Quantum-Access Security of the Winternitz One-Time Signature Scheme

Christian Majenz
Centrum Wiskunde & Informatica and QuSoft, Amsterdam, The Netherlands

Chanelle Matadah Manfouo
African Institute for Mathematical Science & Quantum Leap Africa, Kigali, Rwanda

Maris Ozols
Institute for Logic, Language, and Computation, Korteweg-de Vries Institute for Mathematics, and Institute for Theoretical Physics, University of Amsterdam and QuSoft, Amsterdam, The Netherlands

Abstract

Quantum-access security, where an attacker is granted superposition access to secret-keyed functionalities, is a fundamental security model and its study has inspired results in post-quantum security. We revisit, and fill a gap in, the quantum-access security analysis of the Lamport one-time signature scheme (OTS) in the quantum random oracle model (QROM) by Alagic et al. (Eurocrypt 2020). We then go on to generalize the technique to the Winternitz OTS. Along the way, we develop a tool for the analysis of hash chains in the QROM based on the superposition oracle technique by Zhandry (Crypto 2019) which might be of independent interest.

2012 ACM Subject Classification Theory of computation → Quantum information theory; Security and privacy → Digital signatures; Security and privacy → Information-theoretic techniques

Keywords and phrases quantum cryptography, one-time signature schemes, quantum random oracle model, post-quantum cryptography, quantum world, hash-based signatures, information-theoretic security

Digital Object Identifier 10.4230/LIPIcs.ITC.2021.21

Related Version *Full Version*: `https://arxiv.org/abs/2103.12448` [23]

Funding *Christian Majenz*: NWO Veni grant (Project No. VI.Veni.192.159).
Chanelle Matadah Manfouo: NWO Gravitation grant QSC (Project No. 024.003.037) and AIMS-NEI.
Maris Ozols: NWO Vidi grant (Project No. VI.Vidi.192.109).

Acknowledgements The authors thank anonymous reviewers for insightful comments and Stacey Jeffery for helpful discussions. CMM deeply thanks the African Institute for Mathematical Sciences, Quantum Leap Africa Rwanda, and QuSoft Amsterdam for their support.

1 Overview

1.1 Introduction

Recently, research and development efforts towards building a universal quantum computer have intensified. As quantum computers will break currently deployed public-key cryptosystems [27], finding adequate replacement schemes (called *post-quantum* secure) has been increasingly a priority, too, as reflected by the ongoing NIST standardization effort for post-quantum secure digital signature schemes and key encapsulation mechanisms [1].

Quantum-access security. While post-quantum security is the most important attack model involving quantum computers, the stronger *quantum-access* or *quantum world* attack model [7, 13], where attackers are granted quantum access to secret-keyed functionalities,

2nd Conference on Information-Theoretic Cryptography (ITC 2021).
Editor: Stefano Tessaro; Article No. 21; pp. 21:1–21:22
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

has received considerable attention, too. There are a number of reasons why this stronger attack model is important. On the one hand, it is of theoretical importance because it captures the strongest-known achievable security notions for standard classical cryptographic primitives. On the other hand, there are a number of conceivable scenarios where they become relevant, e.g. for composability with obfuscation or when constructing quantum-cryptographic schemes, or to prevent implementation-level vulnerabilities in a future hybrid quantum-classical computing infrastructure. Finally, results in the quantum access model can inform post-quantum cryptographic research, as exemplified by the offline Simon's algorithm attack [8].

Blind unforgeability. In this work, we study the security of signature schemes under quantum-access attacks, in the quantum random oracle model (QROM) [6]. Here, generalizing the standard notion of existential unforgeability under chosen message attacks, the attacker is granted quantum query access to the signing algorithm. In the end, the adversary should output a forgery that they did not obtain from a query. Formalizing such a security notion is complicated due to the so-called *quantum no-cloning principle* according to which quantum states cannot be copied. We use the notion of blind unforgeability introduced in [2] (see [7, 15] for previous and complementary notions). We remark that the choice of the blind unforgeability definition is due to the fact that it implies the previous notions, which are the Boneh and Zhandry definition [7] and the one-time unforgeabilty [15], as established in [2]. Informally, blind unforgeability credits an adversary with a successful break of, e.g., a digital signature scheme, if it outputs a valid message-signature pair given a modified signing oracle that is "blinded" on a random subset of all messages, in the sense that it outputs a dummy symbol instead of a signature, and if the output message is among these blinded messages (see Section 2 for details).

Hash-based signature schemes. Hash-based signature schemes are prominent candidates for the replacement of digital signature schemes based on quantum-broken number-theoretic hardness assumptions. In particular, the stateful hash-based signature scheme XMSS [10] has been standardized as RFC8391 [19], and the stateless hash-based signature scheme SPHINCS+ [4] is an alternate candidate in the ongoing NIST standardization process for post-quantum cryptographic schemes [1]. The security of hash-based signature schemes can be based on weak computational assumptions, like e.g. the one-wayness of the underlying hash function. Common hash-based signature schemes, including the mentioned examples, are constructed using one-time[1] signature (OTS) schemes in combination with a hash-based authentication graph (e.g. a Merkle tree). The most well-known OTSs are the Lamport [21] and Winternitz [24] OTS. Variations of the latter are used in both XMSS and SPHINCS+.

Previous work. In [2], the Lamport OTS is studied in the context of blind-unforgeability. More precisely, a proof of one-time blind-unforgeability in the QROM is provided. That proof, however, has a gap in the analysis of the adversarial success. In particular, an auxiliary measurement is used to "collapse" an invariant property that holds *in superposition* into holding *classically*, but the effect of the dependence of this auxiliary measurement on the forgery message is not analyzed.

[1] And sometimes few-time signature schemes, e.g. in SPHINCS+.

Related work. Quantum-access security for encryption is an active research area, and generalizing chosen-ciphertext security notions to the quantum-access setting has posed, and poses, similar challenges as the ones encountered in the authenticity setting [7, 13, 14]. On the negative side, key recovery attacks in the quantum-access model against a number of symmetric-key primitives that are secure in the respective standard attack models have been discovered [26, 20], and have lead to the discovery of quantum attacks that can be performed without quantum access to secret-keyed functionalities [8].

There are a number of works that prove query lower bounds using variants of the superposition oracle technique [22, 17, 11, 5]. The last two papers prove query complexity lower bounds for creating hash chains, which are not directly useful for the analysis of hash-based signatures.

1.2 Summary of results

The Lamport OTS is blind-unforgeable. We revisit the analysis of the Lamport OTS in the QROM presented in [2] and give a complete proof of blind unforgeability as stated in the following theorem.

▶ **Theorem 1** (Blind unforgeability of the Lamport OTS, informal). *The Lamport OTS is blind-unforgeable if the underlying hash function h is modeled as a quantum-accessible random oracle. More precisely, the success probability of any blind unforgeability adversary $\mathcal{A}$ against the Lamport OTS that makes $q > 0$ quantum queries to the random oracle is bounded as*

$$\Pr[\mathcal{A} \text{ succeeds}] \le C_L q^2 l^3 \cdot 2^{-n},$$

where C_L is a constant, n is the security parameter of the Lamport OTS and l is the message length.

