result of [13], one can immediately obtain *asymptotic* (i.e., non-concrete) versions of our QROM proof as a simple corollary. In this work, we instead give direct proofs with concrete, tight security bounds.

To demonstrate the efficacy of our generic framework, we construct a lattice-based signature scheme. The most compact lattice-based schemes, in terms of public key and signature sizes, crucially require sampling from a discrete Gaussian distribution [15,17]. Such schemes, however, have been shown to be particularly vulnerable to side-channel attacks (c.f. [14,19]), and it therefore seems prudent to consider schemes that only require simple uniform sampling over the integers. Of those, the most currently efficient one is the Dilithium signature scheme [16]. This signature scheme is proved secure based on the MSIS (Module-SIS) and the MLWE (Module-LWE) assumptions in the ROM implicitly using the framework from Fig. 1.

In this paper, we provide a practical instantiation of a lossy identification scheme to obtain a new digital signature scheme, Dilithium-QROM, with a tight security reduction in the QROM from the MLWE problem, derived using our new framework from Fig. 2. Dilithium-QROM is essentially a less compact variant ($\approx$3X larger) of Dilithium with modified parameters to allow the underlying

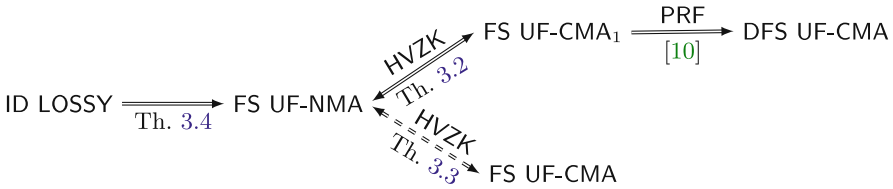

Fig. 2. Security of standard Fiat-Shamir signatures $\mathsf{FS} = \mathsf{FS}[\mathsf{ID}, \mathsf{H}]$ and deterministic Fiat-Shamir signatures $\mathsf{DFS} = \mathsf{DFS}[\mathsf{ID}, \mathsf{H}, \mathsf{PRF}]$ in the QROM. Solid arrows denote tight reductions, dashed arrows non-tight reductions. The considered security notions are: UF-CMA (unforgeability against chosen-message attack), $\mathsf{UF\text{-}CMA}_1$ (unforgeability against one-query-per-message chosen-message attack), and UF-NMA (unforgeability against no-message attack).

identification scheme to admit a lossy mode. We additionally prove the security of the original Dilithium scheme in the QROM based on MLWE and another non-interactive assumption.

Security of Fiat-Shamir Signatures. Security of deterministic Fiat-Shamir signatures $\mathsf{DFS}[\mathsf{ID}, \mathsf{H}, \mathsf{PRF}]$ in the QROM is proved in two independent steps, see Fig. 2.

Step 1: $\mathsf{LOSSY} \Longrightarrow \mathsf{UF\text{-}NMA}$. We sketch an adaptation of the standard history-free proof implicitly contained in [3]. By the security properties of the lossy identification scheme, the public key can be set in lossy mode which remains unnoticed by a computationally bounded quantum adversary. Further, breaking the signature scheme in lossy mode with at most Q_{H} queries to the quantum random oracle essentially requires to solve the generic quantum search problem, whose complexity is $\Theta(Q_{\mathsf{H}}^2 \cdot \varepsilon_{\mathsf{ls}})$ [21,39], where $\varepsilon_{\mathsf{ls}}$ is the statistical soundness parameter of ID in lossy mode. A similar argument is implicitly contained in [5,37].

Step 2: $\mathsf{UF\text{-}NMA} \Longrightarrow \mathsf{UF\text{-}CMA}$. We will now sketch a history-free proof of $\mathsf{UF\text{-}NMA} \Rightarrow \mathsf{UF\text{-}CMA}_1$, where (compared to UF-CMA security) $\mathsf{UF\text{-}CMA}_1$ security limits the number of queried signatures per message M to one. We then apply a standard (history-free, tight) reduction to show that $\mathsf{UF\text{-}CMA}_1$ secure signatures de-randomized with a PRF yield UF-CMA secure signatures with deterministic signing [10].

The standard ROM proof of $\mathsf{UF\text{-}NMA} \Rightarrow \mathsf{UF\text{-}CMA}$ (implicitly contained in [3]) works as follows: one uses the HVZK property of ID to show that the signing oracle can be efficiently simulated only knowing the public-key. Concretely, the HVZK simulator generates a transcript (W, c, Z) and later "patches" the random oracle by defining $\mathsf{H}(W \parallel M) := c$ to make (W, Z) a valid signature. The problem is that the random oracle patching (i.e., defining $\mathsf{H}(W \parallel M) := c$) can only be done *after* the signing query on M because only then W and c are known. This renders the AFLT standard reduction non history-free. In our

history-free UF-NMA $\Rightarrow$ UF-CMA$_1$ proof, we resolve this problem as follows. We use the HVZK property to generate the transcript (W_M, c_M, Z_M) *deterministically* using message-dependent randomness. Hence, for each message M, the transcript (W_M, c_M, Z_M) is unique and can be computed at any time. This uniqueness allows us to patch the random oracle $\mathsf{H}(W \parallel M)$ to c_M at any time of the proof (i.e., iff $W = W_M$), even before the adversary has established a signing query on message M. This trick makes the proof history-free, see Theorem 3.2. Clearly, this only works if the adversary receives at most one signature for each messages M, which is guaranteed by the UF-CMA$_1$ experiment.

In order to deal with (full) UF-CMA security of probabilistic Fiat-Shamir signatures $\mathsf{FS}[\mathsf{ID}, \mathsf{H}]$, the above trick can be adapted to also obtain a history-free reduction, see Theorem 3.3. However, the proof is less tight as the reduction suffers from a quadratic blow-up in its running time.

Our results furthermore prove *strong* unforgeability if the identification scheme satisfies an additional property called computational unique response (CUR). CUR essentially says that it is hard to come up with two accepting transcripts with the same commitment and challenge but different responses.

Dilithium-QROM*: A signature scheme with provable security in the QROM.* The digital signature scheme Dilithium [16] is constructed from a canonical identification scheme using the Fiat-Shamir with aborts approach [26]. In the ROM, its security is based (via non-tight reductions) on the hardness of the MSIS and MLWE problems. We show that by increasing the size of the modulus and the dimension of the public key matrix, the resulting identification scheme admits a lossy mode such that distinguishing real from lossy keys is based on the hardness of MLWE. We can then apply our main reduction to conclude that the resulting digital signature scheme is based on the hardness of the MLWE problem.

In order to construct an identification scheme with a lossy mode, in addition to increasing the size of the modulus and the overall dimension, we also choose our prime modulus q so that the underlying ring $\mathbb{Z}_q[X]/(X^n+1)$ has the property that all elements with coefficients less than $\sqrt{q/2}$ have an inverse [29] – having all small elements be invertible is crucial to having lossiness.[1] For the same security levels as Dilithium, the total size of the public key and signature is increased by a factor of a little over 3.

Revisiting the Security of Dilithium. Due to the way the parameters are set, the underlying identification scheme of the original Dilithium scheme does not have a lossy mode, and so we cannot apply Theorem 3.4 in the reduction sequence in Fig. 2. Nevertheless, the reduction from Theorem 3.2 is still applicable. In the classical ROM, one then obtains a reduction from MSIS to the UF-NMA scheme via the forking lemma (see Fig. 1).

The main downside of this last step is that the reduction is inherently non-tight. In practice, however, parameters are set based on the hardness of the underlying MSIS problem and the non-tightness of the reduction is ignored.

[1] There do not exist q for which $\mathbb{Z}_q[X]/(X^n + 1)$ is a field.

This is not just the case in lattice-based schemes, but is the prevalent practice for every signature scheme built via the Fiat-Shamir transform. The implicit assumption is, therefore, that the UF-NMA scheme is *exactly* as secure as MSIS (assuming that H is secure). We point out that the assumption that the UF-NMA scheme is secure is a non-interactive assumption that is reasonably simple to state, and so the fact that several decades of cryptanalysis haven't produced any improved attacks against schemes whose parameters ignore the non-tightness of the reduction, gives us confidence that equating the hardness of the UF-NMA scheme with the hardness of the underlying problem is very reasonable.

In Sect. 4.5, we formulate the security of the UF-NMA scheme as a "convolution" of a lattice/hash function problem, which we call SelfTargetMSIS, and then show that based on the hardness of MLWE and SelfTargetMSIS, the deterministic version of the Dilithium scheme is (tightly) UF-CMA secure in the QROM. In other words, we show that the security of the *tight* version of the signature scheme is based on exactly the same assumptions in the ROM and the QROM.

Other Instantiations. Our framework can be applied to obtain a security proof in the QROM for a number of existing Fiat-Shamir signature schemes that are similar to Dilithium (e.g., [3,5,7,26]) and those that have a somewhat different structure and possibly based on different assumptions (e.g., [23]). Our rationale for setting the parameters in Dilithium-QROM was to minimize the total sum of the public key and the signature. If one, on the other hand, wished to only minimize the signature size, one could create a public key whose "height" is larger than its "width" (e.g., as in [5]). For optimal efficiency, this may possibly require working over polynomial rings $\mathbb{Z}_q[X]/(f(x))$ which are finite fields.

1.2 Concrete Bounds and Comparison with Unruh [37,38]

Ignoring all constants and the computational term accounting for the pseudorandom function, our concrete bound for the UF-CMA security of deterministic Fiat-Shamir signatures DFS in the QROM is

$$\mathrm{Adv}^{\mathsf{UF\text{-}CMA}}_{\mathsf{DFS}}(\mathsf{A}) \le \mathrm{Adv}^{\mathsf{LOSS}}_{\mathsf{ID}}(\mathsf{B}) + Q_{\mathsf{H}}^2 \cdot \varepsilon_{\mathsf{ls}} + Q_S \cdot \varepsilon_{\mathsf{zk}} + 2^{-\alpha}, \quad \mathrm{Time}(\mathsf{B}) \approx \mathrm{Time}(\mathsf{A}) \tag{1}$$

where $\mathrm{Adv}^{\mathsf{LOSS}}_{\mathsf{ID}}(\mathsf{B})$ is the lossyness advantage of ID, $\varepsilon_{\mathsf{ls}}$ is the statistical soundness parameter of ID in lossy mode, α is the min-entropy of ID's commitments, and $\varepsilon_{\mathsf{zk}}$ is the HVZK parameter of ID.

From Unruh [38] one can derive the following concrete bound which even holds for (standard) probabilistic Fiat-Shamir signatures FS.

$$\begin{aligned} \mathrm{Adv}^{\mathsf{UF\text{-}CMA}}_{\mathsf{FS}}(\mathsf{A}) &\le \mathrm{Adv}^{\mathsf{LOSS}}_{\mathsf{ID}}(\mathsf{B}) + Q_{\mathsf{H}}^2 \cdot \varepsilon_{\mathsf{ls}} + Q_S \cdot \varepsilon_{\mathsf{zk}} + Q_S Q_H^{1/2} \cdot 2^{-\alpha/4}, \\ \mathrm{Time}(\mathsf{B}) &\approx \mathrm{Time}(\mathsf{A}) + Q_{\mathsf{H}} Q_S. \end{aligned} \tag{2}$$

Compared to (1), bound (2) has two sources of non-tightness.

The first source of non-tightness in (2) is the term $Q_S Q_H^{1/2} \cdot 2^{-\alpha/4}$ which stems from a generic re-programming technique from [36]. In most practical lattice-based schemes the commitment's min-entropy α is large enough not to make a big

impact on the worse bounds. However, this term puts a lower bound on the min-entropy of commitments which translates to an unnatural lower bound on the size of quantum-resistant Fiat-Shamir signatures. Furthermore, it is sometimes not that easy to exactly compute the min-entropy α. Further, simple techniques to get a "good-enough" bound (as we did for regular Dilithium when we obtained $\alpha = 255$) would no longer result in something meaningful when used with (2).

The second and more important sources of non-tightness in (2) is the quadratic (in the number of queries) blow-up in the running time $\mathrm{Time}(\mathsf{B}) \approx \mathrm{Time}(\mathsf{A}) + Q_{\mathsf{H}} Q_S$ which renders the reduction non-tight in all practical aspects. Interestingly, our proof for the security of *probabilistic* Fiat-Shamir signatures (Theorem 3.3) introduces the same source of non-tightness. However, under the assumption that superposition queries to classical data can be performed in a single time step (denoted by QRAM in [38]), the running time in (2) drops to $\mathrm{Time}(\mathsf{B}) \approx \mathrm{Time}(\mathsf{A})$ and hence the reduction is tight again. We leave it as an open problem to come up with a tight reduction for probabilistic Fiat-Shamir signatures in the QROM without using QRAM.

2 Preliminaries

For $n \in \mathbb{N}$, let $[n] := \{1, \ldots, n\}$. For a set S, $|S|$ denotes the cardinality of S. For a finite set S, we denote the sampling of a uniform random element x by $x \leftarrow S$, while we denote the sampling according to some distribution $\mathfrak{D}$ by $x \leftarrow \mathfrak{D}$. By $[\![B]\!]$ we denote the bit that is 1 if the Boolean Statement B is true, and 0 otherwise.

Algorithms. Let A be an algorithm. Unless stated otherwise, we assume all our algorithms to be probabilistic. We denote by $y \leftarrow \mathsf{A}(x)$ the probabilistic computation of algorithm A on input x. If A is deterministic, we write $y := \mathsf{A}(x)$. The notation $y \in \mathsf{A}(x)$ is used to indicate all possible outcomes y of the probabilistic algorithm A on input x. We can make any probabilistic A deterministic by running it with fixed randomness. We write $y := \mathsf{A}(x; r)$ to indicate that A is run on input x with randomness r. Finally, the notation $\mathsf{A}(x) \Rightarrow y$ denotes the event that A on input x returns y.

Games. We use code-based games. We implicitly assume boolean flags to be initialized to false, numerical types to 0, sets to $\varnothing$, and strings to the empty string ϵ. We make the convention that a procedure terminates once it has returned an output.

2.1 Quantum Computation

Quantum States. The state of a qubit $|\phi\rangle$ is described by a two-dimensional complex vector $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ where $\{|0\rangle, |1\rangle\}$ form an orthonormal basis of $\mathbb{C}^2$ and $\alpha, \beta \in \mathbb{C}$ with $|\alpha|^2 + |\beta|^2 = 1$ are called the complex *amplitudes* of $|\phi\rangle$. The qbit $|\phi\rangle$ is said to be *in superposition* if $0 < |\alpha| < 1$. A classical bit $b \in \{0, 1\}$ is naturally encoded as state $|b\rangle$ of a qubit.

The state $|\psi\rangle$ of n qubits can be expressed as $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x|x\rangle \in \mathbb{C}^{2^n}$ where $\{\alpha_x\}_{x\in\{0,1\}^n}$ is a set of 2^n complex amplitudes such that $\sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1$. As for one qubit, the standard orthonormal or *computational basis* is given by $\{|x\rangle\}_{x\in\{0,1\}^n}$. When the quantum state $|\psi\rangle$ is *measured* in the computational basis, the outcome is the classical string $x \in \{0,1\}^n$ with probability $|\alpha_x|^2$ and the quantum state collapses to what is observed, namely $|x\rangle$.