Compared to [2], our security proof features the following improvements:

- We streamline the usage of the superposition oracle technique of Zhandry [28]. In particular, our analysis only uses (a variant of) the superposition oracle technique to sample the secret key. We reprogram, *in superposition*, the standard random oracle at inputs contained in the secret key. This technique represents a general tool to analyze hash chains in the QROM and might be of independent interest.
- We give a full analysis of the success probability using an auxiliary measurement idea from [2]. To tackle the problem mentioned above, we introduce a novel technique of tracking an invariant property *in superposition* using projectors and commutators.

The Winternitz OTS is blind-unforgeable. With the full blind unforgeability analysis of the Lamport OTS in hand, we generalize the approach to the Winternitz OTS.

▶ **Theorem 2** (Blind unforgeability of the Winternitz OTS, informal). *The Winternitz OTS is blind-unforgeable if the underlying hash function h is modeled as a quantum-accessible random oracle. More precisely, the success probability of any blind unforgeability adversary $\mathcal{A}$ against the Winternitz OTS that makes $q > 0$ quantum queries to the random oracle is bounded as*

$$\Pr[\mathcal{A} \text{ succeeds}] \le C_W q^2 a^3 \frac{w^4}{\log^3 w} \cdot 2^{-n},$$

where C_W is a constant, n is the security parameter of the Winternitz OTS, a is the message length and $w \ge 2$ is the Winternitz parameter used to trade off signature size versus signing and verification time.

While the simplified analysis of hash chains in the QROM described above was advantageous in proving the blind unforgeability security of the Lamport OTS, it is indispensable in the analysis of the Winternitz scheme. Here, long hash chains are considered and the technique of using the superposition oracle to detect which hash chain elements are known to the adversary relies on the oracle register (or rather here: the hash chain register) being in a product state.

1.3 Technical overview

In this technical overview, we give a high-level description of our techniques for analyzing the blind unforgeability security of the Lamport and Winternitz OTSs in the QROM.

The superposition oracle technique and hash chains. As in many contexts that concern message authenticity and integrity, the main roadblock we have to overcome in our analysis is the so-called *recording barrier*: quantum oracle queries can, in general, not be recorded for later use. In particular, after a single quantum signing query, it is not possible to reason about the unused parts of the secret key. This is because, in general, all secret key strings have been used in some part of the superposition.

In [2], Zhandry's superposition oracle technique is used in a novel way to recover the ability to reason about which secret key strings are (un)known to the adversary. There, the secret key of the Lamport scheme, which is a $2 \times l$ array of independent uniformly random n-bit strings, is essentially regarded as a random function from $\{0,1\} \times \{1,\ldots,l\}$. This function, as well as the hash function the Lamport OTS is constructed from, is then modelled using the superposition oracle technique.

We improve this technique as follows. We use the fact that sampling two correlated random variables X and Y can be done by first sampling X, and then Y according to the conditional distribution, or vice versa. In the context of *hash chains* in the (Q)ROM, i.e. sequences of strings x_0, $x_1 = H(x_0)$, $x_2 = H(x_1)$, $\ldots$ for a random oracle H, this means that instead of sampling x_0 and H, and then computing the remaining hash chain elements, we can as well sample $x_0, x_1, \ldots$ from their joint distribution, sample H, and *reprogram H to be consistent with the x_i*. This allows us to i) change the distribution of the x_i to a simpler one that is close in total variational distance, and ii) refrain from using the full superposition oracle technique for H. In particular, we use i) to replace the hash chains that are generated by the key generation algorithms of the Lamport and Winternitz schemes by tuples of independent random strings. This incurs only a small error, as the uniform distribution and the distribution of a hash chain in the (Q)ROM with random starting value x_0 are equal conditioned on all x_i being distinct. But collisions between different hash chain elements are unlikely.

Now that the hash chain elements are independent strings, we can use the full power of the superposition oracle technique. In particular, the one-to-one correspondence between the adversary's ignorance of a hash chain element and the corresponding superposition oracle register being in uniform superposition, is restored.

Throughout the paper, and in the rest of this technical overview, we perform the analysis in a world where hash chains are formed using a superposition oracle modeling independent uniformly random strings, and the random oracle is reprogrammed accordingly. We call this the Quantum independent world. To conclude our analysis, we make use of the approximate indistinguishability of the Real and the Quantum independent world.

Blind unforgeability and classical invariants in superposition. With the tools for analyzing hash chains in the QROM in hand, the next challenge consists of generalizing the classical security arguments for the Blind Unforgeability (BU) of the Lamport and Winternitz OTSs to the quantum-access setting. The core of these security arguments is, at a high level, that for each unqueried message, any valid signature contains a string that is unknown to the adversary.[2] As mentioned above, this kind of reasoning does not generalize to the quantum-access setting, as here an adversary can query all messages in superposition.

In the security game for the notion of BU instead of the full signing oracle the adversary is provided with a modified oracle that is "blinded" on a random subset of messages, in the sense that for these messages it outputs a dummy symbol $\perp$ instead of a signature. These "blinded messages" can now replace the unqueried messages in security arguments, as by definition the adversary is prevented from obtaining a valid signature for them from the blinded signing oracle.

For obtaining a quantum generalization, we need to reformulate this argument. The statement that for each unqueried message any valid signature contains a string unknown to the adversary, is equivalent to saying that, for each fixed message m^* and all $m \neq m^*$, some information related to the secret key and not revealed by the signature of m is necessary to compute the signature for m^*. For BU, it suffices to consider blinded m^* and unblinded m. In the superposition oracle framework, the statement "there exists an unblinded message such that the registers corresponding to all parts of the secret key not revealed by that message are in the uniform superposition state" defines a subspace I. By definition, the global state after a BU-adversary makes a single query to the blinded signing oracle, and no queries to the random oracle, is in that subspace.

The crucial step in our analysis is to show that the joint adversary-oracle state approximately remains in the subspace I, even if the adversary performs a moderate number of quantum queries to the random oracle. This means the subspace I can serve as an *invariant*.

Random oracle queries and commutators. To analyze the "leakage" from the invariant subspace I, we use bounds on the norm of matrix commutators: to prove that the final oracle-adversary state is approximately in the invariant subspace I, we can equivalently show that applying the corresponding projector Π_I does not change the state by a lot. We know, however, that the projector does not change the state at all before any random oracle queries have been made. Therefore it suffices to bound the operator norm of the commutator between the projector Π_I and the unitary operator that facilitates random oracle queries in the Quantum independent world. We derive such a norm bound (see e.g. Lemma 15 for the Lamport case), and the proof follows the classical intuition about the one-wayness of the random oracle.

2 Preliminaries

We introduce some notation and conventions that will be used throughout the paper. Registers of quantum systems will be denoted by capital letters. We say that $\epsilon = \epsilon(n)$ is negligible if, for all polynomials $p(n)$, $\epsilon(n) < 1/p(n)$ for large enough $n \in \mathbb{N}$. We use the notation $x \overset{\$}{\leftarrow} D$ to say that x is chosen uniformly at random from a set D. We write S^c to denote the

[2] When basing the security on one-wayness, "unknown" is to be taken in a computational sense, but as this paper is about security in the (Q)ROM, it is sufficient to interpret "unknown to" as "independent of the state of".

complement of set S (in a superset that is clear from the context). We write $s \parallel t$ to denote the *concatenation* of strings s and t, and $[A, B] = AB - BA$ to denote the *commutator* of operators A and B. Throughout this paper, quantum adversaries refer to quantum polynomial-time algorithms and are denoted by $\mathcal{A}$.