The evolution of a quantum system in state $|\psi\rangle$ can be described by a linear length-preserving transformation $U : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$. Such transformations correspond to *unitary* matrices U of size 2^n by 2^n, i.e. U has the property that $UU^\dagger = \mathbb{1}$, where $U^\dagger$ is the complex-conjugate transpose of U.

For further details about basic concepts and notation of quantum computing, we refer to the standard text book by Nielsen and Chuang [31].

Quantum oracles and quantum adversaries. For a classical oracle function $\mathrm{O} : \{0,1\}^n \to \{0,1\}^m$, we follow the standard approach as in [8,13] to make the execution of the classical function O a reversible unitary transformation. We model quantum access to O by

$$U_\mathrm{O} : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus \mathrm{O}(x)\rangle,$$

where $x \in \{0,1\}^n$ and $y \in \{0,1\}^m$. Note that due to the XOR function in the second register, U_O is its own inverse, i.e. executing U_O twice results in the identity for any function O.[2] Quantum oracle adversaries $\mathsf{A}^{|\mathrm{O}\rangle}$ can access O in superposition by applying U_O. The quantum time it takes to apply U_O is linear in the time it takes to evaluate O classically. We write $\mathsf{A}^{|\mathrm{O}\rangle}$ to indicate that an oracle is quantum-accessible, contrary to oracles which can only be accessed classically which are denoted by A^{O}. We also abuse notation and use $|O\rangle$ to denote the oracle that is quantumly accessible.

Quantum random-oracle model. We consider security games in the quantum random-oracle model (QROM) [13] like their counterparts in the classical random-oracle model [11], with the difference that we consider quantum adversaries that are given **quantum** access to the random oracles involved, and **classical** access to all other oracles (e.g., the signing oracle). Zhandry [40] proved that no quantum algorithm $\mathsf{A}^{|\mathsf{H}\rangle}$, issuing at most Q quantum queries to $|\mathsf{H}\rangle$, can distinguish between a random function $\mathsf{H} : \{0,1\}^m \to \{0,1\}^n$ and a $2Q$-wise independent function f_{2Q}. For concreteness, we view $f_{2Q} : \{0,1\}^m \to \{0,1\}^n$ as a random polynomial of degree $2Q$ over the finite field $\mathbb{F}_{2^n}$. The running time to evaluate f_{2Q} is linear in Q.

In this article, we will use this observation in the context of security reductions, where quantum adversary B simulates quantum adversary $\mathsf{A}^{|\mathsf{H}\rangle}$ which

[2] Together with the observation that taking the conjugate-complex and transposing U_O do not change U_O, we obtain $U_\mathrm{O}^\dagger = U_\mathrm{O}$, and hence, $U_\mathrm{O}U_\mathrm{O}^\dagger = U_\mathrm{O}^2 = \mathbb{1}$, showing that U_O is indeed a unitary transformation.

GAME GSPB_λ
01 $(\lambda(x))_{x\in X} \leftarrow \mathsf{A}_1$
02 If $\exists x \in X$ s.t. $\lambda(x) > \lambda$ then **return** 0
03 For all $x \in X$: $g(x) \leftarrow \mathcal{B}_{\lambda(x)}$
04 $x \leftarrow \mathsf{A}_2^{|g\rangle}$
05 **return** $g(x)$

Fig. 3. The generic search game GSPB_λ with bounded maximal Bernoulli parameter $\lambda \in [0,1]$.

makes at most Q queries to $|\mathsf{H}\rangle$. Hence, the running time of B is $\mathrm{Time}(\mathsf{B}) = \mathrm{Time}(\mathsf{A}) + q \cdot \mathrm{Time}(\mathsf{H})$, where $\mathrm{Time}(\mathsf{H})$ is the time it takes to simulate $|\mathsf{H}\rangle$. Using the observation above, B can use a $2Q$-wise independent function in order to (information-theoretically) simulate $|\mathsf{H}\rangle$ and we obtain that the running time of B is $\mathrm{Time}(\mathsf{B}) = \mathrm{Time}(\mathsf{A}) + Q \cdot \mathrm{Time}(f_{2Q})$, and the time $\mathrm{Time}(f_{2Q})$ to evaluate f_{2Q} is linear in Q. The second term of this running time (quadratic in Q) can be further reduced to linear in Q in the quantum random-oracle model where B can simply use another random oracle to simulate $|\mathsf{H}\rangle$. Assuming evaluating the random oracle takes one time unit, we write $\mathrm{Time}(\mathsf{B}) = \mathrm{Time}(\mathsf{A}) + Q$ which is approximately $\mathrm{Time}(\mathsf{A})$.

Generic Quantum Search. For $\lambda \in [0,1]$ let $\mathcal{B}_\lambda$ be the Bernoulli distribution, i.e., $\Pr[b = 1] = \lambda$ for the bit $b \leftarrow \mathcal{B}_\lambda$. Let X be some finite set. The generic quantum search problem GSP [21,39] is to find an $x \in X$ satisfying $g(x) = 1$ given quantum access to an oracle $g : X \to \{0,1\}$, such that for each $x \in X$, $g(x)$ is distributed according to $\mathcal{B}_\lambda$. We will need the following slight variation of GSP. The Generic quantum Search Problem with Bounded probabilities GSPB is like the quantum search problem with the difference that the Bernoulli parameter $\lambda(x)$ may (adversarially) depend on x but it is upper bounded by a global λ.

Lemma 2.1. *(Generic Search Problem with Bounded Probabilities). Let $\lambda \in [0,1]$. For any (unbounded, quantum) algorithm A issuing at most Q quantum queries to $|g\rangle$, $\Pr[\mathsf{GSPB}_\lambda^{\mathsf{A}} \Rightarrow 1] \leq 8 \cdot \lambda \cdot (Q+1)^2$, where Game GSPB_λ is defined in Fig. 3.*

The bound on GSPB can be reduced to the known bound on GSP [21,39] by artificially increasing the Bernoulli parameter to obtain the dependence on each $x \in X$.

2.2 Pseudorandom Functions

A pseudorandom function PRF is a mapping $\mathsf{PRF} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^k$, where $\mathcal{K}$ is a finite key space and n, k are integers. To a quantum adversary A and PRF we associate the advantage function

$$\mathrm{Adv}^{\mathsf{PR}}_{\mathsf{PRF}}(\mathsf{A}) := \left| \Pr[\mathsf{A}^{\mathsf{PRF}(K,\cdot)} \Rightarrow 1 \mid K \leftarrow \mathcal{K}] - \Pr[\mathsf{A}^{\mathsf{RF}(\cdot)} \Rightarrow 1] \right|,$$

where $\mathsf{RF} : \{0,1\}^n \to \{0,1\}^k$ is a perfect random function. We note that while adversary A is quantum, it only gets classical access to the oracles $\mathsf{PRF}(K,\cdot)$ and $\mathsf{RF}(\cdot)$.

2.3 Canonical Identification Schemes

A canonical identification scheme ID is a three-move protocol of the form depicted in Fig. 4. The prover's first message W is called *commitment*, the verifier selects a uniform *challenge* c from set ChSet, and, upon receiving a *response* Z from the prover, makes a deterministic decision.

Definition 2.2 (Canonical Identification Scheme). *A canonical identification scheme* ID *is defined as a tuple of algorithms* $\mathsf{ID} := (\mathsf{IGen}, \mathsf{P}, \mathsf{ChSet}, \mathsf{V})$.

- *The key generation algorithm* IGen *takes system parameters* par *as input and returns public and secret key* (pk, sk). *We assume that* pk *defines* ChSet *(the set of challenges),* WSet *(the set of commitments), and* ZSet *(the set of responses).*
- *The prover algorithm* $\mathsf{P} = (\mathsf{P}_1, \mathsf{P}_2)$ *is split into two algorithms.* P_1 *takes as input the secret key* sk *and returns a commitment* $W \in \mathsf{WSet}$ *and a state* St*;* P_2 *takes as input the secret key* sk*, a commitment* W*, a challenge* c*, and a state* St *and returns a response* $Z \in \mathsf{ZSet} \cup \{\perp\}$*, where* $\perp \notin \mathsf{ZSet}$ *is a special symbol indicating failure.*
- *The verifier algorithm* V *takes the public key* pk *and the conversation transcript as input and outputs a* deterministic decision*, 1 (acceptance) or 0 (rejection).*

We make a couple of useful definitions. A *transcript* is a three-tuple $(W, c, Z) \in \mathsf{WSet} \times \mathsf{ChSet} \times \mathsf{ZSet} \cup \{\perp, \perp, \perp\}$. It is called *valid* (with respect to public-key pk) if $\mathsf{V}(pk, W, c, Z) = 1$. In Fig. 5 we also define a transcript oracle Trans that returns a real interaction (W, c, Z) between prover and verifier as depicted in Fig. 4, with the important convention that the transcript is defined as $(\perp, \perp, \perp)$ if $Z = \perp$.

Definition 2.3 (Correctness Error). *Identification scheme* ID *has correctness error* δ *if for all* $(pk, sk) \in \mathsf{IGen}(\mathsf{par})$ *the following holds:*

- *All possible transcripts* (W, c, Z) *satisfying* $Z \neq \perp$ *are valid, i.e., for all* $(W, St) \in \mathsf{P}_1(sk)$*, all* $c \in \mathsf{ChSet}$ *and all* $Z \in \mathsf{P}_2(sk, W, c, St)$ *with* $Z \neq \perp$*, we have* $\mathsf{V}(pk, W, c, Z) = 1$.

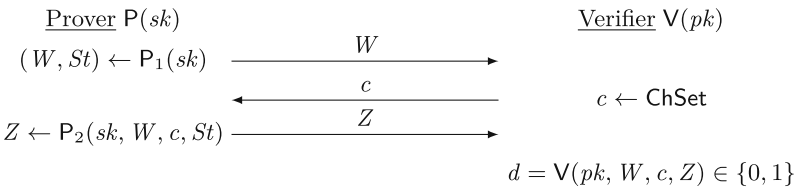

Fig. 4. A canonical identification scheme and its transcript (W, c, Z).

Algorithm $\mathsf{Trans}(sk)$:
01 $(W, St) \leftarrow \mathsf{P}_1(sk)$
02 $c \leftarrow \mathsf{ChSet}$
03 $Z \leftarrow \mathsf{P}_2(sk, W, c, St)$
04 **if** $Z = \perp$ then return $(\perp, \perp, \perp)$
05 **return** (W, c, Z)

Fig. 5. An honestly generated transcript (W, c, Z) output by the transcript oracle $\mathsf{Trans}(sk)$.

– *The probability that an honestly generated transcript* (W, c, Z) *contains* $Z = \perp$ *is bounded by* δ*, i.e.,* $\Pr[Z = \perp \mid (W, c, Z) \leftarrow \mathsf{Trans}(sk)] \leq \delta$.

Definition 2.4. *We call* ID commitment-recoverable*, if for any* $(pk, sk) \in \mathsf{IGen}(\mathsf{par})$*,* $c \in \mathsf{ChSet}$*, and* $Z \in \mathsf{ZSet}$*, there exists a unique* $W \in \mathsf{WSet}$ *such that* $\mathsf{V}(pk, W, c, Z) = 1$*. This unique* W *can be publicly computed using a commitment recovery algorithm as* $W := \mathsf{Rec}(pk, c, Z)$.

We define no-abort honest-verifier zero-knowledge, a weak variant of honest-verifier zero-knowledge that requires the transcript (as generated by $\mathsf{Trans}(sk)$) to be publicly simulatable, conditioned on $Z \neq \perp$.

Definition 2.5 (No-Abort Honest-verifier Zero-knowledge). *A canonical identification scheme* ID *is said to be* $\varepsilon_{\mathsf{zk}}$*-perfect* naHVZK *(no-abort honest-verifier zero-knowledge) if there exists an algorithm* Sim *that, given only the public key* pk*, outputs* (W, c, Z) *such that the following conditions hold:*

– *The distribution of* $(W, c, Z) \leftarrow \mathsf{Sim}(pk)$ *has statistical distance at most* $\varepsilon_{\mathsf{zk}}$ *from* $(W', c', Z') \leftarrow \mathsf{Trans}(sk)$*, where* Trans *is defined in Fig. 5.*
– *The distribution of* c *from* $(W, c, Z) \leftarrow \mathsf{Sim}(pk)$ *conditioned on* $c \neq \perp$ *is uniform random in* ChSet.

Note that if ID is commitment-recoverable, then we can abandon the W in the output of Trans and Sim since W can be publicly computed from (c, Z).

Definition 2.6 (Min-Entropy). *If the most likely value of a random variable* W *that is chosen from a discrete distribution* D *occurs with probability* $2^{-\alpha}$*, then we say that min-entropy*$(W \mid W \leftarrow D) = \alpha$*. We will say that a canonical identification scheme* ID *has* α bits of min-entropy*, if*

$$\Pr_{(pk,sk)\leftarrow\mathsf{IGen}(\mathsf{par})}[\textit{min-entropy}(W \mid (W, St) \leftarrow \mathsf{P}_1(sk)) \geq \alpha] \geq 1 - 2^{-\alpha}.$$

In other words, except with probability $2^{-\alpha}$ *over the choice of* (pk, sk)*, the min-entropy of* W *will be at least* α.

An identification scheme has unique responses if for all W and c there exists at most one Z to make the verifier accept, i.e., $\mathsf{V}(pk, W, c, Z) = 1$. We relax this property to computational unique response (CUR) for which we require it to be computationally difficult to come up with (W, c, Z, Z') with $\mathsf{V}(pk, W, c, Z) = \mathsf{V}(pk, W, c, Z') = 1$ and $Z' \neq Z$.

Definition 2.7 (Computational Unique Response). *To an adversary* A *we associate the advantage function*

$$\mathrm{Adv}^{\mathsf{CUR}}_{\mathsf{ID}}(\mathsf{A}) := \Pr\left[\begin{array}{l|l} \mathsf{V}(pk,W,c,Z)=1 & (pk,sk)\leftarrow \mathsf{IGen}(\mathsf{par});\\ \mathsf{V}(pk,W,c,Z')=1 \wedge Z\neq Z' & (W,c,Z,Z')\leftarrow \mathsf{A}(pk)\end{array}\right].$$

Lossy Identification schemes. We now recall lossy identification schemes [3].

Definition 2.8. *An identification scheme* $\mathsf{ID}=(\mathsf{IGen},\mathsf{P},\mathsf{ChSet},\mathsf{V})$ *is lossy if there exists a lossy key generation algorithm* $\mathsf{LossyIGen}$ *that takes system parameters* par *as input and returns public key* pk_{ls} *(and no secret key* sk*).*

We refer to $\mathsf{LID}=(\mathsf{IGen},\mathsf{LossyIGen},\mathsf{P},\mathsf{ChSet},\mathsf{V})$ as a lossy identification scheme.