Quantum computing. We use standard quantum computing notation, see e.g. [25]. A d-level quantum system is associated with a d-dimensional complex Euclidean space $\mathcal{H} = \mathbb{C}^d$ with inner product $\langle\cdot|\cdot\rangle$. We refer to the standard basis of $\mathbb{C}^d$ as the *computational basis*. The *state* of a system is described by a unit vector in $|\psi\rangle \in \mathcal{H}$, and $\langle\psi|$ denotes its dual vector. Given two quantum systems A and B, the composite system AB has state space equal to the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$. We will often refer to the subsystems A and B as *registers*. We denote the n-bit uniform superposition and the corresponding projector by

$$|\Phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle, \qquad\qquad \Phi = |\Phi\rangle\langle\Phi|. \tag{1}$$

Quantum computation proceeds by applying *unitary transformations*, i.e., complex $d \times d$ matrices U such that $UU^\dagger = I$, where $U^\dagger = \bar{U}^\mathsf{T}$ denotes the conjugate transpose of U. We omit tensor products with identity matrices, indicating which registers an operator acts on by subscripts, e.g. $U_A|\psi\rangle_{AB} = (U_A \otimes I_B)|\psi\rangle_{AB}$.

We can extract information from a quantum state $|\psi\rangle$ by performing a *measurement*. A (projective) measurement is described by a set $\{P_1, \dots, P_k\}$ of orthogonal projectors ($P_i^\dagger = P_i$ and $P_i^2 = P_i$) such that $\sum_{i=1}^k P_i = I$. When performing a measurement on a quantum state $|\psi\rangle$, the probability of getting outcome i is $p(i) = \langle\psi|P_i|\psi\rangle$. Upon getting outcome i, the state $|\psi\rangle$ collapses to $P_i|\psi\rangle/\sqrt{p(i)}$.

The standard way of modelling quantum black-box access to a function $f : \{0,1\}^n \to \{0,1\}^m$ is by providing an oracle for the unitary operation O_f that acts on $n + m$ qubits as $O_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ for all $x \in \{0,1\}^n$ and $y \in \{0,1\}^m$. Without loss of generality, an algorithm $\mathcal{A}$ that makes q queries to such an oracle has the form $U_q O_f \cdots U_1 O_f U_0 |\Psi_0\rangle = V_\mathcal{A}^{O_f}|\Psi_0\rangle = |\Psi\rangle$, possibly followed by a measurement. Here, $|\Psi_0\rangle$ is an initial state and U_i are arbitrary unitary operations that do not depend on f.

We will deal with algorithms that have two oracles, O_1 and O_2, but may only query O_2 at most once (O_1 will be a random oracle and O_2 a signing oracle for a one-time signature scheme). We can regard such an algorithm $\mathcal{A}^{O_1,O_2} = (\mathcal{A}_0^{O_1}, \mathcal{A}_1^{O_1})$ as a two-stage process: $\mathcal{A}_0^{O_1}$ prepares the input for O_2 and an internal register, $\mathcal{A}_1^{O_1}$ receives the internal state and the output of O_2, and produces the final output of $\mathcal{A}$, $|\Psi\rangle = V_{\mathcal{A}_1}^{O_1} O_2 V_{\mathcal{A}_0}^{O_1} |\Psi_0\rangle$.

The most well-known situation in cryptography that features a quantum oracle is the so-called *quantum random oracle model* (QROM) [6]. In the QROM, just as in the classical random oracle model (ROM) [3], a hash function is modeled as a uniformly random function h that all agents have oracle access to.

Tools from linear algebra. In this section, we state a couple of simple lemmas used in security proofs in Sections 4 and 5. For the first lemma, we use the formulation from [7] (Lemma 2.1), and the proof is also provided in the same reference.

▶ **Lemma 3** (Special case of the pinching lemma [18]). *Let $\mathcal{A}$ be a quantum algorithm and x any output value of $\mathcal{A}$. Let $\mathcal{A}_0$ be another quantum algorithm obtained from $\mathcal{A}$ by pausing $\mathcal{A}$ in an arbitrary stage of execution, performing a projective measurement that obtains one of k outcomes, and then resuming $\mathcal{A}$. Then,* $\Pr[\mathcal{A}_0(1^n) = x] \geq \Pr[\mathcal{A}(1^n) = x]/k$.

▶ **Lemma 4.** *Let A and $\{B_i\}_{i=1}^n$ be operators, acting on the same space, with $\|A\|_\infty, \|B_i\|_\infty \leq 1$. Then $\big\|[A, \prod_{i=1}^n B_i]\big\|_\infty \leq \sum_{i=1}^n \|[A, B_i]\|_\infty$.*

▶ **Lemma 5.** *Let X and Y be two n-qubit quantum systems and let $P_{XY}^{=} = \sum_{x\in\{0,1\}^n} |x\rangle\langle x|_X \otimes |x\rangle\langle x|_Y$ be the projector onto the subspace spanned by those computational basis vectors where the two registers are equal. Let $\Phi = |\Phi\rangle\langle\Phi|$ denote the projector onto the uniform superposition, see Equation* (1)*. Then $\|P_{XY}^{=}\Phi_Y\|_\infty = 2^{-n/2}$.*

By applying the triangle inequality, Lemma 5 implies $\|[P_{XY}^{=}, \Phi_Y]\|_\infty \leq 2 \cdot 2^{-n/2}$.

Hash-based one-time signature schemes. Hash-based signature schemes [21, 24] are digital signature schemes whose security relies on cryptographic hash functions. In this paper, we study hash-based one-time signatures (OTSs), i.e. schemes that use a pair of keys for a single message. Below we introduce the Lamport and Winternitz OTSs.

The **Lamport OTS** is the simplest hash-based OTS. It uses a hash function $h : \{0,1\}^n \to \{0,1\}^n$ for key generation and verification and is defined as follows:

1. *Parameters*: Security parameter $n \in \mathbb{N}$ and message length $l \in \mathbb{N}$.
2. *Key generation algorithm* (KeyGen): On receiving the security parameter n in unary, KeyGen outputs a secret signing key $\mathrm{sk} = (s_i^j)_{i=1,\ldots,l}^{j=0,1}$ with $s_i^j \xleftarrow{\$} \{0,1\}^n$ and a public verification key $\mathrm{pk} = (p_i^j)_{i=1,\ldots,l}^{j=0,1}$ where $p_i^j = h(s_i^j) \in \{0,1\}^n$.
3. *Signature algorithm* ($\mathsf{Sign}_{\mathrm{sk}}$): On input message $m = m_1 \ldots m_l \in \{0,1\}^l$ of length l, $\mathsf{Sign}_{\mathrm{sk}}$ outputs $\mathsf{Sign}_{\mathrm{sk}}(m) = \sigma = \sigma_1 \ldots \sigma_l$ where $\sigma_i = s_i^{m_i} \in \{0,1\}^n$.
4. *Verification procedure* ($\mathsf{Ver}_{\mathrm{pk}}$): Upon receiving a message m and a signature $\sigma = \sigma_1 \ldots \sigma_l$, $\mathsf{Ver}_{\mathrm{pk}}$ outputs `acc` if $h(\sigma_i) = p_i^{m_i}$ for all $i \in \{1, \ldots, l\}$, and `rej` otherwise.