We now define two security properties of a lossy identification scheme LID. The first property says that public keys generated with the real key generator IGen are indistinguishable from ones generated by the lossy key generator $\mathsf{LossyIGen}$. Concretely, we define the LOSS *advantage function of a quantum adversary* A *against* ID as

$$\begin{aligned}\mathrm{Adv}^{\mathsf{LOSS}}_{\mathsf{LID}}(\mathsf{A}) := \big|&\Pr[\mathsf{A}(pk_{\mathsf{ls}})\Rightarrow 1 \mid pk_{\mathsf{ls}}\leftarrow \mathsf{LossyIGen}(\mathsf{par})]\\ &-\Pr[\mathsf{A}(pk)\Rightarrow 1 \mid (pk,sk)\leftarrow \mathsf{IGen}(\mathsf{par})]\big|.\end{aligned}$$

The second security property is statistical and says that relative to a lossy key pk_{ls}, not even an unbounded quantum adversary can impersonate the prover. We say that ID has $\varepsilon_{\mathsf{ls}}$-lossy soundness if for every (possibly unbounded, quantum) adversary C, $\Pr[\mathsf{LOSSY\text{-}IMP}^{\mathsf{C}}\Rightarrow 1]\leq\varepsilon_{\mathsf{ls}}$, where game $\mathsf{LOSSY\text{-}IMP}$ is defined in Fig. 6.

Since C is unbounded, we can upper bound $\Pr[\mathsf{LOSSY\text{-}IMP}^{\mathsf{C}}\Rightarrow 1]$ as

$$\begin{aligned}&\Pr[\mathsf{LOSSY\text{-}IMP}^{\mathsf{C}}\Rightarrow 1]\\ &\quad\leq \mathbf{E}\left[\max_{W\in\mathsf{WSet}}\left(\Pr_{c\leftarrow\mathsf{ChSet}}[\exists Z\in\mathsf{ZSet}:\mathsf{V}(pk_{\mathsf{ls}},W,c,Z)=1]\right)\right],\end{aligned}\tag{3}$$

where the expectation is taken over $pk_{\mathsf{ls}}\leftarrow\mathsf{LossyIGen}(\mathsf{par})$. Note that equality in Eq. (3) is achieved for the "optimal" adversary C which on the "easiest" commitment $W\in\mathsf{WSet}$ and a random challenge $c\leftarrow\mathsf{ChSet}$ finds a response $Z\in\mathsf{ZSet}$ that the verifier accepts.

GAME LOSSY-IMP:
01 $pk_{\mathsf{ls}}\leftarrow\mathsf{LossyIGen}(\mathsf{par})$
02 $(W^*,St)\leftarrow\mathsf{C}(pk_{\mathsf{ls}})$
03 $c^*\leftarrow\mathsf{ChSet}$
04 $Z^*\leftarrow\mathsf{C}(St,c^*)$
05 **return** $[\![\mathsf{V}(pk_{\mathsf{ls}},W^*,c^*,Z^*)]\!]$

Fig. 6. The lossy impersonation game $\mathsf{LOSSY\text{-}IMP}$.

2.4 Digital Signatures

We now define syntax and security of a digital signature scheme. Let par be common system parameters shared among all participants.

Definition 2.9 (Digital Signature). *A digital signature scheme* SIG *is defined as a triple of algorithms* $\mathsf{SIG} = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$.

- *The key generation algorithm* $\mathsf{Gen}(\mathsf{par})$ *returns the public and secret keys* (pk, sk). *We assume that* pk *defines the message space* MSet.
- *The signing algorithm* $\mathsf{Sign}(sk, M)$ *returns a signature* σ.
- *The deterministic verification algorithm* $\mathsf{Ver}(pk, M, \sigma)$ *returns 1 (accept) or 0 (reject).*

Signature scheme SIG has correctness error γ if for all $(pk, sk) \in \mathsf{Gen}(\mathsf{par})$, all messages $M \in \mathsf{MSet}$, we have $\Pr[\mathsf{Ver}(pk, M, \mathsf{Sign}(sk, M)) = 0] \leq \gamma$.

Security. We define the $\mathsf{UF\text{-}CMA}$ (unforgeability against chosen-message attack), $\mathsf{UF\text{-}CMA}_1$ (unforgeability against one-per-message chosen-message attack), and $\mathsf{UF\text{-}NMA}$ (unforgeability against no-message attack) advantage functions of a quantum adversary A against SIG as $\mathrm{Adv}^{\mathsf{UF\text{-}CMA}}_{\mathsf{SIG}}(\mathsf{A}) := \Pr[\mathsf{UF\text{-}CMA}^{\mathsf{A}} \Rightarrow 1]$, $\mathrm{Adv}^{\mathsf{UF\text{-}CMA}_1}_{\mathsf{SIG}}(\mathsf{A}) := \Pr[\mathsf{UF\text{-}CMA}_1{}^{\mathsf{A}} \Rightarrow 1]$, and $\mathrm{Adv}^{\mathsf{UF\text{-}NMA}}_{\mathsf{SIG}}(\mathsf{A}) := \Pr[\mathsf{UF\text{-}NMA}^{\mathsf{A}} \Rightarrow 1]$, where the games $\mathsf{UF\text{-}CMA}$, $\mathsf{UF\text{-}CMA}_1$, and $\mathsf{UF\text{-}NMA}$ are given in Fig. 7. We also consider *strong* unforgeability where the adversary may return a forgery on a message previously queried to the signing oracle, but with a different signature. In the corresponding experiments $\mathsf{sUF\text{-}CMA}$ and $\mathsf{sUF\text{-}CMA}_1$, the set $\mathcal{M}$ contains tuples (M, σ) and for the winning condition it is checked that $(M^*, \sigma^*) \notin \mathcal{M}$.

Any $\mathsf{UF\text{-}CMA}_1$ ($\mathsf{sUF\text{-}CMA}_1$) secure signature scheme can be combined with a pseudo-random function PRF to obtain an $\mathsf{UF\text{-}CMA}$ ($\mathsf{sUF\text{-}CMA}$) secure signature scheme by defining $\mathsf{Sign}'((sk, K), M) := \mathsf{Sign}(sk, M; \mathsf{PRF}_K(M))$, where K is a secret PRF key which is part of the secret key. This construction is well known in the classical setting [10], and the same proof works in the quantum setting. Here PRF only has to provide security against quantum adversaries where the access to PRF is classical.

GAMES UF-CMA/UF-CMA$_1$/UF-NMA:

01 $(pk, sk) \leftarrow \mathsf{Gen}(\mathsf{par})$
02 $(M^*, \sigma^*) \leftarrow \mathsf{A}^{\textsc{Sign}}(pk)$ // UF-CMA
03 $(M^*, \sigma^*) \leftarrow \mathsf{A}^{\textsc{Sign}_1}(pk)$ // UF-CMA$_1$
04 $(M^*, \sigma^*) \leftarrow \mathsf{A}(pk)$ // UF-NMA
05 **return** $[\![M^* \notin \mathcal{M}]\!] \wedge \mathsf{Ver}(pk, M^*, \sigma^*)$

Sign(M)
06 $\mathcal{M} = \mathcal{M} \cup \{M\}$
07 $\sigma \leftarrow \mathsf{Sign}(sk, M)$
08 **return** σ

Sign$_1(M)$
09 **if** $M \in \mathcal{M}$ then return $\perp$
10 $\mathcal{M} = \mathcal{M} \cup \{M\}$
11 $\sigma \leftarrow \mathsf{Sign}(sk, M)$
12 **return** σ

Fig. 7. Games $\mathsf{UF\text{-}CMA}$, $\mathsf{UF\text{-}CMA}_1$, and $\mathsf{UF\text{-}NMA}$.

3 Fiat-Shamir in the Quantum Random-Oracle Model

3.1 Signatures from Identification Schemes

Let $\mathsf{ID} := (\mathsf{IGen}, \mathsf{P}, \mathsf{ChSet}, \mathsf{V})$ be a canonical identification scheme, let κ_m be a positive integer, and let $\mathsf{H} : \{0,1\}^* \to \mathsf{ChSet}$ be a hash function. The following signature scheme $\mathsf{SIG} := (\mathsf{Gen} = \mathsf{IGen}, \mathsf{Sign}, \mathsf{Ver})$ is obtained by the Fiat-Shamir transformation with aborts $\mathsf{FS}[\mathsf{ID}, \mathsf{H}, \kappa_m]$ [26].

$\underline{\mathsf{Sign}(sk, M)}$	$\underline{\mathsf{Ver}(pk, M, \sigma)}$
01 $\kappa := 0$	09 Parse $\sigma = (W, Z) \in \mathsf{WSet} \times \mathsf{ZSet}$
02 **while** $Z = \bot$ and $\kappa \le \kappa_m$ do	10 $c = \mathsf{H}(W \parallel M)$
03 $\quad \kappa := \kappa + 1$	11 **return** $\mathsf{V}(pk, W, c, Z) \in \{0,1\}$
04 $\quad (W, St) \leftarrow \mathsf{P}_1(sk)$	
05 $\quad c = H(W \parallel M)$	
06 $\quad Z \leftarrow \mathsf{P}_2(sk, W, c, St)$	
07 **if** $Z = \bot$ **return** $\sigma = \bot$	
08 **return** $\sigma = (W, Z)$	

We make the convention that if $\sigma = (W, Z)$ is not in $\mathsf{WSet} \times \mathsf{ZSet}$, then $\mathsf{Ver}(pk, M, \sigma)$ returns 0 (reject). Clearly, if ID has correctness error δ, then SIG has correctness error $\gamma = \delta^{\kappa_m}$.

Fiat-Shamir for Commitment-Recoverable Identification. For commitment-recoverable ID (see Definition 2.4), we can define an alternative Fiat-Shamir transformation $\mathsf{SIG}' = \mathsf{FS}'[\mathsf{ID}, \mathsf{H}, \kappa_m] := (\mathsf{Gen} = \mathsf{IGen}, \mathsf{Sign}', \mathsf{Ver}')$. Algorithm $\mathsf{Sign}'(sk, M)$ is defined as $\mathsf{Sign}(sk, M)$ with the modified output $\sigma' = (c, Z)$. Algorithm $\mathsf{Ver}'(pk, M, \sigma')$ first parses $\sigma' = (c, Z)$, then recomputes the commitment as $W' := \mathsf{Rec}(pk, c, Z)$, and finally returns 1 iff $\mathsf{H}(W' \parallel M) = c$.

$\underline{\mathsf{Sign}'(sk, M)}$	$\underline{\mathsf{Ver}'(pk, M, \sigma')}$
01 $\kappa := 0$	09 Parse $\sigma' = (c, Z) \in \mathsf{ChSet} \times \mathsf{ZSet}$
02 **while** $Z = \bot$ and $\kappa \le \kappa_m$ do	10 $W' := \mathsf{Rec}(pk, c, Z)$
03 $\quad \kappa := \kappa + 1$	11 **return** $[\![\mathsf{H}(W' \parallel M) = c]\!]$
04 $\quad (W, St) \leftarrow \mathsf{P}_1(sk)$	
05 $\quad c = \mathsf{H}(W \parallel M)$	
06 $\quad Z \leftarrow \mathsf{P}_2(sk, W, c, St)$	
07 **if** $Z = \bot$ **return** $\sigma' = \bot$	
08 **return** $\sigma' = (c, Z)$	

Since $\sigma = (W, Z)$ can be publicly transformed into $\sigma' = (c, Z)$ and vice versa, SIG and SIG' are equivalent in terms of security. The alternative Fiat-Shamir transform yields shorter signatures if $c \in \mathsf{ChSet}$ has a smaller representation size than the commitment $W \in \mathsf{WSet}$.

Main Security Statement. The following is our main security statement for $\mathsf{SIG} := \mathsf{FS}[\mathsf{ID}, \mathsf{H}, \kappa_m]$ in the QROM.

Theorem 3.1. *Assume the identification scheme* ID *is lossy,* $\varepsilon_{\mathsf{zk}}$*-perfect* naHVZK*, has* α *bits of min entropy, and is* $\varepsilon_{\mathsf{ls}}$*-lossy sound. For any quantum adversary* A *against* $\mathsf{UF\text{-}CMA}_1$ *(*$\mathsf{sUF\text{-}CMA}_1$*) security that issues at most* Q_{H} *queries to the quantum random oracle* $|\mathsf{H}\rangle$ *and* Q_S *classical queries to the signing oracle* $\textsc{Sign}_1$*, there exists a quantum adversary* B *(and a quantum adversary* C *against* CUR*)such that*

$$\begin{aligned}\mathrm{Adv}^{\mathsf{UF\text{-}CMA}_1}_{\mathsf{SIG}}(\mathsf{A}) &\le \mathrm{Adv}^{\mathsf{LOSS}}_{\mathsf{ID}}(\mathsf{B}) + 8(Q_{\mathsf{H}}+1)^2\cdot\varepsilon_{\mathsf{ls}} + \kappa_m Q_S\cdot\varepsilon_{\mathsf{zk}} + 2^{-\alpha+1},\\ \mathrm{Adv}^{\mathsf{sUF\text{-}CMA}_1}_{\mathsf{SIG}}(\mathsf{A}) &\le \mathrm{Adv}^{\mathsf{LOSS}}_{\mathsf{ID}}(\mathsf{B}) + 8(Q_{\mathsf{H}}+1)^2\cdot\varepsilon_{\mathsf{ls}} + \kappa_m Q_S\cdot\varepsilon_{\mathsf{zk}} + 2^{-\alpha+1}\\ &\quad + \mathrm{Adv}^{\mathsf{CUR}}_{\mathsf{ID}}(\mathsf{C}),\end{aligned}$$

and $\mathrm{Time}(\mathsf{B}) = \mathrm{Time}(\mathsf{C}) = \mathrm{Time}(\mathsf{A}) + \kappa_m Q_{\mathsf{H}} \approx \mathrm{Time}(\mathsf{A})$.

Note that with this observation the bound of Theorem 3.1 is tight, i.e., the computational advantages appear with a constant factor (one). In the classical ROM setting, the only difference is that the bound depends linearly on Q_{H}, instead of quadratic.

Deterministic Fiat-Shamir. Let PRF be a pseudo-random function. Consider a deterministic variant $\mathsf{DSIG} := \mathsf{DFS}[\mathsf{ID}, \mathsf{H}, \mathsf{PRF}, \kappa_m] = (\mathsf{Gen}, \mathsf{DSign}, \mathsf{Ver})$ of FS where lines 04 and 06 of Sign is derandomized using the PRF, where the random key K is part of the secret key.

$\underline{\mathsf{DSign}((sk, K), M)}$
01 $\kappa := 0$
02 **while** $Z = \perp$ and $\kappa \le \kappa_m$ do
03 $\quad\kappa := \kappa + 1$
04 $\quad(W, St) := \mathsf{P}_1(sk; \mathsf{PRF}_K(0 \parallel m \parallel \kappa))$
05 $\quad c = \mathsf{H}(W \parallel M)$
06 $\quad Z := \mathsf{P}_2(sk, W, c, St; \mathsf{PRF}_K(1 \parallel m \parallel \kappa))$
07 **if** $Z = \perp$ **return** $\sigma = \perp$
08 **return** $\sigma = (W, Z)$

As discussed at the end of Sect. 2.4, the $\mathsf{UF\text{-}CMA}$ ($\mathsf{sUF\text{-}CMA}$) security of DSIG is implied by the $\mathsf{UF\text{-}CMA}_1$ ($\mathsf{sUF\text{-}CMA}_1$) security of FS. Concretely the advantages are upper bounded by the same terms as in Theorem 3.1 plus an additional term $\mathrm{Adv}^{\mathsf{PR}}_{\mathsf{PRF}}(\mathsf{D})$ accounting for the quantum security of the PRF.