The **Winternitz OTS** was introduced by Merkle [24]. In this work, we study a variant that uses a hash function $h : \{0,1\}^n \to \{0,1\}^n$ and is defined as follows:

1. *Parameters*: Security parameter n, binary message length a, and the Winternitz parameter $w \geq 2$. Based on parameters a and w we define

$$l_1 = \lceil a/\log(w)\rceil, \qquad l_2 = \lfloor \log(l_1(w-1))/\log(w)\rfloor + 1, \qquad l = l_1 + l_2. \tag{2}$$

2. *Key generation algorithm* (KeyGen): On receiving the security parameter n, choose uniformly at random l values that form the signing key $\mathrm{sk} = (s_1, \ldots, s_l) \xleftarrow{\$} (\{0,1\}^n)^l$. Then, compute the public verification key $\mathrm{pk} = (p_1, \ldots, p_l) = \big(h^{w-1}(s_1), \ldots, h^{w-1}(s_l)\big)$.
3. *Signature algorithm* ($\mathsf{Sign}_{\mathrm{sk}}$): For a given input message $x \in \{0,1\}^a$ and secret key sk, convert x to base w: $m = (b_1, \ldots, b_{l_1})$ where $b_i \in \{0, \ldots, w-1\}$. Next, compute the checksum $C(m) = \sum_{i=1}^{l_1}(w-1-b_i)$ and convert it to base w: $C(m) = (b_{l_1+1}, \ldots, b_l)$. The reader may refer to [12] for more details on the checksum. Then set $b(m) = (b_1, \ldots, b_l) = m \parallel C(m)$. The signature is then computed as $\sigma = (\sigma_1, \ldots, \sigma_l) = \big(h^{b_1}(s_1), \ldots, h^{b_l}(s_l)\big)$.
4. *Verification algorithm* ($\mathsf{Ver}_{\mathrm{pk}}$): Given input message m, signature σ and public verification key pk, compute $(b_1, \ldots, b_l)$ as described above and output `acc` if $h^{w-1-b_i}(\sigma_i) = p_i$ for all $i \in \{1, \ldots, l\}$, and `rej` otherwise.

Blind unforgeability. *Blind unforgeability* (BU) [2] is a quantum-access replacement for EU-CMA introduced in [16]. It uses the concept of *blinding*. Let $f : X \to Y$ be a function and $B \subset X$ a subset of X. The *blinded* function Bf with respect to the *blinding set* B is defined as $Bf(x) = \perp$ if $x \in B$ and $Bf(x) = f(x)$ otherwise, where $\perp$ is a special blinding symbol. One concrete way to instantiate this is by means of an extra bit: given a function $f : \{0,1\}^n \to \{0,1\}^m$, we define $Bf : \{0,1\}^n \to \{0,1\}^{m+1}$ by setting $\perp = 0^n \parallel 1$ and replacing $f(x)$ by $f(x)\|0$. We refer to B^c as the set of *unblinded* messages.

Let $S = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Ver})$ be a digital signature scheme with a security parameter n and message space M. Let $\mathcal{A}$ be an adversary and let $\epsilon : \mathbb{N} \to \mathbb{R}_+$ be a negligible function. We define the *blind forgery* experiment $\mathsf{BlindForge}_{S,\mathcal{A}}(n, \epsilon)$ as follows:

- *Key generation*: $(\mathrm{sk}, \mathrm{pk}) \leftarrow \mathsf{KeyGen}(1^n)$.
- *Generation of blinding set*: Select $B \subseteq M$ by choosing each $m \in M$ independently at random with probability $\epsilon(n)$ provided by the adversary $\mathcal{A}$.
- *Forgery*: $(m, \sigma) \leftarrow \mathcal{A}^{B\,\mathsf{Sign}_{\mathrm{sk}}}(1^n)$.
- *Outcome*: Win if $\mathsf{Ver}_{\mathrm{pk}}(m, \sigma) = \mathtt{acc}$ and $m \in B$, and lose otherwise.

▶ **Definition 6** (Blind unforgeability (BU))**.** *A digital signature scheme S is* q-BU secure *if for any adversary $\mathcal{A}$ making at most q queries to $B\,\mathsf{Sign}_{\mathrm{sk}}$ and for all ϵ, the success probability of winning the blind forgery experiment is negligible in the security parameter n.*

3 Hash chains in the QROM

3.1 Quantum hash chain sampling

In this section, we introduce hash chains and describe a technical tool consisting of modeling hash chains as independent uniform superposition states akin to Zhandry's compressed oracle technique [28]. This technique will enable us to prove BU security for the Lamport and Winternitz OTSs. *Hash chain* is a sequences of strings obtained by iteratively applying a hash function. They provide key pairs for the Lamport and Winternitz OTS'.

In the (Q)ROM, to generate a hash chain based on a hash function h, we first sample an initial string s_0 uniformly at random and then compute $s_i = h(s_{i-1})$ for $i = 1, \ldots, w-1$ to obtain a hash chain of length w. For key generation in the Lamport and Winternitz OTSs, the secret key sk is, respectively, a tuple of $2l$ and l initial strings sampled uniformly at random in the domain $\{0,1\}^n$. Then a tuple of hash chains $\gamma = (\gamma_i^j)_{i=1,\ldots,l}^{j=0,\ldots,w-1}$ is obtained by querying the hash function h on each string of the secret key $w-1$ times:

$$\gamma_i^0 = s_i, \quad \gamma_i^j = h^j(\gamma_i^0), \quad p_i = \gamma_i^{w-1} = h^{w-1}(\gamma_i^0), \quad j = 0, \ldots, w-1, \quad i = 1, \ldots, l,$$

where w is the length of the hash chain ($w = 2$ for Lamport) and l is the number of hash chains. The final entry of each chain is used as a public key.

In the $\mathsf{BlindForge}$ game, the secret key is only used by the blinded signing oracle. When analyzing this game, we can thus modify the key generation, signing and random oracle algorithms in an arbitrary way, as long as the modified triple is indistinguishable from the real one to an adversary.

In the proofs in Sections 4 and 5 we make use of the following modified triple, which we will refer to as defining the Quantum independent world. We construct the secret key and the intermediate hash chain elements initially in uniform superposition. That is, we prepare each hash chain register $(\Gamma_i^j)_{i=1,\ldots,l}^{j=0,\ldots,w-2}$ in the uniform superposition state $|\Phi\rangle$, with the intention of measuring them to sample the strings γ_i^j in mind. Then, we sample the final hash chain at random. The random oracle is then "reprogrammed in superposition" to be approximately consistent with the hash chains.

We proceed to show that the way of implementing the hash chain and the random oracle in the Real world and in the Quantum independent world are indistinguishable. For that purpose, we first formally define both worlds and some intermediate worlds between them. Each world is specified by two oracles, H and Sign, replacing the random oracle h and the signing oracle in the Real world (in each world, the KeyGen algorithm is implicitly replaced by the setup described below that generates the initial state and the public key). The oracles of the Quantum independent world are described below as well.

Real world. In the Real world, the first element γ_i^0 of each hash chain γ_i is generated at random and the hash function is evaluated to generate the rest of the hash chain, i.e., $\gamma_i^j = h^j(\gamma_i^0)$. Here, the random oracle is implemented at random, i.e. $H = h$, and the Sign oracle uses the secret key sk consisting of the γ_i^0.

Intermediate world 1. Here, the first hash chain element is generated at random and the following elements are successively sampled uniformly except for the collision tuples. That is $s_i = \gamma_i^0 \xleftarrow{\$} \{0,1\}^n$ and γ_i^1 is uniform except for the cases where $\gamma_i^1 = \gamma_{i'}^1$ if $\gamma_i^0 = \gamma_{i'}^0$; γ_i^2 is uniform except for the cases where $\gamma_i^2 = \gamma_{i'}^1$ if $\gamma_i^1 = \gamma_{i'}^0$; $\gamma_{i'}^2 = \gamma_i^2$ if $\gamma_i^1 = \gamma_{i'}^1$, etc. This world is very similar to the Real world, the only difference is that here we first sample the secret and public key (hash chain), then we reprogram the random oracle according to the secret and public key that we sampled, i.e. whenever the input to the random oracle is equal to a hash chain element γ_i^j with $j \leq w-2$, we return γ_i^{j+1}, otherwise answer with the actual random oracle. The Sign oracle is the same as in the Real world.

Intermediate world 2. In this world, the hash chain elements γ_i^j are first sampled uniformly at random with possible collision tuples. It means that the γ_i^j are uniformly independent strings. Afterwards, the random oracle is reprogrammed to be consistent with the secret and public keys. When queried, it compares the input with the hash chain. If the input is not equal to any of the hash chain elements, the oracle answers with a random function $\hat{h}$. Otherwise, for each hash chain element the input is equal to, it XORs the next hash chain element into the output register. If there are two hash chain elements that are the same, the random oracle XORs both following hash chain elements into the output register. In this case, the Sign oracle uses the full list of hash chains $(\gamma_i^j)_{i=1,\dots,l}^{j=0,\dots,w-1}$ to answer the query with all the hash chain elements consistent with the input.

Quantum independent world. In this world, the hash chain registers $(\Gamma_i^j)_{i=1,\dots,l}^{j=0,\dots,w-2}$ are initially prepared in the uniform superposition $|\Phi\rangle$, and the last hash chain elements $(\gamma_i^{w-1})_{i=1,\dots,l}$ are sampled uniformly at random. The random oracle is constructed in such a way that it is compatible with the hash chain. When queried with register X and Y, the random oracle compares the X and Γ registers, then answers the query in the Y register. Abstractly speaking, H is implemented as in the Intermediate world 2, except that the comparison and XOR operations involving γ_i^j are replaced by controlled unitary operations with Γ as the control register. It can be expanded as[3]

$$(U_h)_{XY\Gamma} = \left(\prod_{i=1}^{l}\prod_{j=0}^{w-2}(U_i^j)_{XY\Gamma_i^j\Gamma_i^{j+1}}\right)U_{XY\Gamma}^{\neq}, \tag{3}$$

where the unitaries U_{ij} apply CNOT from register Γ_i^{j+1} into Y, controlled on registers X and Γ_i^j being equal, and $U^{\neq}$ uses the actual random oracle in case X is not equal to any of the registers Γ_i^j. The signing oracle on the other hand just uses the superposition hash chain elements by means of a controlled unitary with control register Γ. For a detailed mathematical description, see the full version [23].

[3] Note that the ordering of the product is unimportant because the operators U_i^j commute.

3.2 Indistinguishability

The following lemma allows us to conclude the indistinguishability of the Real world and the Quantum independent world.

▶ **Lemma 7.** *Let p and q be output distributions over n-bit strings of an algorithm $\mathcal{A}$ interacting with the* Real *and the* Quantum independent world*, respectively. Then $\|p - q\|_1 \leq 3(wl)^2/2^n$.*

This lemma follows from the following three results (see the full version [23] for proofs).

▶ **Lemma 8.** *The* Real world *and the* Intermediate world 1 *are indistinguishable.*

▶ **Lemma 9.** *The distribution p and q of hash chains in the* Intermediate worlds 1 *and* 2 *are close: $\|p - q\|_1 \leq 3(wl)^2/2^n$.*

▶ **Lemma 10.** *The way the random oracle is implemented in the* Intermediate world 2 *and in the* Quantum independent world *are indistinguishable.*

4 One-time BU security of the Lamport OTS

In the BlindForge experiment, the adversary has quantum access to both a blinded signing oracle and a random oracle. For one-time signature schemes, the adversary is allowed only to query the signing oracle at most once. So, to produce a forged message-signature pair, the adversary can make a desired number of quantum queries to the random oracle, then query the signing oracle once, and then query again the random oracle as many times as desired. Our goal is to prove that the probability that an adversary outputs a correct forged signature on a valid forged message is negligible.

In the Lamport OTS, the signature algorithm uses only half of the secret key to produce the signature. Classically, the property that enables security is that the adversary does not have any information about the other half, the *invariant*, of the secret key. Quantumly, since in the BlindForge experiment the forged message must be outside the queried region, for any queried message there exists at least one bit in which the forged and queried messages differ. Thus, the secret key corresponding to that bit should still be in its initial state. To show blind-unforgeability, we separately analyze three cases: *hash queries before* Sign *query*, Sign *query*, and *hash queries after* Sign *query*. We describe below our proof strategy in these cases on a high level.

For *hash queries before* Sign *query*, we know that before any query the entire secret key is in uniform superposition. We therefore define a projector of the secret key register being in uniform superposition, and show that this projector approximately commutes with the random oracle unitary. This means that after a moderate number of queries, the secret key registers will still be in uniform superposition, indicating that the adversary learns almost no information about the secret key.

In the Sign *query* case, the first step is to track the unused part of the secret key. This part can be easily determined in the classical setting since the adversary queries only one message in each query. In contrast, in the quantum setting we consider quantum queries and hence have to track the invariant in superposition over the different queried messages. This is difficult because the invariant is different within each term of the superposition, so we cannot simply describe the invariant for the whole state. We address this problem as follows. We define an *invariant projector* that tracks the invariance of the unused superposition-secret-keys under queries and show that this projector is orthogonal to the projector corresponding to the outcome where *none of the secret key registers relevant to the forged signature belong to the invariant*. Then, we show that if there is only Sign query, this new projector does not change the adversary state immediately after the signature. We also establish that if the adversary state after forgery is in the range of this new projector, then the adversary has negligible probability to win the BlindForge game. Besides, we prove that the new projector approximately commutes with the random oracle unitary.

Finally, for the case of *hash queries after* Sign *query*, we use the latter argument of the commutator to prove that after hash queries the final adversary state remains roughly in the image of the invariant projector of the secret key.

The arguments from these three cases together constitute a proof of the following theorem.

▶ **Theorem 11.** *The Lamport OTS is 1-*BU *secure if the hash function h is modeled as a quantum-accessible random oracle. More precisely, let $\mathcal{A}$ be an adversary that plays the* BlindForge *game for the Lamport OTS, making a total of q queries to the random oracle. Then $\mathcal{A}$ succeeds with a probability bounded as*

$$\Pr[\mathcal{A} \textit{ wins } \mathsf{BlindForge}] \leq l^2 \cdot 2^{-n} \left(3137q^2(l+1) + 12\right) \leq 6286q^2l^3 \cdot 2^{-n}, \tag{4}$$

where n is the security parameter of the Lamport OTS, l is the message length, and the simplified bound holds for $q > 0$.