3.2 Security Proof

The proof of Theorem 3.1 is modular. First, in Theorem 3.2 we prove that $\mathsf{UF\text{-}NMA}$ security plus naHVZK implies $\mathsf{UF\text{-}CMA}_1$ security. Second, in Theorem 3.4 we prove that a lossy identification scheme is always $\mathsf{UF\text{-}NMA}$ secure.

Theorem 3.2. *Assume the identification scheme* ID *is* $\varepsilon_{\mathsf{zk}}$*-perfect* naHVZK *and has* α *bits of min entropy. For any* $\mathsf{UF\text{-}CMA}_1$ *(*$\mathsf{sUF\text{-}CMA}_1$*) quantum adversary* A *that issues at most* Q_{H} *queries to the quantum random oracle* $|\mathsf{H}\rangle$ *and* Q_S

(classical) queries to the signing oracle SIGN_1*, there exists a quantum adversary* B *against* $\mathsf{UF\text{-}NMA}$ *security making* Q_H *queries to its own quantum random oracle (and a quantum adversary* C *against* CUR*) such that*

$$\mathrm{Adv}^{\mathsf{UF\text{-}CMA}_1}_{\mathsf{SIG}}(\mathsf{A}) \le \mathrm{Adv}^{\mathsf{UF\text{-}NMA}}_{\mathsf{SIG}}(\mathsf{B}) + 2^{-\alpha+1} + \kappa_m Q_S \cdot \varepsilon_{\mathsf{zk}}$$
$$\mathrm{Adv}^{\mathsf{sUF\text{-}CMA}_1}_{\mathsf{SIG}}(\mathsf{A}) \le \mathrm{Adv}^{\mathsf{UF\text{-}NMA}}_{\mathsf{SIG}}(\mathsf{B}) + 2^{-\alpha+1} + \mathrm{Adv}^{\mathsf{CUR}}_{\mathsf{ID}}(\mathsf{C}) + \kappa_m Q_S \cdot \varepsilon_{\mathsf{zk}},$$

and $\mathrm{Time}(\mathsf{B}) = \mathrm{Time}(\mathsf{C}) = \mathrm{Time}(\mathsf{A}) + \kappa_m(Q_\mathsf{H} + Q_S) \approx \mathrm{Time}(\mathsf{A})$.

Proof (of Theorem 3.2). We first prove standard unforgeability ($\mathsf{UF\text{-}CMA}_1$ security) and then show how the proof can be modified to obtain strong unforgeability ($\mathsf{sUF\text{-}CMA}_1$ security). Let A be a quantum adversary against the $\mathsf{UF\text{-}CMA}_1$ security of SIG, issuing at most Q_H queries to $|\mathsf{H}\rangle$ and at most Q_S queries to SIGN_1. Consider the games given in Fig. 8. Recall that A has classical access to the signing oracle SIGN_1 and quantum access to the random oracle H. The quantum random oracle H is called with $|W \parallel M\rangle$ and returns $|\mathsf{H}(|W \parallel M\rangle)\rangle$. The games in Fig. 8 describe the computation that is performed for any $W \parallel M$ that has a non-zero amplitude in $|W \parallel M\rangle$.

GAME G_0. Note that game G_0 is the original $\mathsf{UF\text{-}CMA}_1$ game. The signing oracle SIGN_1 produces a signature using internal deterministic algorithm $\mathsf{GetTrans}$ which, in lines 10 and 12, derives the randomness of P_1 and P_2 using a perfect random function RF that cannot be accessed by A. Since in the $\mathsf{UF\text{-}CMA}_1$ game only one single signing query is allowed per message,

$$\Pr[G_0^\mathsf{A} \Rightarrow 1] = \mathrm{Adv}^{\mathsf{UF\text{-}CMA}_1}_{\mathsf{SIG}}(\mathsf{A}).$$

GAME G_0-G_2

01 $(pk, sk) \leftarrow \mathsf{IGen}(\mathsf{par})$
02 $(M^*, \sigma^*) \leftarrow \mathsf{A}^{|\mathsf{H}\rangle, \text{SIGN}_1}(pk)$
03 Parse $\sigma^* = (W^*, Z^*)$
04 $c^* := \mathsf{H}(W^* \parallel M^*)$
05 **if** $c^* \neq \mathsf{H}'(W^* \parallel M^*)$ then **return** 0 // G_2
06 **return** $[\![M^* \notin \mathcal{M}]\!] \wedge \mathsf{V}(pk, W^*, c^*, Z^*)$

$\underline{\mathsf{GetTrans}(M)}$ // G_0
07 $\kappa := 0$
08 **while** $Z_M = \perp$ and $\kappa \le \kappa_m$ do
09 $\quad \kappa := \kappa + 1$
10 $\quad (W_M, St) := \mathsf{P}_1(sk; \mathsf{RF}(0 \parallel M \parallel \kappa))$
11 $\quad c_M := \mathsf{H}(W_M \parallel M)$
12 $\quad Z_M := \mathsf{P}_2(sk, W_M, c_M, St; \mathsf{RF}(1 \parallel M \parallel \kappa))$
13 **if** $Z_M = \perp$ then $(W_M, c_M, Z_M) = (\perp, \perp, \perp)$
14 **return** (W_M, c_M, Z_M)

$\underline{\text{SIGN}_1(M)}$
15 **if** $M \in \mathcal{M}$ then **return** $\perp$
16 $\mathcal{M} = \mathcal{M} \cup \{M\}$
17 $(W_M, c_M, Z_M) := \mathsf{GetTrans}(M)$
18 **return** $\sigma_M := (W_M, Z_M)$

$\underline{\mathsf{H}(W \parallel M)}$ //quantum access
19 $(W_M, c_M, Z_M) := \mathsf{GetTrans}(M)$ // G_1-G_2
20 **if** $W = W_M$ then **return** $c := c_M$ // G_1-G_2
21 **return** $c := \mathsf{H}'(W \parallel M)$

$\underline{\mathsf{GetTrans}(M)}$ // G_1-G_2
22 $\kappa := 0$
23 **while** $Z_M = \perp$ and $\kappa \le \kappa_m$ do
24 $\quad \kappa := \kappa + 1$
25 $\quad (W_M, c_M, Z_M) := \mathsf{Sim}(pk; \mathsf{RF}(M \parallel \kappa))$
26 **if** $Z_M = \perp$ then $(W_M, c_M, Z_M) = (\perp, \perp, \perp)$
27 **return** (W_M, c_M, Z_M)

Fig. 8. Games G_0, G_1, G_2 for the proof of Theorem 3.2. Here RF and H' are perfect random function that cannot be accessed by A. Deterministic algorithm $\mathsf{GetTrans}(M)$ is only used internally and cannot be accessed by A.

GAME G_1. This game computes the signatures on M using the naHVZK simulation algorithm Sim and patches the quantum random oracle H accordingly.

Concretely, consider a classical query $\text{SIGN}_1(M)$ and let κ_M be the smallest integer $1 \le \kappa \le \kappa_m$ satisfying $(W, c, Z) := \mathsf{Sim}(pk; \mathsf{RF}(M \parallel \kappa))$ and $Z \neq \bot$. If no such integer exists, then we define $\kappa_M := \bot$. It deterministically computes

$$(W_M, c_M, Z_M) := \mathsf{GetTrans}(M) = \begin{cases} \mathsf{Sim}(pk; \mathsf{RF}(M \parallel \kappa_M)) & 1 \le \kappa_M \le \kappa_m \\ (\bot, \bot, \bot) & \kappa_M = \bot \end{cases} \quad (4)$$

The signature on M is returned as

$$\sigma_M := (W_M, Z_M).$$

By the naHVZK property and the union bound, the distribution of each σ_M has statistical distance at most $\kappa_m \varepsilon_{\mathsf{zk}}$ from one computed in game G_0. To ensure that σ_M is a valid signature on M, in line 20 the random oracle is patched such that $\mathsf{H}(W_M \parallel M) = c_M$ holds. Concretely, a query $W \parallel M$ to quantum random oracle H with non-zero amplitude is patched with $\mathsf{H}(W \parallel M) := c_M$ iff $W = W_M$, where c_M and W_M are computed by $\mathsf{GetTrans}(M)$, see Eq. (4). Note that the output distribution of the random oracle H in this game remains unchanged since c_M generated by the naHVZK simulator Sim is required to be uniformly distributed.

Overall, by a union bound we obtain

$$|\Pr[G_1^{\mathsf{A}} \Rightarrow 1] - \Pr[G_0^{\mathsf{A}} \Rightarrow 1]| \le \kappa_m Q_S \cdot \varepsilon_{\mathsf{zk}}.$$

GAME G_2. This game returns 0 in line 05 if $c^* \neq \mathsf{H}'(W^* \parallel M^*)$. Games G_1 and G_2 can only differ if $W_{M^*} = W^*$ and $M^* \notin \mathcal{M}$. (In that case G_2 returns 0 and G_1 returns 1.) Since $M^* \notin \mathcal{M}$, the random variable W_{M^*} was not yet revealed as part of an established signature and is completely hidden from the view of the adversary. It has α bits of min-entropy, meaning we have $\Pr[W_{M^*} = W^*] \le 2^{-\alpha}$. We obtain

$$|\Pr[G_2^{\mathsf{A}} \Rightarrow 1] - \Pr[G_1^{\mathsf{A}} \Rightarrow 1]| \le 2^{-\alpha+1}.$$

Consider adversary B against the UF-NMA game from Fig. 9 having quantum access to random oracle H'. It perfectly simulates A's view in game G_2, using its own random oracle H' to simulate H and perfectly simulating the random function RF with a $2\kappa_m Q_{\mathsf{H}}$-wise independent hash function. Assume A's forgery (M^*, σ^*) is valid in game G_2, i.e., $M^* \notin \mathcal{M}$ and $\mathsf{V}(pk, W^*, c^*, Z^*) = 1$, where $c^* = \mathsf{H}(W^* \parallel M^*)$. If $\mathsf{H}(W^* \parallel M^*) = \mathsf{H}'(W^* \parallel M^*)$, then (M^*, σ^*) is also a valid forgery in the UF-NMA game, i.e., $\mathsf{V}(pk, W^*, c^*, Z^*) = 1$, where $c^* = \mathsf{H}'(W^* \parallel M^*)$. Hence,

$$\Pr[G_2^{\mathsf{A}} \Rightarrow 1] = \mathrm{Adv}_{\mathsf{SIG}}^{\mathsf{UF\text{-}NMA}}(\mathsf{B}).$$

The proof of $\mathsf{UF\text{-}CMA}_1$ security follows by collecting the probabilities. The running time Time(B) of adversary B is given by the time Time(A) to run A as a

Adversary $\mathsf{B}^{|\mathsf{H}'\rangle}(pk)$

01 $(M^*, \sigma^*) \leftarrow \mathsf{A}^{|\mathsf{H}\rangle, \text{SIGN}_1}(pk)$
02 Parse $\sigma^* = (W^*, Z^*)$
03 $c^* := \mathsf{H}(W^* \parallel M^*)$
04 **if** $c^* \neq \mathsf{H}'(W^* \parallel M^*)$ then **abort**
05 **if** $[\![M^* \notin \mathcal{M}]\!] \wedge \mathsf{V}(pk, W^*, c^*, Z^*)$ then **return** (M^*, σ^*)
06 **abort**

Fig. 9. Adversary B against UF-NMA security of SIG with quantum access to random oracle H'. The oracles SIGN_1 and H simulated by B are defined as in game G_2 of Fig. 8.

blackbox in game G_2 where in every of the Q_H oracle- and Q_S signature-queries, at most $O(\kappa_m)$ computations need to be performed.

STRONG UNFORGEABILITY. For sUF-CMA$_1$ security we consider exactly the same games with the difference that in all games the winning condition in line 06 is changed to $[\![(M^*, \sigma^*) \notin \mathcal{M}]\!] \wedge \mathsf{V}(pk, W^*, c^*, Z^*)$ to account for strong unforgerability, where $\mathcal{M}$ now records all tuples (M, σ_M) of previously established messages/signature pairs.

The difference between games G_1 and G_2 is that game G_2 returns 0 in line 05 if $c^* \neq \mathsf{H}'(W^* \parallel M^*)$, i.e., if $\mathsf{H}(W^* \parallel M^*)$ was previously patched in line 20 with $\mathsf{H}(W^* \parallel M^*) := c_{M^*}$. Games G_1 and G_2 can only differ if $W_{M^*} = W^*$, $(M^*, \sigma^*) \notin \mathcal{M}$, and $\mathsf{V}(pk, W^*, c^*, Z^*) = 1$. (In that case G_2 returns 0 and G_1 returns 1.)

We distinguish two cases. If $(M^*, \cdot) \notin \mathcal{M}$ then we are in the situation that the adversary did not query a signature on M^* and we can use the same argument as in standard unforgeability to argue $|\Pr[G_2^\mathsf{A} \Rightarrow 1] - \Pr[G_1^\mathsf{A} \Rightarrow 1]| \leq 2^{-\alpha+1}$. It leaves to handle the case $(M^*, \cdot) \in \mathcal{M}$, i.e., the adversary obtained a signatures $\sigma_{M^*} = (W_{M^*}, Z_{M^*})$ on message M^* and submits a correct forgery $\sigma^* = (W^*, Z^*)$ satisfying $W^* = W_{M^*}$ and $Z^* \neq Z_{M^*}$. The problem of finding values (W^*, c^*, Z_{M^*}, Z^*) with two accepting transcripts (W^*, c^*, Z^*) and (W^*, c^*, Z_{M^*}) is exactly bounded by the advantage of an adversary C against the CUR experiment, i.e., $|\Pr[G_2^\mathsf{A} \Rightarrow 1] - \Pr[G_1^\mathsf{A} \Rightarrow 1]| \leq \text{Adv}_{\mathsf{ID}}^{\mathsf{CUR}}(\mathsf{C})$.

In combination this proves

$$|\Pr[G_2^\mathsf{A} \Rightarrow 1] - \Pr[G_1^\mathsf{A} \Rightarrow 1]| \leq 2^{-\alpha+1} + \text{Adv}_{\mathsf{ID}}^{\mathsf{CUR}}(\mathsf{C}).$$

Finally, a straightforward modification of adversary B against UF-NMA security to account for the strong unforgerability check proves

$$\Pr[G_2^\mathsf{A} \Rightarrow 1] = \text{Adv}_{\mathsf{SIG}}^{\mathsf{UF\text{-}NMA}}(\mathsf{B})$$

and completes proof of sUF-CMA$_1$ security.

The running times Time(B) and Time(C) can be derived as above. □

The following theorem shows that we can also prove directly UF-CMA security of SIG, but (in terms of the running time) the reduction is less tight than the one of Theorem 3.2.

Theorem 3.3. *Assume the identification scheme* ID *is* $\varepsilon_{\mathsf{zk}}$*-perfect* naHVZK *and has* α *bits of min entropy. For any* $\mathsf{UF\text{-}CMA}$ *(*$\mathsf{sUF\text{-}CMA}$*) quantum adversary* A *that issues at most* Q_{H} *queries to the quantum random oracle* $|\mathsf{H}\rangle$ *and* Q_S *classical queries to the signing oracle* Sign*, there exists a quantum adversary* B *against* $\mathsf{UF\text{-}NMA}$ *security making* Q_{H} *queries to its own quantum random oracle (and a quantum adversary* C *against* CUR*) such that*

$$\mathrm{Adv}^{\mathsf{UF\text{-}CMA}}_{\mathsf{SIG}}(\mathsf{A}) \le \mathrm{Adv}^{\mathsf{UF\text{-}NMA}}_{\mathsf{SIG}}(\mathsf{B}) + Q_S \cdot 2^{-\alpha+1} + \kappa_m Q_S \cdot \varepsilon_{\mathsf{zk}},$$
$$\mathrm{Adv}^{\mathsf{sUF\text{-}CMA}}_{\mathsf{SIG}}(\mathsf{A}) \le \mathrm{Adv}^{\mathsf{UF\text{-}NMA}}_{\mathsf{SIG}}(\mathsf{B}) + Q_S \cdot 2^{-\alpha+1} + \kappa_m Q_S \cdot \varepsilon_{\mathsf{zk}} + \mathrm{Adv}^{\mathsf{CUR}}_{\mathsf{ID}}(\mathsf{C}),$$

and $\mathrm{Time}(\mathsf{B}) = \mathrm{Time}(\mathsf{C}) = \mathrm{Time}(\mathsf{A}) + \kappa_m Q_{\mathsf{H}} Q_S$.

The proof of Theorem 3.3 is similar to the one of Theorem 3.2 and appears in the full version.

Theorem 3.4. *Assume the identification scheme is lossy and* $\varepsilon_{\mathsf{ls}}$*-lossy sound. For any* $\mathsf{UF\text{-}NMA}$ *quantum adversary* A *that issues at most* Q_{H} *queries to the quantum random oracle* $|\mathsf{H}\rangle$*, there exists a quantum adversary* B *against* LOSS *such that*

$$\mathrm{Adv}^{\mathsf{UF\text{-}NMA}}_{\mathsf{SIG}}(\mathsf{A}) \le \mathrm{Adv}^{\mathsf{LOSS}}_{\mathsf{ID}}(\mathsf{B}) + 8(Q_{\mathsf{H}}+1)^2 \cdot \varepsilon_{\mathsf{ls}},$$

and $\mathrm{Time}(\mathsf{B}) = \mathrm{Time}(\mathsf{A}) + Q_{\mathsf{H}} \approx \mathrm{Time}(\mathsf{A})$.

Proof. Let A be an adversary against the $\mathsf{UF\text{-}NMA}$ security of SIG, issuing at most Q_{H} quantum queries to $|\mathsf{H}\rangle$. Consider the games given in Fig. 10.

Game G_0. Since game G_0 is the original $\mathsf{UF\text{-}NMA}$ game,

$$\Pr[G_0^{\mathsf{A}} \Rightarrow 1] = \mathrm{Adv}^{\mathsf{UF\text{-}NMA}}_{\mathsf{SIG}}(\mathsf{A}).$$

Game G_1. In this game, the public key pk is changed to lossy mode. Clearly, there exists an adversary B simulating H by a $2Q_{\mathsf{H}}$-wise independent hash function such that

$$|\Pr[G_1^{\mathsf{A}} \Rightarrow 1] - \Pr[G_0^{\mathsf{A}} \Rightarrow 1]| \le \mathrm{Adv}^{\mathsf{LOSS}}_{\mathsf{ID}}(\mathsf{B}).$$

Finally, we will reduce a successful A in game G_1 to the generic search problem GSPB to show

$$\Pr[G_1^{\mathsf{A}} \Rightarrow 1] \le 8(Q_{\mathsf{H}}+1)^2 \varepsilon_{\mathsf{ls}}. \tag{5}$$

GAME G_0-G_1

$(pk, sk) \leftarrow \mathsf{IGen}(\mathsf{par})$ // G_0
$pk \leftarrow \mathsf{LossyIGen}(\mathsf{par})$ // G_1
$(M^*, \sigma^*) \leftarrow \mathsf{A}^{|\mathsf{H}\rangle}(pk)$
Parse $\sigma^* = (W^*, Z^*)$
$c^* := \mathsf{H}(W^* \,\|\, M^*)$
return $\mathsf{V}(pk, W^*, c^*, Z^*)$

Fig. 10. Games G_0-G_1 for the proof of Theorem 3.4.

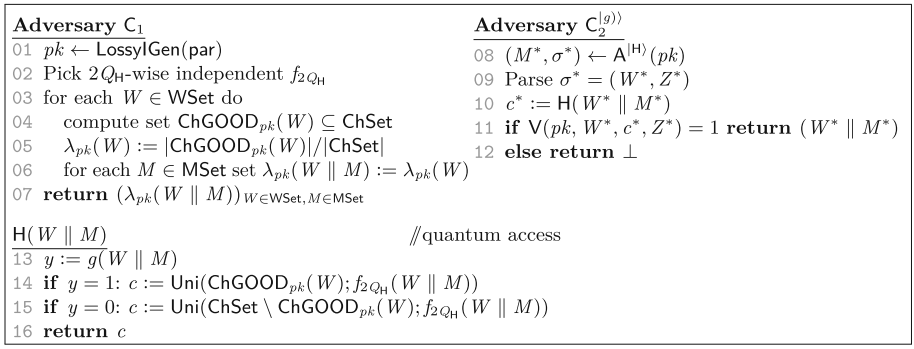

Fig. 11. Adversary $\mathsf{C} = (\mathsf{C}_1, \mathsf{C}_2)$ in game GSPB for the proof of Theorem 3.4. The set of good challenges $\mathsf{ChGOOD}_{pk}(W)$ is defined in Eq. (6).

For a finite set S, let $\mathsf{Uni}(S)$ be a probabilistic algorithm that returns uniform $x \leftarrow S$ and recall that $x := \mathsf{Uni}(S; r)$ denotes the deterministic execution of $\mathsf{Uni}(S)$ using explicitly given random tape r. To prove Eq. (5), consider the unbounded adversary $\mathsf{C} = (\mathsf{C}_1, \mathsf{C}_2)$ defined in Fig. 11 that is executed in the generic search game GSPB, making at most Q_{H} quantum queries to the oracle $|g(\cdot)\rangle$. First note that computing the probabilities $\lambda_{pk}(W \parallel M) = \lambda_{pk}(W)$ in line 05 for all $W \in \mathsf{WSet}$ and $M \in \mathsf{MSet}$ may take exponential time but since C is computationally unbounded it does not matter.

To analyze C's success probability in game GSPB, we first fix a public-key pk. Now consider some $W \parallel M$ with non-zero amplitude as part of a query to quantum random oracle H. Set $\mathsf{ChGOOD}_{pk}(W)$ of "good challenges" is defined as

$$\mathsf{ChGOOD}_{pk}(W) := \{c \in \mathsf{ChSet} \mid \exists Z \in \mathsf{ZSet} : \mathsf{V}(pk, W, c, Z) = 1\}. \tag{6}$$

That is, the set $\mathsf{ChGOOD}_{pk}(W)$ contains all challenges c for which there exists a possible response Z to make (W, c, Z) a valid transcript (with respect to pk). By definition of GSPB, each query to oracle $g(W \parallel M)$ returns $y = 1$ with probability $\lambda_{pk}(W \parallel M) = |\mathsf{ChGOOD}_{pk}(W)|/|\mathsf{ChSet}|$. Hence, the output distribution of $\mathsf{H}(W \parallel M)$ sampled in lines 14 and 15 is uniform over ChSet, as in game G_1. Consistency of H is assured by deriving the randomness to sample c in case $y = 0$ (lines 14 and 15) using fixed random coins $f_{2Q_{\mathsf{H}}}(W \parallel M)$, derived by a $2Q_{\mathsf{H}}$-wise independent hash function $f_{2Q_{\mathsf{H}}}$ (which looks like a perfectly random function to A).

Now consider A's forgery $\sigma^* = (W^*, Z^*)$ on message M^* and define $c^* := \mathsf{H}(W^* \parallel M^*)$. If the signature is valid (i.e., $\mathsf{V}(pk, W^*, c^*, Z^*) = 1$), then clearly c^* is a good challenge from set $\mathsf{ChGOOD}_{pk}(W^*)$ which implies $g(W^* \parallel M^*) = 1$. This proves

$$\Pr[G_1 \Rightarrow 1 \mid pk] = \Pr[\mathsf{GSPB}^{\mathsf{C}}_{\lambda_{pk}} \Rightarrow 1 \mid pk] \leq 8(Q_{\mathsf{H}} + 1)^2 \lambda_{pk}, \tag{7}$$

where

$$\lambda_{pk} = \max_{W \in \mathsf{WSet}, M \in \mathsf{MSet}} \lambda_{pk}(W \parallel M)$$

Averaging Eq. (7) over $pk \leftarrow \mathsf{LossyIGen}$ we finally obtain

$$\Pr[G_1 \Rightarrow 1] \leq 8(Q_\mathsf{H}+1)^2 \cdot \mathbf{E}_{pk}[\lambda_{pk}] \leq 8(Q_\mathsf{H}+1)^2 \varepsilon_{\mathsf{ls}},$$

where the last inequality uses Eq. (3) for the optimal adversary. □

4 Dilithium-QROM

In this section, we present a modification of the Dilithium digital signature scheme [16] whose security is based on MLWE in the QROM. We also present a new security proof of the original Dilithium that shows it to be tightly-secure in the QROM based on a different non-interactive assumption. Since Dilithium is a highly-optimized version of a scheme constructed via the "Fiat-Shamir with Aborts" framework [26], its details may be somewhat overwhelming to readers who are not already comfortable with such constructions. For this reason, we present a much simpler version of the signature scheme without any optimizations in the full version of this paper.

4.1 Preliminaries

Rings and Distributions. We let R and R_q respectively denote the rings $\mathbb{Z}[X]/(X^n+1)$ and $\mathbb{Z}_q[X]/(X^n+1)$, for an integer q. We will assume that $q \equiv 5 (\mathrm{mod}\, 8)$, as such a choice of q ensures that all polynomials in R_q with coefficients less than $\sqrt{q/2}$ have an inverse in the ring [29, Lemma 2.2]. This property is crucial to our security proof. Regular font letters denote elements in R or R_q (which includes elements in $\mathbb{Z}$ and $\mathbb{Z}_q$) and bold lower-case letters represent column vectors with coefficients in R or R_q. By default, all vectors will be column vectors. Bold upper-case letters are matrices.

Modular reductions. For an even (resp. odd) positive integer α, we define $r' = r \bmod^{\pm} \alpha$ to be the unique element r' in the range $-\frac{\alpha}{2} < r' \leq \frac{\alpha}{2}$ (resp. $-\frac{\alpha-1}{2} \leq r' \leq \frac{\alpha-1}{2}$) such that $r' = r \bmod \alpha$. We will sometimes refer to this as a *centered* reduction modulo q. For any positive integer α, we define $r' = r \bmod^{+} \alpha$ to be the unique element r' in the range $0 \leq r' < \alpha$ such that $r' = r \bmod \alpha$. When the exact representation is not important, we simply write $r \bmod \alpha$.

Sizes of elements. For an element $w \in \mathbb{Z}_q$, we write $\|w\|_\infty$ to mean $|w \bmod^{\pm} q|$. We now define the ℓ_∞ and ℓ_2 norms for $w = w_0 + w_1 X + \ldots + w_{n-1} X^{n-1} \in R$:

$$\|w\|_\infty = \max_i \|w_i\|_\infty, \quad \|w\| = \sqrt{\|w_0\|_\infty^2 + \ldots + \|w_{n-1}\|_\infty^2}.$$

Similarly, for $\mathbf{w} = (w_1, \ldots, w_k) \in R^k$, we define

$$\|\mathbf{w}\|_\infty = \max_i \|w_i\|_\infty, \quad \|\mathbf{w}\| = \sqrt{\|w_1\|^2 + \ldots + \|w_k\|^2}.$$

We will write S_η to denote all elements $w \in R$ such that $\|w\|_\infty \leq \eta$.

Extendable output function. Suppose that Sam is an extendable output function, that is a function on bit strings in which the output can be extended to any desired length. If we would like Sam to take as input x and then produce a value y that is distributed according to distribution S (or uniformly over a set S), we write $y \sim S := \mathsf{Sam}(x)$. It is important to note that this procedure is completely deterministic: a given x will always produce the same y. For simplicity we assume that the output distribution of Sam is perfect, whereas in practice Sam will be implemented using random oracles and produce an output that is statistically close to the perfect distribution. If K is a secret key, then $\mathsf{Sam}(K\|x)$ is a pseudo-random function from $\{0,1\}^* \to \{0,1\}^*$.

The Challenge Space. The challenge space in our identification and signature schemes needs to be a subset of the ring R, have size a little larger than 2^{256}, and consist of polynomials with small norms. In this paper, the dimension n of the ring R will be taken to be 512,[3] and so we will define the challenge space accordingly as

$$\mathsf{ChSet} := \{c \in R \,|\, \|c\|_\infty = 1 \text{ and } \|c\| = \sqrt{46}\}. \tag{8}$$

In other words, ChSet consists of elements in R with $-1/0/1$ coefficients that have exactly 46 non-zero coefficients. The size of this set is $\binom{n}{46} \cdot 2^{46}$, which for $n = 512$ is greater than 2^{265}.

The MLWE Assumption. For integers m, k, and a probability distribution $D : R_q \to [0,1]$, we say that the advantage of algorithm A in solving the decisional $\mathsf{MLWE}_{m,k,D}$ problem over the ring R_q is

$$\begin{aligned}\mathrm{Adv}^{\mathsf{MLWE}}_{m,k,D} := \big|&\Pr[\mathsf{A}(\mathbf{A}, \mathbf{t}) \Rightarrow 1 \,|\, \mathbf{A} \leftarrow R_q^{m\times k}; \mathbf{t} \leftarrow R_q^m] \\ &- \Pr[\mathsf{A}(\mathbf{A}, \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2) \Rightarrow 1 \,|\, \mathbf{A} \leftarrow R_q^{m\times k}; \mathbf{s}_1 \leftarrow D^k; \mathbf{s}_2 \leftarrow D^m]\big|.\end{aligned}$$

The MLWE assumption states that the above advantage is negligible for all polynomial-time algorithms A. This assumption was introduced in [25], and is generalization of the LWE assumption from [35]. The $\mathsf{Ring\text{-}LWE}$ assumption [30] is a special case of MLWE where $k = 1$. Analogously to LWE and $\mathsf{Ring\text{-}LWE}$, it was shown in [25] that solving the MLWE problem for certain parameters is as hard as solving certain worst-case problems in certain algebraic lattices.

Summary of Supporting Algorithms. To reduce the size of the public key, we will need some simple algorithms that extract "higher-order" and "lower-order" bits of elements in $\mathbb{Z}_q$. The goal is that when given an arbitrary element

[3] In Sect. 4.5, we will also discuss a scheme where $n = 256$. For that scheme the challenge space consists of 60 ± 1's.