We present a proof of this result in subsequent sections. In particular, we prove it in the Quantum independent world first, and then conclude the statement in the Real world via an application of Lemma 7. In the remainder of the article, we use a subscript QI to indicate that a probability statement holds in the Quantum independent world.

4.1 Q measurement for Lamport OTS

We begin by presenting some concepts and tools which will be used in the proof. Subsequently, we prove the steps outlined above as separate lemmas. Our proof will make use of a projective measurement to track an invariant on the Quantum independent world secret key register for the verification of the forged message in the case of no hash queries. Let (m^*, σ^*) be a forged message-signature pair with $\sigma^* = s_1^{m_1^*} \cdots s_l^{m_l^*}$, where $(s_i^j)_{i=1,\ldots,l}^{j=0,1}$ is the secret key and l is the message length.

For any message $m^* \in \{0,1\}^l$ we define an $(l+1)$-outcome projective measurement that finds the smallest index $i^* \in \{1, \ldots, l\}$ for which the register $S_{i^*}^{m_{i^*}^*}$ *is in uniform superposition*, or determines that *none of the relevant secret key registers are in uniform superposition* (this corresponds to the outcome $l+1$). We define projectors $Q_{i^*}^{m^*}$ with $i^* \in \{1, \ldots, l\}$ in terms of projectors $\Phi = |\Phi\rangle\langle\Phi|$ and $\Phi^\perp = I - |\Phi\rangle\langle\Phi|$ placed onto different registers depending on the message m^* (they act as I on all other registers S_i^j that are not specified):

$$Q_{i^*}^{m^*} = \Phi^\perp_{S_1^{m_1^*}} \otimes \cdots \otimes \Phi^\perp_{S_{i^*-1}^{m_{i^*-1}^*}} \otimes \Phi_{S_{i^*}^{m_{i^*}^*}}, \qquad\qquad Q_{l+1}^{m^*} = \bigotimes_{i=1}^{l} \Phi^\perp_{S_i^{m_i^*}}. \tag{5}$$

4.2 Invariant projector

In this section we define a projector P_S that will be useful for our analysis, and state some of its properties as lemmas.

Let $\alpha = (\alpha_i^j)_{i=1,\ldots,l}^{j=0,1}$ be a $2l$-bit string whose each bit $\alpha_i^j \in \{0,1\}$ indicates that the projector $\Phi(\alpha_i^j)$ is applied on the corresponding secret key register S_i^j where $\Phi(0) = \Phi$ and $\Phi(1) = \Phi^\perp$. For each string α, we define the associated projector $\Phi(\alpha)$ on the whole secret key register S as $\Phi(\alpha)_S = \bigotimes_{i=1}^{l} \bigotimes_{j=0}^{1} \Phi(\alpha_i^j)_{S_i^j}$. Note that $\sum_{\alpha \in \{0,1\}^{2l}} \Phi(\alpha)_S = I_S$.

Since we are interested in the unused part of the secret key register S, we need to filter those α's for which S_i^j is in state $|\Phi\rangle$. Recall from our discussion of blind unforgeability in Section 2 that B denotes the set of blinded messages. Since the blinded signing oracle has signed (at most) a single, un-blinded message, the state after the oracle call can be written as a superposition of states where, for some un-blinded message $m \in B^c$, the secret key register of the complementary value $\bar{m}_i$ is still in the uniform superposition $|\Phi\rangle$, for all i. We collect all strings α that are consistent with no blinded messages having been signed in $\widehat{B^c} = \bigcup_{m \in B^c} \big\{\alpha \in \{0,1\}^{2l} \;\big|\; \alpha_i^{\bar{m}_i} = 0 \text{ for all } i = 1, \dots, l\big\}$. These strings indicate which secret key registers were not used during hash queries and Sign query. Finally, we define $P_S = \sum_{\alpha \in \widehat{B^c}} \Phi(\alpha)_S$ as the projector onto the subspace compatible with $\widehat{B^c}$. Note that P_S is indeed a projector since it is a sum of mutually orthogonal projectors.

We proceed to state several lemmas used to prove our main results both for the Lamport and Winternitz OTSs. Proofs of these lemmas are provided in the full version [23].

The first lemma says that hash queries do not affect the secret key registers significantly as long as they are in their initial state Φ.

▶ **Lemma 12.** *Let U_h be the random oracle unitary for any given function h (see Section 3) and let $\Phi = |\Phi\rangle\langle\Phi|$ denote the projector onto the uniform superposition. Then, for any $i \in \{1, \dots, l\}$ and $j \in \{0, 1\}$, $\big\|\big[U_h, \Phi_{S_i^j}\big]\big\|_\infty \le 6/2^{n/2} = \epsilon_L(n)$ is negligible in n.*

The quantum analogue of the following property holds: signing a message m^* requires at least one secret key string that was not used to sign $m \neq m'$.

▶ **Lemma 13.** *For all $m^* \in B$, the projectors $Q_{l+1}^{m^*}$ defined in Equation (5) and P_S are orthogonal.*

The projector P_S defined above is an invariant of the secret key registers after a signing query but no hash queries.

▶ **Lemma 14.** *Let $B\,\mathsf{Sign}_{\mathrm{sk}}$ be the blinded signing oracle for the Lamport OTS and let $|\psi_0\rangle$ be the adversary's state before the Sign query. If there are no hash queries, $P_S B\,\mathsf{Sign}_{\mathrm{sk}}\,|\psi_0\rangle = B\,\mathsf{Sign}_{\mathrm{sk}}\,|\psi_0\rangle$.*

The invariant specified by P_S approximately holds also after hash queries.

▶ **Lemma 15.** *The invariant projector P_S defined above and the random oracle unitary U_h defined in the $\mathsf{Quantum\ independent\ world}$ approximately commute, i.e., $\big\|[U_h, P_S]\big\|_\infty \le \delta_L(n)$, where $\delta_L(n) = 32l/2^{n/2}$ is negligible in n.*

In the following sections, we use the above lemmas to analyze the situation where the adversary makes q_0 hash queries before the Sign query and q_1 hash queries after. Maximizing the resulting bound under the condition $q_0 + q_1 = q$ gives Theorem 11.

4.3 Hash queries before Sign query

In this section, we study the impact of hash queries before Sign query on the secret key register S. Our main goal is to show that, for a moderate number of queries to the random oracle, no adversary can learn a significant amount of information about the secret key. Therefore, she cannot produce a valid forgery except with a small probability.

Let $|\psi\rangle_{XYM\Sigma E}$ be adversary's initial state before any queries (see Table 1 for a summary of registers and their roles). Before any query is performed, the whole secret key register S is in the uniform superposition state $|\Phi\rangle^{\otimes 2l}$. Assume the adversary $\mathcal{A}_0$ queries the random

Table 1 Registers used in the analysis.