$\underline{\mathsf{Power2Round}_q(r, d)}$
01 $r := r \bmod^+ q$
02 $r_0 := r \bmod^\pm 2^d$
03 **return** $(r - r_0)/2^d$

$\underline{\mathsf{UseHint}_q(h, r, \alpha)}$
04 $m := (q-1)/\alpha$
05 $(r_1, r_0) := \mathsf{Decompose}_q(r, \alpha)$
06 **if** $h = 1$ and $r_0 > 0$ **return** $(r_1 + 1) \bmod^+ m$
07 **if** $h = 1$ and $r_0 \leq 0$ **return** $(r_1 - 1) \bmod^+ m$
08 **return** r_1

$\underline{\mathsf{MakeHint}_q(z, r, \alpha)}$
09 $r_1 := \mathsf{HighBits}_q(r, \alpha)$
10 $v_1 := \mathsf{HighBits}_q(r + z, \alpha)$
11 **return** $[\![r_1 \neq v_1]\!]$

$\underline{\mathsf{Decompose}_q(r, \alpha)}$
12 $r := r \bmod^+ q$
13 $r_0 := r \bmod^\pm \alpha$
14 **if** $r - r_0 = q - 1$
15 **then** $r_1 := 0$; $r_0 := r_0 - 1$
16 **else** $r_1 := (r - r_0)/\alpha$
17 **return** (r_1, r_0)

$\underline{\mathsf{HighBits}_q(r, \alpha)}$
18 $(r_1, r_0) := \mathsf{Decompose}_q(r, \alpha)$
19 **return** r_1

$\underline{\mathsf{LowBits}_q(r, \alpha)}$
20 $(r_1, r_0) := \mathsf{Decompose}_q(r, \alpha)$
21 **return** r_0

Fig. 12. Supporting algorithms for Dilithium and Dilithium-QROM.

$r \in \mathbb{Z}_q$ and another small element $z \in \mathbb{Z}_q$, we would like to be able to recover the higher order bits of $r + z$ without needing to store z. We therefore define algorithms that take r, z and produce a 1-bit hint h that allows one to compute the higher order bits of $r + z$ just using r and h. This hint is essentially the "carry" caused by z in the addition. The algorithms are exactly as in [16], and we repeat them for convenience in Fig. 12. The algorithms are described as working on integers modulo q, but are extended to polynomials in R_q by simply being applied individually to each coefficient.

The below Lemmas recall the crucial properties of these supporting algorithms that are necessary for the correctness and security of our scheme.

Lemma 4.1. *Suppose that q and α are positive integers satisfying $q > 2\alpha$, $q \equiv 1 \pmod{\alpha}$ and α even. Let $\mathbf{r}$ and $\mathbf{z}$ be vectors of elements in R_q where $\|\mathbf{z}\|_\infty \leq \alpha/2$, and let $\mathbf{h}, \mathbf{h}'$ be vectors of bits. Then the $\mathsf{HighBits}_q$, $\mathsf{MakeHint}_q$, and $\mathsf{UseHint}_q$ algorithms satisfy the following properties:*

1. $\mathsf{UseHint}_q(\mathsf{MakeHint}_q(\mathbf{z}, \mathbf{r}, \alpha), \mathbf{r}, \alpha) = \mathsf{HighBits}_q(\mathbf{r} + \mathbf{z}, \alpha)$.
2. *Let* $\mathbf{v}_1 = \mathsf{UseHint}_q(\mathbf{h}, \mathbf{r}, \alpha)$. *Then* $\|\mathbf{r} - \mathbf{v}_1 \cdot \alpha\|_\infty \leq \alpha + 1$.
3. *For any* $\mathbf{h}, \mathbf{h}'$, *if* $\mathsf{UseHint}_q(\mathbf{h}, \mathbf{r}, \alpha) = \mathsf{UseHint}_q(\mathbf{h}', \mathbf{r}, \alpha)$, *then* $\mathbf{h} = \mathbf{h}'$.

Lemma 4.2. *If $\|\mathbf{s}\|_\infty \leq \beta$ and $\|\mathsf{LowBits}_q(\mathbf{r}, \alpha)\|_\infty < \alpha/2 - \beta$, then*

$$\mathsf{HighBits}_q(\mathbf{r}, \alpha) = \mathsf{HighBits}_q(\mathbf{r} + \mathbf{s}, \alpha).$$

4.2 The Identification Protocol

The constituting algorithms of our identification protocol $\mathsf{ID} = (\mathsf{IGen}, \mathsf{P}_1, \mathsf{P}_2, \mathsf{V})$ are described in Fig. 13 with the concrete parameters $\mathsf{par} = (q, n, k, \ell, d, \gamma, \gamma', \eta, \beta)$ given later in Table 1.

$\underline{\mathsf{IGen}(\mathsf{par})}$
01 $\rho \leftarrow \{0,1\}^{256}$
02 $\mathbf{A} \leftarrow R_q^{k\times\ell} := \mathsf{Sam}(\rho)$
03 $(\mathbf{s}_1, \mathbf{s}_2) \leftarrow S_\eta^\ell \times S_\eta^k$
04 $\mathbf{t} := \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2$
05 $\mathbf{t}_1 := \mathsf{Power2Round}_q(\mathbf{t}, d)$
06 $\mathbf{t}_0 := \mathbf{t} - \mathbf{t}_1 \cdot 2^d$
07 $pk = (\rho, \mathbf{t}_1, \boxed{\mathbf{t}_0})$
08 $sk = (\rho, \mathbf{s}_1, \mathbf{s}_2, \mathbf{t}_0)$
09 **return** (pk, sk)

$\underline{\mathsf{P}_1(sk)}$
10 $\mathbf{A} \leftarrow R_q^{k\times\ell} := \mathsf{Sam}(\rho)$
11 $\mathbf{y} \leftarrow S_{\gamma'-1}^\ell$
12 $\mathbf{w} := \mathbf{A}\mathbf{y}$
13 $\mathbf{w}_1 := \mathsf{HighBits}_q(\mathbf{w}, 2\gamma)$
14 **return** $(W = \mathbf{w}_1, St = (\mathbf{w}, \mathbf{y}))$

$\underline{\mathsf{P}_2(sk, W = \mathbf{w}_1, c, St = (\mathbf{w}, \mathbf{y}))}$
15 $\mathbf{z} := \mathbf{y} + c\mathbf{s}_1$
16 **if** $\|\mathbf{z}\|_\infty \geq \gamma' - \beta$ **or** $\|\mathsf{LowBits}_q(\mathbf{w} - c\mathbf{s}_2, 2\gamma)\|_\infty \geq \gamma - \beta$
17 then $(\mathbf{z}, \mathbf{h}) := \perp$
18 **else** $\mathbf{h} := \mathsf{MakeHint}_q(-c\mathbf{t}_0, \mathbf{w} - c\mathbf{s}_2 + c\mathbf{t}_0, 2\gamma)$
19 **return** $Z = (\mathbf{z}, \mathbf{h})$

$\underline{\mathsf{V}(pk, W = \mathbf{w}_1, c, Z = (\mathbf{z}, \mathbf{h}))}$
20 **return** $[\![\|\mathbf{z}\|_\infty < \gamma' - \beta]\!]$ **and** $[\![\mathbf{w}_1 = \mathsf{UseHint}_q(\mathbf{h}, \mathbf{A}\mathbf{z} - c\mathbf{t}_1 \cdot 2^d, 2\gamma)]\!]$

Fig. 13. Our ID scheme – a concrete instantiation based on the hardness of the MLWE problem of the commitment-recoverable (Definition 2.4) canonical identification scheme in Fig. 4. The $\mathbf{t}_0$ part of the public key is assumed to be known by the adversary in the security proofs, but is not needed by the verifier for verification. Thus in the real scheme, $\mathbf{t}_0$ would not be included as part of the public key.

Key Generation. The key generation proceeds by choosing a random 256-bit seed ρ and expanding into a matrix $\mathbf{A} \in R_q^{k\times\ell}$ by an extendable output function Sam modeled as a random oracle. The secret keys $(\mathbf{s}_1, \mathbf{s}_2) \in S_\eta^\ell \times S_\eta^k$ have uniformly random coefficients between $-\eta$ and η (inclusively). The value $\mathbf{t} = \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2$ is then computed. The public key that is needed for verification is $(\rho, \mathbf{t}_1)$ with $\mathbf{t}_1$ output by the $\mathsf{Power2Round}_q(\mathbf{t}, d)$ algorithm in Fig. 12 (we have $\mathbf{t} = \mathbf{t}_1 \cdot 2^d + \mathbf{t}_0$ for some small $\mathbf{t}_0$), while the secret key is $(\rho, \mathbf{s}_1, \mathbf{s}_2, \mathbf{t}_0)$.

While the verifier never needs the value $\mathbf{t}_0$ (and thus it does not need to be included in the public key of the actual scheme), we do need this value in order to simulate transcripts (see Sect. 4.3). Thus the security of our scheme is based on the fact that the adversary gets $\mathbf{t}_1$ and $\mathbf{t}_0$, whereas in reality he only gets $\mathbf{t}_1$.

The set ChSet is defined as in Eq. (8), and $\mathsf{ZSet} = S_{\gamma'-\beta-1}^\ell \times \{0,1\}^k$. The set of commitments WSet is defined as $\mathsf{WSet} = \{\mathbf{w}_1 \ : \ \exists \mathbf{y} \in S_{\gamma'-1}^\ell \text{ s.t. } \mathbf{w}_1 = \mathsf{HighBits}_q(\mathbf{A}\mathbf{y}, 2\gamma)\}$.

Protocol Execution. The prover starts the identification protocol by reconstructing $\mathbf{A}$ from the random seed ρ. The next step has the prover sample $\mathbf{y} \leftarrow S_{\gamma'-1}^\ell$ and then compute $\mathbf{w} = \mathbf{A}\mathbf{y}$. He then writes $\mathbf{w} = 2\gamma \cdot \mathbf{w}_1 + \mathbf{w}_0$, with $\mathbf{w}_0$ between $-\gamma$ and γ (inclusively), and then sends $\mathbf{w}_1$ to the verifier. The verifier generates a random challenge $c \leftarrow \mathsf{ChSet}$ and sends it to the prover. The prover computes $\mathbf{z} = \mathbf{y} + c\mathbf{s}$. If $\mathbf{z} \notin S_{\gamma'-\beta-1}^\ell$, then the prover sets his response to $\perp$. He also replies with $\perp$ if $\mathsf{LowBits}_q(\mathbf{w} - c\mathbf{s}_2, 2\gamma) \notin S_{\gamma-\beta-1}^k$. This part of the protocol is necessary for security – it makes sure that $\mathbf{z}$ does not leak anything about the secret key $\mathbf{s}_1, \mathbf{s}_2$.

If the checks pass and a $\perp$ is not sent, then it can be shown (see Sect. 4.3) that $\mathsf{HighBits}_q(\mathbf{Az} - c\mathbf{t}, 2\gamma) = \mathbf{w}_1$. At this point, if the verifier knew the entire element $\mathbf{t}$ and $(\mathbf{z}, c)$, he could have recovered $\mathbf{w}_1$ and checked that $\|\mathbf{z}\|_\infty < \gamma' - \beta$ and that the high-order bits of $\mathbf{Az} - c\mathbf{t}$ are indeed $\mathbf{w}_1$. However, since we want to compress the size of the public key, the verifier only knows $\mathbf{t}_1$. Hence, the signer needs to provide a "hint" $\mathbf{h}$ which will allow the verifier to compute $\mathsf{HighBits}_q(\mathbf{Az} - c\mathbf{t}, 2\gamma)$.

The verifier checks whether $\|\mathbf{z}\|_\infty < \gamma' - \beta$ and that $\mathbf{Az} - c\mathbf{t}_1 \cdot 2^d$ together with the hint $\mathbf{h}$ allow him to reconstruct $\mathbf{w}_1$. We should point out that in the identification scheme it is actually not necessary for the verifier to be able to recover exactly $\mathbf{w}_1$. He could have simply checked that $\mathbf{Az} - c\mathbf{t}_1 \cdot 2^d \approx \mathbf{w}_1$ and this would be good enough for security. The reason that we want the verifier to be able to exactly recover $\mathbf{w}_1$ is to make the ID scheme *commitment-recoverable* and be able to reduce the communication size in the Fiat-Shamir transform (see Sect. 3.1).

4.3 Security Properties

In this section we analyze the security of ID. Most of the proofs are postponed to the full version.

Non Abort Honest Verifier Zero-Knowledge. In this section, we will show that ID is perfectly naHVZK, i.e., the distribution of the output of the Trans algorithm (Fig. 14, left) that uses the secret key as input is exactly that of the Sim algorithm (Fig. 14, right) that uses only the public key as input.

Lemma 4.3. *If* $\beta \geq \max_{s \in S_\eta, c \in \mathsf{ChSet}} \|cs\|_\infty$*, then* ID *is perfectly* naHVZK.

Correctness. In this section, we compute the probability that the Prover does not send $\perp$ and then show that the verification procedure will always accept a transcript when the Prover does not send $\perp$.

Lemma 4.4. *If* $\beta \geq \max_{s \in S_\eta, c \in \mathsf{ChSet}} \|cs\|_\infty$ *then* ID *has correctness error* $\delta \approx 1 - \exp\left(-\beta n \cdot (k/\gamma + \ell/\gamma')\right)$.

Algorithm $\mathsf{Trans}(sk)$:
01 $\mathbf{A} \leftarrow R_q^{k \times \ell} := \mathsf{Sam}(\rho)$
02 $\mathbf{y} \leftarrow S_{\gamma'-1}^{\ell}$
03 $\mathbf{w} := \mathbf{Ay}$
04 $\mathbf{w}_1 := \mathsf{HighBits}_q(\mathbf{w}, 2\gamma)$
05 $c \leftarrow \mathsf{ChSet}$
06 $\mathbf{z} := \mathbf{y} + c\mathbf{s}_1$
07 **if** $\|\mathbf{z}\|_\infty \geq \gamma' - \beta$ **then return** $\perp$
08 **if** $\|\mathsf{LowBits}_q(\mathbf{w} - c\mathbf{s}_2, 2\gamma)\|_\infty \geq \gamma - \beta$ **then return** $\perp$
09 $\mathbf{h} := \mathsf{MakeHint}_q(-c\mathbf{t}_0, \mathbf{w} - c\mathbf{s}_2 + c\mathbf{t}_0, 2\gamma)$
10 **return** $(c, (\mathbf{z}, \mathbf{h}))$

Algorithm $\mathsf{Sim}(pk)$:
11 $\mathbf{A} \leftarrow R_q^{k \times \ell} := \mathsf{Sam}(\rho)$
12 with probability $1 - \frac{|S_{\gamma'-\beta-1}^{\ell}|}{|S_{\gamma'-1}^{\ell}|}$, **return** $\perp$
13 $\mathbf{z} \leftarrow S_{\gamma'-\beta-1}^{\ell}$
14 $c \leftarrow \mathsf{ChSet}$
15 **if** $\|\mathsf{LowBits}_q(\mathbf{Az} - c\mathbf{t}, 2\gamma)\|_\infty \geq \gamma - \beta$
16 **then return** $\perp$
17 $\mathbf{h} := \mathsf{MakeHint}_q(-c\mathbf{t}_0, \mathbf{Az} - c\mathbf{t} + c\mathbf{t}_0, 2\gamma)$
18 **return** $(c, (\mathbf{z}, \mathbf{h}))$

Fig. 14. Left: a real transcript output by the transcript algorithm $\mathsf{Trans}(sk)$; Right: a simulated transcript output by the $\mathsf{Sim}(pk)$ algorithm.

$\underline{\mathsf{LossyIGen}(\mathsf{par})}$
01 $\rho \leftarrow \{0,1\}^{256}$; $\mathbf{A} \leftarrow R_q^{k\times\ell} := \mathsf{Sam}(\rho)$
02 $\mathbf{t} \leftarrow R_q^k$
03 $\mathbf{t}_1 := \mathsf{Power2Round}_q(\mathbf{t}, d)$
04 $\mathbf{t}_0 := \mathbf{t} - \mathbf{t}_1 \cdot 2^d$
05 **return** $pk = (\rho, \mathbf{t}_1, \mathbf{t}_0)$

Fig. 15. The lossy instance generator LossyIGen.

Lossyness. In this section, we analyze the scheme in which the public key is generated uniformly at random, as in algorithm LossyIGen of Fig. 15, rather than as in IGen of Fig. 13. Our goal is to show that even if the prover is computationally unbounded, he only has approximately a $1/|\mathsf{ChSet}|$ probability of making the verifier accept during each run of the identification scheme. This will show that the probability in Eq. (3) is upper-bounded by approximately $1/|\mathsf{ChSet}|$.

By observing that the output of LossyIGen is uniformly random over $R_q^{k\times\ell} \times R_q^k$ and the output of IGen in Fig. 13 is $(\mathbf{A}, \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2)$ where $\mathbf{A} \leftarrow R_q^{k\times\ell}$ and $(\mathbf{s}_1, \mathbf{s}_2) \leftarrow S_\eta^\ell \times S_\eta^k$, we have that

$$\mathrm{Adv}^{\mathsf{LOSS}}_{\mathsf{ID}}(\mathsf{A}) = \mathrm{Adv}^{\mathsf{MLWE}}_{k,\ell,D}(\mathsf{A}),$$

where D is the uniform distribution over S_η.

Lemma 4.5. *If* $4\gamma + 2, 2\gamma' < \sqrt{q/2}$ *and* $\gamma' < \gamma\beta$, *and* $\ell \le k$, *then* ID *has* $\varepsilon_{\mathsf{ls}}$*-lossy soundness for*

$$\varepsilon_{\mathsf{ls}} \le \frac{1}{|\mathsf{ChSet}|} + 2 \cdot |\mathsf{ChSet}|^2 \cdot \left(\frac{32\gamma\gamma'}{q}\right)^{nk}.$$

Our proof follows the framework from [3,22]. Then to prove Lemma 4.5, we show that if C, who outputs the first message $(\mathbf{w}_1, St)$ in the LOSSY-IMP game (see Fig. 16) is able to correctly respond to more than one random challenge c, then the previously mentioned linear equation will have a solution, which with high probability is not possible. Therefore we conclude that for virtually all $\mathbf{A}, \mathbf{t}$ output by LossyIGen, there exists (at most) only one challenge for which the prover can respond to, and therefore his success probability is at most $1/|\mathsf{ChSet}|$.

Min Entropy. In Lemma 4.6 we will prove that the $\mathbf{w}_1$ sent by the honest prover in the first step is extremely likely to be distinct for every run of the protocol.

Lemma 4.6. *If* $2\gamma, 2\gamma' < \sqrt{q/2}$ *and* $\ell \le k$, *then the identification scheme* ID *in Fig. 13 has*

$$\alpha > n\ell \cdot \log\left(\min\left\{\frac{q}{(4\gamma+1)(4\gamma'+1)}, 2\gamma' - 1\right\}\right)$$

bits of min-entropy (as in Definition 2.6).

GAME LOSSY-IMP:
01 $pk_{\mathsf{ls}} := (\rho, \mathbf{t}_1, \mathbf{t}_0) \leftarrow \mathsf{LossyIGen}(\mathsf{par})$
02 $(\mathbf{w}_1, St) \leftarrow \mathsf{C}(pk_{\mathsf{ls}})$
03 $c \leftarrow \mathsf{ChSet}$
04 $(\mathbf{z}, \mathbf{h}) \leftarrow \mathsf{C}(St, c)$
05 **return** $[\![\mathbf{w}_1 = \mathsf{UseHint}_q(\mathbf{h}, \mathbf{Az} - c\mathbf{t}_1 \cdot 2^d, 2\gamma)]\!]$ **and** $[\![\|\mathbf{z}\|_\infty < \gamma' - \beta]\!]$

Fig. 16. The lossy impersonation game LOSSY-IMP in case of Dilithium.

Computational Unique Response. In this section we state that our scheme satisfies the Computational Unique Response (CUR) property required for strong-unforgeability of the signature scheme.

Lemma 4.7. *If* $4\gamma + 2$, $2\gamma' < \sqrt{q/2}$ *and* $\gamma' < \gamma\beta$, *and* $\ell \leq k$ *(i.e. the same conditions as in Lemma 4.5), then* $\mathrm{Adv}^{\mathsf{CUR}}_{\mathsf{ID}}(\mathsf{A}) < \left(\frac{32\gamma\gamma'}{q}\right)^{nk}$ *for every (even unbounded) adversary* A.

4.4 The Dilithium-QROM Signature Scheme and Concrete Parameters

In this section, we describe the signature scheme Dilithium-QROM (Fig. 17) which is obtained via the Fiat-Shamir transform from the scheme ID of Fig. 13 and using $\mathsf{Sam}(K \parallel \cdot)$ as a pseudorandom function. We then instantiate it with concrete parameters (Table 1) and compare them for the same security level with those in [16].

The parameters for our scheme are dictated by the requirements for the scheme to be strongly-unforgeable in Theorem 3.1 which gives an upper bound on $\mathrm{Adv}^{\mathsf{sUF\text{-}CMA}}_{\mathsf{Dilithium\text{-}QROM}}(\mathsf{A})$. Following [24], for "$\kappa$ bits of quantum security" for Dilithium-QROM we require that for all quantum adversaries A running in time at most 2^κ,

$$\mathrm{Adv}^{\mathsf{UF\text{-}CMA}}_{\mathsf{Dilithium\text{-}QROM}}(\mathsf{A})/\mathrm{Time}(\mathsf{A}) \leq 2^{-\kappa}. \tag{9}$$

To this end, we need to put bounds on the parameters $\varepsilon_{\mathsf{ls}}, \varepsilon_{\mathsf{zk}}$, and α. Lemma 4.3 tells us that

$$\varepsilon_{\mathsf{zk}} = 0.$$

To lower-bound α, note that in the parameters, we always have $2\gamma = 2\gamma' < \sqrt{q/2}$, and using a lemma in the full version of the paper, we can conclude that α is greater than 2900. Thus the $2^{-\alpha}$ term has absolutely no practical effect in Theorem 3.1 for the parameters in Sect. 4.4.

Lemma 4.7 states that as long as $4\gamma + 2$ and $2\gamma' < \sqrt{q/2}$, we will have $\mathrm{Adv}^{\mathsf{CUR}}_{\mathsf{ID}}(\mathsf{C}) < \left(\frac{32\gamma\gamma'}{q}\right)^{nk}$. The parameters in Table 1 indeed satisfy the preconditions, and so $\mathrm{Adv}^{\mathsf{CUR}}_{\mathsf{ID}}(\mathsf{C}) < \left(\frac{32\gamma\gamma'}{q}\right)^{nk} < 2^{-865}$.

We finally turn to bounding $\varepsilon_{\mathsf{ls}}$. Notice that Lemma 4.5 directly implies that

$$\varepsilon_{\mathsf{ls}} \leq \frac{1}{|\mathsf{ChSet}|} + 2 \cdot |\mathsf{ChSet}|^2 \cdot \left(\frac{32\gamma\gamma'}{q}\right)^{nk}.$$

The size of the challenge set ChSet defined in Eq. (8) is larger than 2^{265}, and so the above is at most

$$\varepsilon_{\mathsf{ls}} \leq 2^{-265} + 2^{-334} \leq 2^{-264}.$$

Plugging everything into the equation at the end of Sect. 3.1, we obtain

$$\begin{aligned}\mathrm{Adv}^{\mathsf{UF\text{-}CMA}}_{\mathsf{Dilithium\text{-}QROM}}(\mathsf{A}) &\leq \mathrm{Adv}^{\mathsf{LOSS}}_{\mathsf{ID}}(\mathsf{B}) + \mathrm{Adv}^{\mathsf{CUR}}_{\mathsf{ID}}(\mathsf{C}) + 8 \cdot (Q_{\mathsf{H}}+1)^2 \cdot \varepsilon_{\mathsf{ls}} \\ &\quad + \mathrm{Adv}^{\mathsf{PR}}_{\mathsf{Sam}}(\mathsf{D}) + \frac{200}{(1-\delta)} \cdot Q_S \cdot \varepsilon_{\mathsf{zk}} + 2^{-\alpha} \\ &< \mathrm{Adv}^{\mathsf{MLWE}}_{\mathsf{ID}}(\mathsf{B}) + Q_{\mathsf{H}}^2 \cdot 2^{-261} + \mathrm{Adv}^{\mathsf{PR}}_{\mathsf{Sam}}(\mathsf{D}).\end{aligned}$$

Table 1 also shows that the parameters of the MLWE problem are chosen such that it provides 128 bits of quantum security (using the same metric as was used in the original Dilithium scheme [16].) Assuming Sam provides 128 bits security when used as a pseudorandom function, we conclude that for all

$\underline{\mathsf{Sign}((sk, K), M)}$
01 $\kappa := 0$
02 $\mathbf{A} \leftarrow R_q^{k\times\ell} := \mathsf{Sam}(\rho)$
03 **while** $(\mathbf{z}, \mathbf{h}) = \perp$ and $\kappa \leq 200/(1-\delta)$ do
04 $\quad \kappa := \kappa + 1$
05 $\quad \mathbf{y} \leftarrow S^{\ell}_{\gamma'-1} := \mathsf{Sam}(K \parallel M \parallel \kappa)$
06 $\quad \mathbf{w} := \mathbf{Ay}$
07 $\quad \mathbf{w}_1 := \mathsf{HighBits}_q(\mathbf{w}, 2\gamma)$
08 $\quad c := \mathsf{H}(\mathbf{w}_1 \parallel M)$
09 $\quad \mathbf{z} := \mathbf{y} + c\mathbf{s}_1$
10 $\quad$ **if** $\|\mathbf{z}\|_\infty \geq \gamma' - \beta$ **or** $\|\mathsf{LowBits}_q(\mathbf{w} - c\mathbf{s}_2, 2\gamma)\|_\infty \geq \gamma - \beta$ then $(\mathbf{z}, \mathbf{h}) := \perp$
11 $\quad$ **else** $\mathbf{h} := \mathsf{MakeHint}_q(-c\mathbf{t}_0, \mathbf{w} - c\mathbf{s}_2 + c\mathbf{t}_0, 2\gamma)$
12 **return** $\sigma = (\mathbf{z}, \mathbf{h}, c)$

$\underline{\mathsf{Ver}(pk, M, \sigma = (\mathbf{z}, \mathbf{h}, c))}$
13 $\mathbf{A} \leftarrow R_q^{k\times\ell} := \mathsf{Sam}(\rho)$
14 $\mathbf{w}'_1 := \mathsf{UseHint}_q(\mathbf{h}, \mathbf{Az} - c\mathbf{t}_1 \cdot 2^d, 2\gamma)$
15 **return** $[\![\|\mathbf{z}\|_\infty < \gamma' - \beta]\!]$ **and** $[\![c = \mathsf{H}(\mathbf{w}'_1 \parallel M)]\!]$

Fig. 17. Our signature scheme $\mathsf{Dilithium\text{-}QROM} := \mathsf{DFS}[\mathsf{ID}]$. The key generation algorithm is IGen from Fig. 13, where the secret key also contains a random key K for the pseudorandom function $\mathsf{Sam}(K \parallel \cdot)$. The bound $200/(1-\delta)$ on κ can be ignored as there is only a $\delta^{200/(1-\delta)} < \exp(-200)$ chance that it will be reached in any call to the signing procedure. Its presence is for consistency with the generic signing algorithm in Sect. 3.1.

Table 1. Parameters for Dilithium-QROM and Dilithium. The security analysis for the MLWE and MSIS problems is as described in [16].

	Dilithium-QROM		Dilithium [16]	
	Recomm.	Very high	Recomm.	Very high
q (ring modulus)	$2^{45} - 21283$	$2^{45} - 21283$	$2^{23} - 8191$	$2^{23} - 8191$
n (ring dimension)	512	512	256	256
(k, ℓ) (dimension of matrix $\mathbf{A}$)	$(4, 4)$	$(5, 5)$	$(5, 4)$	$(6, 5)$
d (dropped bits from $\mathbf{t}$)	15	15	14[a]	14
# of ± 1's in $c \in \mathsf{ChSet}$	46	46	60	60
γ s.t $2\gamma \mid q - 1$	905679	905679	261888	261888
γ' ($\approx$ max. sig. coefficient)	905679	905679	523776	523776
η (maximum coefficient of $\mathbf{s}_1, \mathbf{s}_2$)	7	3	5	3
β ($= \eta \cdot$(# of ± 1's in c))	322	138	275[b]	175
pk size (bytes)	7712	9632	1472	1760
Sig size (bytes)	5690	7098	2701	3366
Exp. repeats $(1/(1-\delta)$ from Lemma 4.4)	4.3	2.2	6.6	4.3
BKZ block-size to break LWE	480	600	485	595
Best known classical bit-cost	140	175	141	174
Best known quantum bit-cost	127	159	128	158
BKZ block-size to break SIS	NA	NA	475	605
Best known classical bit-cost	NA	NA	138	176
Best known quantum bit-cost	NA	NA	125	160

[a]For added compactness of the public key, the size of d (i.e. the amount of bits that one can drop from $\mathbf{t}$) can be such that the necessary condition $\|c\mathbf{t}_0\|_\infty < \gamma$ is not always satisfied. This would invalidate the correctness of the scheme – in particular the proof of Lemma 4.4. Nevertheless, if this condition is satisfied most of the time and the signer simply checks whether $\|c\mathbf{t}_0\|_\infty < \gamma$ before sending the signature (and aborts the signing attempt otherwise), then the scheme retains its correctness property. Since for security, we assumed that $\mathbf{t}_0$ is known to the adversary, this check does not affect security. In the Dilithium scheme, this check is performed at the end of the while loop of the signing algorithm.

[b]The β values for Dilithium were chosen such that $\Pr_{s \leftarrow S_\eta, c \leftarrow \mathsf{ChSet}}[\|sc\|_\infty > \beta]$ is very close to 0. Increasing/decreasing the value of β changes the value δ, which has an effect on the run-time of the scheme.

quantum adversaries running in time at most 2^{128} and making $1 \leq Q_\mathsf{H} \leq 2^{128}$ (quantum) queries to H, and we have

$$\frac{\mathrm{Adv}^{\mathsf{UF\text{-}CMA}}_{\mathsf{Dilithium\text{-}QROM}}(\mathsf{A})}{\mathrm{Time}(\mathsf{A})} \leq \frac{\mathrm{Adv}^{\mathsf{MLWE}}_{\mathsf{ID}}(\mathsf{B})}{\mathrm{Time}(\mathsf{B})} + \frac{\mathrm{Adv}^{\mathsf{PR}}_{\mathsf{Sam}}(\mathsf{D})}{\mathrm{Time}(\mathsf{D})} + Q_\mathsf{H} \cdot 2^{-261} \leq 2^{-128}$$

The signature size in Dilithium-QROM is $(n \cdot \ell \cdot (\lceil \log(2\gamma) \rceil) + nk + 46 \cdot (\log(n) + 1))/8$ bytes, while the public key is $(n \cdot k \cdot (\lceil \log(q) \rceil - d) + 256)/8$ bytes.

In Table 1, we compare the parameters from the current scheme, which can be proved secure based on the hardness of MLWE in the QROM, to those of the original Dilithium scheme from [16], which only has a classical security reduction from the combination of MLWE and MSIS (we introduce this latter problem in the next section). One can see that the sum of the public key and signature sizes are approximately 3.2 times larger in Dilithium-QROM than in Dilithium.

4.5 Security Assumptions for Non-lossy Schemes

The reduction from the MLWE problem to the hardness of the Dilithium-QROM scheme was a direct consequence of Theorem 3.1, which is itself a combination of Theorems 3.2 and 3.4. In this section, we consider the security of schemes for which Theorem 3.4 is inapplicable. In particular, in these schemes it is no longer true that a computationally-unbounded adversary cannot win the LOSSY-IMP game. The reason that one would like to use schemes constructed in such a manner is because they turn out to be more efficient. In particular, the original Dilithium scheme[4] [16], which is virtually identical to the Dilithium-QROM presented in this paper except for the parameter sizes, has outputs (of the public key plus signature) that are smaller by a factor of a little over 3 (see Table 1).

But while the Dilithium scheme has a security reduction from standard lattice problems in the *classical* random-oracle model, there is no such reduction in the quantum random-oracle model. Nevertheless, it is unclear whether this lack of reduction implies any weakness against quantum attacks. It would therefore be useful to understand exactly what assumptions the more efficient scheme is relying on in the quantum random-oracle model.

Let us suppose that the parameters for the Dilithium scheme are set such that Theorem 3.2 is still applicable. That is, suppose that $\varepsilon_{\mathsf{zk}} = 0$, α is very large, and the scheme is commitment-recoverable. In this case, ignoring the $2^{-\alpha+1}$ term, Theorem 3.2 states that the security of the full signature scheme is exactly the security of the UF-NMA signature scheme in the quantum random-oracle model. Since the adversary does not obtain any valid signatures in the UF-NMA security game, the security assumption of such signatures is non-interactive.

Below, we recall the standard MSIS assumption and then define a new assumption, SelfTargetMSIS, upon which the security of Dilithium is based. We also point out that in the *classical* random-oracle model, there is a (non-tight) reduction from the MSIS to the SelfTargetMSIS problem. Then we show that the Dilithium scheme for which Theorem 3.4 is not necessarily applicable, still has a security reduction from the combination of MLWE and SelfTargetMSIS problems.

The MSIS and SelfTargetMSIS Problems. The MSIS problem [25] is a generalization of the SIS [4] and Ring-SIS [28,33] problems in the same way that MLWE is a generalization of LWE and Ring-LWE. To an algorithm A we associate the advantage function $\mathrm{Adv}^{\mathsf{MSIS}}_{m,k,\gamma}(\mathsf{A})$ to solve the (Hermite Normal Form) $\mathsf{MSIS}_{m,k,\gamma}$ problem over the ring R_q as

$$\mathrm{Adv}^{\mathsf{MSIS}}_{m,k,\gamma}(\mathsf{A}) := \Pr\left[0 < \|\mathbf{y}\|_\infty \le \gamma \wedge [\mathbf{I} \,|\, \mathbf{A}] \cdot \mathbf{y} = \mathbf{0} \mid \mathbf{A} \leftarrow R_q^{m \times k}; \mathbf{y} \leftarrow \mathsf{A}(\mathbf{A})\right].$$

As for SIS and Ring-SIS, it was shown that solving MSIS for certain parameters is as hard as worst-case instances of lattice problems over algebraic lattices of a certain form [25].

[4] We refer to the deterministic version of the scheme.

Suppose that $\mathsf{H} : \{0,1\}^* \to \mathsf{ChSet}$ is a cryptographic hash function. To an algorithm A we associate the advantage function $\mathrm{Adv}^{\mathsf{SelfTargetMSIS}}_{\mathsf{H},m,k,\gamma}(\mathsf{A})$ to solve the $\mathsf{SelfTargetMSIS}_{\mathsf{H},m,k,\gamma}$ problem over the ring R_q as

$$\mathrm{Adv}^{\mathsf{SelfTargetMSIS}}_{\mathsf{H},m,k,\gamma}(\mathsf{A}) := \Pr\left[\begin{array}{l}\|\mathbf{y}\|_\infty \le \gamma \\ \wedge \mathsf{H}([\mathbf{I} \,|\, \mathbf{A}] \cdot \mathbf{y} \parallel M) = c\end{array}\middle| \mathbf{A} \leftarrow R_q^{m\times k}; \left(\mathbf{y} := \begin{bmatrix}\mathbf{r}\\ c\end{bmatrix}, M\right) \leftarrow \mathsf{A}^{|\mathsf{H}\rangle}(\mathbf{A})\right].$$

If A only has classical access to H, then there is a reduction, using the forking lemma [9,34], to prove that $\mathrm{Adv}^{\mathsf{SelfTargetMSIS}}_{\mathsf{H},m,k,\gamma}(\mathsf{B}) \approx \sqrt{\mathrm{Adv}^{\mathsf{MSIS}}_{m,k,2\gamma}(\mathsf{A})/Q_\mathsf{H}}$, where Q_H is the number of classical queries to H.[5] This reduction is standard and is implicit in the (classical) security proofs of digital signatures based on the hardness of the SIS problem (cf. [16,27]).

Security based on MLWE, MSIS, and $\mathsf{SelfTargetMSIS}$ in the QROM. The QROM security of (deterministic) $\mathsf{Dilithium}$ can be expressed as

$$\mathrm{Adv}^{\mathsf{sUF\text{-}CMA}}_{\mathsf{Dilithium}}(\mathsf{A}) \le \mathrm{Adv}^{\mathsf{MLWE}}_{k,\ell,D}(\mathsf{B}) + \mathrm{Adv}^{\mathsf{SelfTargetMSIS}}_{\mathsf{H},k,\ell+1,\zeta}(\mathsf{C}) \tag{10}$$

$$+ \mathrm{Adv}^{\mathsf{PR}}_{\mathsf{Sam}}(\mathsf{D}) + \mathrm{Adv}^{\mathsf{MSIS}}_{k,\ell,\zeta'}(\mathsf{E}) + 2^{-\alpha+1}, \tag{11}$$

for D a uniform distribution over S_η,

$$\zeta = \max\{\gamma' - \beta, 2\gamma + 1 + 2^{d-1} \cdot \rho\}, \tag{12}$$

where ρ is the number of ± 1's in the challenge set ChSet, and

$$\zeta' = \max\{2(\gamma' - \beta), 4\gamma + 2\}. \tag{13}$$

The proof that the min-entropy α is greater than 255, and the proof for strong unforgeability appears in the full version of the paper. The bound in Eq. (10) is then obtained by combining Theorem 3.2 with results from Sect. 4.3.

Acknowledgments. Eike Kiltz was supported in part by ERC Project ERCC (FP7/615074) and by DFG SPP 1736 Big Data. Vadim Lyubashevsky was supported by the SNSF ERC Transfer Starting Grant CRETP2-166734-FELICITY and the H2020 Project SAFEcrypto. Christian Schaffner was supported by a NWO VIDI grant (639.022.519). The authors are grateful to Dominique Unruh and the anonymous reviewers for comments and discussions.

[5] This can be improved to $Q_\mathsf{H}\mathrm{Adv}^{\mathsf{SelfTargetMSIS}}_{\mathsf{H},m,k,\gamma}(\mathsf{B})/\mathrm{Time}(\mathsf{B}) \approx \mathrm{Adv}^{\mathsf{MSIS}}_{m,k,2\gamma}(\mathsf{A})/\mathrm{Time}(\mathsf{A})$.

References

1. NIST Special Publication 800–165 Computer Security Division 2012 Annual Report, p. 39, June 2013. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography. Accessed 30 Jan 2014. 554
2. Abdalla, M., An, J.H., Bellare, M., Namprempre, C.: From identification to signatures via the Fiat-Shamir transform: minimizing assumptions for security and forward-security. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 418–433. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-46035-7_28. 553
3. Abdalla, M., Fouque, P.-A., Lyubashevsky, V., Tibouchi, M.: Tightly-secure signatures from lossy identification schemes. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 572–590. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_34. 553, 554, 555, 556, 558, 564, 578
4. Ajtai, M.: Generating hard instances of lattice problems (extended abstract). In: 28th ACM STOC, pp. 99–108. ACM Press, May 1996. 582
5. Alkim, E., Bindel, N., Buchmann, J., Dagdelen, Ö., Eaton, E., Gutoski, G., Krämer, J., Pawlega, F.: Revisiting TESLA in the quantum random oracle model. In: Lange, T., Takagi, T. (eds.) PQCrypto 2017. LNCS, vol. 10346, pp. 143–162. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-59879-6_9. 554, 555, 556, 558
6. Ambainis, A., Rosmanis, A., Unruh, D.: Quantum attacks on classical proof systems: the hardness of quantum rewinding. In: 55th FOCS, pp. 474–483. IEEE Computer Society Press, October 2014. 554
7. Bai, S., Galbraith, S.D.: An improved compression technique for signatures based on learning with errors. In: Benaloh, J. (ed.) CT-RSA 2014. LNCS, vol. 8366, pp. 28–47. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-04852-9_2. 554, 558
8. Beals, R., Buhrman, H., Cleve, R., Mosca, M., Wolf, R.: Quantum lower bounds by polynomials. In: 39th FOCS, pp. 352–361. IEEE Computer Society Press, November 1998. 560
9. Bellare, M., Neven, G.: Multi-signatures in the plain public-key model and a general forking lemma. In: Juels, A., Wright, R.N., Vimercati, S. (eds.) ACM CCS 2006, pp. 390–399. ACM Press, October/November 2006. 553, 583
10. Bellare, M., Poettering, B., Stebila, D.: From identification to signatures, tightly: a framework and generic transforms. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part II. LNCS, vol. 10032, pp. 435–464. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53890-6_15. 556, 565
11. Bellare, M., Rogaway, P.: Random oracles are practical: a paradigm for designing efficient protocols. In: Ashby, V. (ed.) ACM CCS 1993, pp. 62–73. ACM Press, November 1993. 553, 560
12. Bennett, C.H., Bernstein, E., Brassard, G., Vazirani, U.V.: Strengths and weaknesses of quantum computing. SIAM J. Comput. **26**(5), 1510–1523 (1997). 554, 555
13. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 41–69. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_3. 554, 555, 560

14. Groot Bruinderink, L., Hülsing, A., Lange, T., Yarom, Y.: Flush, gauss, and reload – a cache attack on the BLISS lattice-based signature scheme. In: Gierlichs, B., Poschmann, A.Y. (eds.) CHES 2016. LNCS, vol. 9813, pp. 323–345. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53140-2_16. 555
15. Ducas, L., Durmus, A., Lepoint, T., Lyubashevsky, V.: Lattice signatures and bimodal Gaussians. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 40–56. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40041-4_3. 555
16. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS-Dilithium: a lattice-based digital signature scheme. IACR Trans. Cryptogr. Hardw. Embed. Syst. **2018**(1), 238–268 (2018). 554, 555, 557, 573, 575, 579, 580, 581, 582, 583
17. Ducas, L., Lyubashevsky, V., Prest, T.: Efficient identity-based encryption over NTRU lattices. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014, Part II. LNCS, vol. 8874, pp. 22–41. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45608-8_2. 555, 554
18. Eaton, E., Song, F.: Making existential-unforgeable signatures strongly unforgeable in the quantum random-oracle model. In: 10th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2015, Brussels, Belgium, pp. 147–162, 20–22 May 2015. 554
19. Espitau, T., Fouque, P., Gérard, B., Tibouchi, M.: Side-channel attacks on BLISS lattice-based signatures - exploiting branch tracing against strongSwan and electromagnetic emanations in microcontrollers. IACR Cryptology ePrint Archive 2017, 505 (2017). http://eprint.iacr.org/2017/505. 555
20. Fiat, A., Shamir, A.: How to prove yourself: practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987). https://doi.org/10.1007/3-540-47721-7_12. 553
21. Hülsing, A., Rijneveld, J., Song, F.: Mitigating multi-target attacks in hash-based signatures. In: Cheng, C.-M., Chung, K.-M., Persiano, G., Yang, B.-Y. (eds.) PKC 2016, Part I. LNCS, vol. 9614, pp. 387–416. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49384-7_15. 556, 561
22. Katz, J., Wang, N.: Efficiency improvements for signature schemes with tight security reductions. In: Jajodia, S., Atluri, V., Jaeger, T. (eds.) ACM CCS 2003, pp. 155–164. ACM Press, October 2003. 553, 578
23. Kawachi, A., Tanaka, K., Xagawa, K.: Concurrently secure identification schemes based on the worst-case hardness of lattice problems. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 372–389. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-89255-7_23. 554, 558
24. Kiltz, E., Masny, D., Pan, J.: Optimal security proofs for signatures from identification schemes. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part II. LNCS, vol. 9815, pp. 33–61. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53008-5_2. 554, 579
25. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Des. Codes Cryptogr. **75**(3), 565–599 (2015). 574, 582
26. Lyubashevsky, V.: Fiat-Shamir with aborts: applications to lattice and factoring-based signatures. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 598–616. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10366-7_35. 553, 554, 555, 557, 558, 566, 573

27. Lyubashevsky, V.: Lattice signatures without trapdoors. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 738–755. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_43. 583
28. Lyubashevsky, V., Micciancio, D.: Generalized compact knapsacks are collision resistant. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006, Part II. LNCS, vol. 4052, pp. 144–155. Springer, Heidelberg (2006). https://doi.org/10.1007/11787006_13. 582
29. Lyubashevsky, V., Neven, G.: One-shot verifiable encryption from lattices. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017, Part I. LNCS, vol. 10210, pp. 293–323. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56620-7_11. 557, 573
30. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_1. 574
31. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000). 560
32. Paillier, P., Vergnaud, D.: Discrete-log-based signatures may not be equivalent to discrete log. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 1–20. Springer, Heidelberg (2005). https://doi.org/10.1007/11593447_1. 553
33. Peikert, C., Rosen, A.: Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 145–166. Springer, Heidelberg (2006). https://doi.org/10.1007/11681878_8. 582
34. Pointcheval, D., Stern, J.: Security arguments for digital signatures and blind signatures. J. Cryptol. **13**(3), 361–396 (2000). 553, 554, 583
35. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) 37th ACM STOC, pp. 84–93. ACM Press, May 2005. 574
36. Unruh, D.: Non-interactive zero-knowledge proofs in the quantum random oracle model. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part II. LNCS, vol. 9057, pp. 755–784. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46803-6_25. 554, 558
37. Unruh, D.: Post-quantum security of Fiat-Shamir. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017, Part I. LNCS, vol. 10624, pp. 65–95. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70694-8_3. 555, 556, 558
38. Unruh, D.: Post-quantum security of fiat-shamir. Cryptology ePrint Archive, Report 2017/398 (2017). http://eprint.iacr.org/2017/398. 555, 558, 559
39. Zhandry, M.: How to construct quantum random functions. In: 53rd FOCS, pp. 679–687. IEEE Computer Society Press, October 2012. 561, 556
40. Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 758–775. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32009-5_44. 560