Register	Meaning
X	adversary's input
Y	adversary's output
M	Sign query input
Σ	Sign query output
E	adversary's internal workspace
S	secret key

oracle q_0 times before querying the signing oracle. If V^i_{XYE} denotes the unitary she performs after the i-th query, the final adversary state after q_0 hash queries is

$$|\psi_0\rangle_{XYM\Sigma ES} = V^{q_0}_{XYE}(U_h)_{XYS}V^{q_0-1}_{XYE}\cdots V^2_{XYE}(U_h)_{XYS}V^1_{XYE}(U_h)_{XYS}|\psi\rangle_{XYM\Sigma E}|\Phi\rangle^{\otimes 2l}_S \tag{6}$$

where U_h is the random oracle unitary that answers hash queries. The following lemma shows that secret key registers of this state are still close to the uniform superposition.

▶ **Lemma 16.** *In the* Quantum independent world, *without querying the B* Sign *oracle, hash queries leave the state of the secret key registers approximately unchanged:*

$$\left\|\Phi^{\otimes 2l}_S|\psi_0\rangle_{XYM\Sigma ES} - |\psi_0\rangle_{XYM\Sigma ES}\right\|_2 \leq 2lq_0\epsilon_L(n).$$

Proof. We want to show that after q_0 hash queries, the state of the secret key register S is still approximately in the uniform superposition state $|\Phi\rangle^{\otimes 2l}$. Let us abbreviate the overall unitary in Equation (6) by W_{XYES}. Since the only operations in W_{XYES} that act on the S register are the hash queries U_h, and they are in fact controlled by the S register, we have $W_{XYES}\Phi^{\otimes 2l}_S = W_{XYES}$. Using this, we get

$$\begin{aligned}
&\left\|\Phi^{\otimes 2l}_S|\psi_0\rangle_{XYM\Sigma ES} - |\psi_0\rangle_{XYM\Sigma ES}\right\|_2 \\
&= \left\|\Phi^{\otimes 2l}_S W_{XYES}|\psi\rangle_{XYM\Sigma E}|\Phi\rangle^{\otimes 2l}_S - W_{XYES}\Phi^{\otimes 2l}_S|\psi\rangle_{XYM\Sigma E}|\Phi\rangle^{\otimes 2l}_S\right\|_2 && (7)\\
&= \left\|\left[\Phi^{\otimes 2l}_S, W_{XYES}\right]|\psi\rangle_{XYM\Sigma E}|\Phi\rangle^{\otimes 2l}_S\right\|_2 && (8)\\
&\leq \left\|\left[\Phi^{\otimes 2l}_S, W_{XYES}\right]\right\|_\infty \underbrace{\left\||\psi\rangle_{XYM\Sigma E}|\Phi\rangle^{\otimes 2l}_S\right\|_2}_{=1} && (9)\\
&= \left\|\left[\Phi^{\otimes 2l}_S, V^{q_0}_{XYE}(U_h)_{XYS}V^{q_0-1}_{XYE}\cdots V^2_{XYE}(U_h)_{XYS}V^1_{XYE}(U_h)_{XYS}\right]\right\|_\infty && (10)\\
&\leq q_0\left\|\left[\Phi^{\otimes 2l}_S, (U_h)_{XYS}\right]\right\|_\infty + \sum_{i=1}^{q_0}\left\|\left[\Phi^{\otimes 2l}_S, V^i_{XYE}\right]\right\|_\infty, && (11)
\end{aligned}$$

where Equation (9) follows from the definition of the operator norm and the last inequality follows from Lemma 4.

The first term in Equation (11) can be bounded as follows:

$$\left\|\left[\Phi^{\otimes 2l}_S, (U_h)_{XYS}\right]\right\|_\infty \leq \sum_{\substack{i\in\{1,\ldots,l\}\\ j\in\{0,1\}}}\left\|\left[\Phi_{S^j_i}, (U_h)_{XYS}\right]\right\|_\infty \leq 2l\epsilon_L(n),$$

which follows by first applying Lemma 4 and then Lemma 12. Since $\Phi^{\otimes 2l}_S$ and V^i_{XYE} act on different registers, they commute and the second term in Equation (11) vanishes. Hence

$$\left\|\Phi^{\otimes 2l}_S|\psi_0\rangle_{XYM\Sigma ES} - |\psi_0\rangle_{XYM\Sigma ES}\right\|_2 \leq 2lq_0\epsilon_L(n).$$ ◀

4.4 Query to the signing oracle

Now that we have control over the advantage an adversary can gain from making hash queries before the sign query, we need to analyze the possible advantage from hash queries after the sign query and bound the overall success probability using Lemma 16.

A crucial property of the Lamport OTS when analyzing classical security is that for all messages m that have not been queried, there exists an index j such that $s_j^{m_j}$ is hidden from the adversary by the one-wayness of the used hash function. In blind-unforgeability (for classical adversaries), this property holds for all *blinded messages.* In the setting of quantum queries, we have to track this property in superposition while the adversary is making hash queries after the sign query. As this is complicated by the "for all"-quantifier, we begin by analyzing the case where the adversary makes no hash queries after the sign query to ease the reader into our proof technique.

The discussion in this section does not concern the random oracle, so we absorb the random oracle query registers XY into E for the purpose of this section. In the 1-BlindForge game, an adversary $\mathcal{A}$ is allowed to query the Sign-oracle at most once to produce a valid forged message-signature pair (m^*, σ^*). To analyze the interaction between $\mathcal{A}$ and the signing oracle, we will break it into the following steps:

$$|\psi_0\rangle_{M\Sigma BES} \xmapsto{B\,\mathsf{Sign}_{\mathrm{sk}}} |\psi_1\rangle_{M\Sigma BES} \xmapsto{U_{M\Sigma E}} |\psi_2\rangle_{M\Sigma BES} \xmapsto{\langle m^*|_M} |\psi_3(m^*)\rangle_{\Sigma BES} \xmapsto{\langle \sigma^*|_\Sigma} |\psi_4(m^*,\sigma^*)\rangle_{BES}.$$

They correspond to applying the Sign-oracle and an arbitrary unitary $U_{M\Sigma E}$, followed by measuring the message and signature registers M and Σ. Let us now analyze these steps in more detail and write down the corresponding quantum states.

First, $\mathcal{A}$ prepares her input state as an arbitrary superposition of messages:

$$|\psi_0\rangle_{M\Sigma BES} = \left(\sum_{m\in\{0,1\}^l} \sum_{\sigma\in(\{0,1\}^n)^l} \sum_{b\in\{0,1\}} \kappa_{m\sigma b} |m\rangle_M |\sigma\rangle_\Sigma |b\rangle_B |\alpha_{m\sigma b}\rangle_E \right) \otimes \left(|\Phi\rangle^{\otimes 2l}\right)_S \tag{12}$$

where the B register indicates whether the message is blinded or not ($|1\rangle_B$ for blinded and $|0\rangle_B$ for un-blinded). The adversary then supplies this to the Sign oracle which produces the following signed state:

$$|\psi_1\rangle_{M\Sigma BES} = B\,\mathsf{Sign}_{\mathrm{sk}}\,|\psi_0\rangle_{M\Sigma BES} = |\psi_1^1\rangle_{M\Sigma BES} + |\psi_1^0\rangle_{M\Sigma BES} \tag{13}$$

where superscripts 1 and 0 refer to blinded (B) and un-blinded (B^c) messages, respectively:

$$|\psi_1^1\rangle_{M\Sigma BES} = \sum_{m\in B} \sum_{\sigma\in(\{0,1\}^n)^l} \kappa_{m\sigma 1} |m\rangle_M |\sigma\rangle_\Sigma |1\rangle_B |\alpha_{m\sigma 1}\rangle_E |\Phi\rangle_S^{\otimes 2l},$$

$$|\psi_1^0\rangle_{M\Sigma BES} = \sum_{m\in B^c} \sum_{\sigma\in(\{0,1\}^n)^l} \frac{1}{2^{nl/2}} \sum_{s\in(\{0,1\}^n)^l} \kappa_{m\sigma 0} |m\rangle_M |\sigma\oplus s\rangle_\Sigma |0\rangle_B |\alpha_{m\sigma 0}\rangle_E |\Omega(s,m)\rangle_S,$$

where $m = m_1 \dots m_l$, $\sigma = \sigma_1 \dots \sigma_l$, and

$$|\Omega(s,m)\rangle_S = |s_1^{m_1}\rangle_{S_1^{m_1}} \cdots |s_l^{m_l}\rangle_{S_l^{m_l}} |\Phi\rangle_{S_1^{\bar{m}_1}} \cdots |\Phi\rangle_{S_l^{\bar{m}_l}}. \tag{14}$$

Once the adversary $\mathcal{A}$ gets the signed state $|\psi_1\rangle_{M\Sigma BES}$, she performs some operations with the intention of producing a forgery message m^*. Intuitively, those operations can be considered as applying an arbitrary unitary $U_{M\Sigma E}$ to $|\psi_1\rangle_{M\Sigma BES}$. Let us denote the resulting state by $|\psi_2\rangle_{M\Sigma BES} = U_{M\Sigma E}|\psi_1\rangle_{M\Sigma BES}$.

Next, $\mathcal{A}$ measures the registers M and Σ to produce a forgery candidate (m^*, σ^*), collapsing the state to $|\psi_4(m^*, \sigma^*)\rangle_{BES} = \langle\sigma^*|_\Sigma|\psi_3(m^*)\rangle_{\Sigma BES} = \langle m^*|_M\langle\sigma^*|_\Sigma|\psi_2\rangle_{M\Sigma BES}$. Similar to Equation (13), we can split the final (unnormalized) post-measurement state as

$$|\psi_4(m^*, \sigma^*)\rangle_{BES} = |\psi_4^1(m^*, \sigma^*)\rangle_{BES} + |\psi_4^0(m^*, \sigma^*)\rangle_{BES}$$

where $|\psi_4^i(m^*, \sigma^*)\rangle_{BES} = \langle m^*|_M\langle\sigma^*|_\Sigma U_{M\Sigma E}|\psi_1^i\rangle_{M\Sigma BES}$. We can rewrite $|\psi_4^0\rangle_{BES}$ as

$$|\psi_4^0(m^*, \sigma^*)\rangle_{BES} = \sum_{m\in B^c} \frac{1}{2^{nl/2}} \sum_{s\in(\{0,1\}^n)^l} |\eta(m,s)\rangle_{BE}|\Omega(s,m)\rangle_S \tag{15}$$

where only $|\eta(m,s)\rangle_{BE}$ depends on m^* and σ^*:

$$|\eta(m,s)\rangle_{BE} = \sum_{\sigma\in(\{0,1\}^n)^l} \kappa_{m\sigma 0}\langle m^*|_M\langle\sigma^*|_\Sigma U_{M\Sigma E}|m\rangle_M|\sigma\oplus s\rangle_\Sigma|0\rangle_B|\alpha_{m\sigma 0}\rangle_E.$$

Finally, the adversary $\mathcal{A}$ outputs the measurement outcome (m^*, σ^*) as a forged message-signature pair. The probability of producing this pair is $\||\psi_4^0(m^*, \sigma^*)\rangle_{BES}\|^2$.

The next step is to analyse the probability that $\mathcal{A}$'s forgery candidate (m^*, σ^*) is correct. For that purpose, we consider two cases. The first case, namely when $m^* \notin B$, is trivial since then $\mathcal{A}$ has lost the BlindForge experiment because m^* must be blinded by definition. The rest of this section is devoted to analyzing the second case.

If $m^* \in B$, the forged message m^* has not been signed since the blinded signing oracle signs only un-blinded messages. Hence, for any message $m \notin B$, there exists at least one index $i \in \{1, \ldots, l\}$ such that $m_i \neq m_i^*$. This implies that for some index $i^* \in \{1, \ldots, l\}$ the register $S_{i^*}^{m_{i^*}^*}$ has not been used for the signature of the adversary's queried message and is therefore still in the uniform superposition state $|\Phi\rangle$. Note that this holds only in superposition over m. Indeed, i^* depends on m and is in general different for each term of the superposition.

We break that superposition by analyzing a modified BlindForge experiment, where an additional measurement, the *Q-measurement* defined in Equation (5), is performed on the secret key register after the adversary has output their forgery, but before the secret key register is measured to actually sample the secret key as required in the Quantum independent world. Since the measurement has few outcomes, its effect on the adversary's winning probability is limited and can be bounded by the pinching lemma (Lemma 3).

If the Q-measurement yields outcome $i^* \in \{1, \ldots, l\}$, then the secret key sub-register $S_{i^*}^{m_{i^*}}$ is in uniform superposition, and the adversary is bound to fail as σ^* is independent of the secret key string $s_{i^*}^{m_{i^*}}$ (the result of measuring $S_{i^*}^{m_{i^*}}$). Hence, it remains to analyze the outcome $l+1$ that corresponds to the projector $Q_{l+1}^m = (\Phi^\perp)^{\otimes l}$, see Equation (5), where $\Phi^\perp = I - |\Phi\rangle\langle\Phi|$ projects onto the orthogonal complement of $|\Phi\rangle$.

For the rest of our analysis, we fix the message m^* and focus on the un-blinded term $|\psi_4^0(m^*, \sigma^*)\rangle_{BES}$ whose expression is given by Equation (15). Given that for each $m \notin B$ there is at least one index $i \in \{1, \ldots, l\}$ such that $m_i \neq m_i^*$, we define $i(m) = \min\{j \in \{1, \ldots, l\} \mid m_j \neq m_j^*\}$ as the smallest index for which $m \neq m^*$. Intuitively, it is the first sub-register of S that still remains in uniform superposition. In the following, let $S(m) := S_1^{m_1} \cdots S_l^{m_l}$. We want to split the first sum in Equation (15) into l parts, one for each value of $i(m)$, so that we can easily evaluate $(\Phi^\perp)_{S(\bar{m})}^{\otimes l}|\psi_4^0(m^*, \sigma^*)\rangle_{BES}$. For that purpose, we define $B_j^c = \{m \in B^c \mid i(m) = j\}$ and note that $\bigcup_{j=1}^{l} B_j^c = B^c$. We can now rewrite $|\psi_4^0(m^*, \sigma^*)\rangle_{BES}$ as

$$\begin{aligned} |\psi_4^0(m^*, \sigma^*)\rangle_{BES} &= \sum_{j=1}^{l} \sum_{m \in B_j^c} \frac{1}{2^{nl/2}} \sum_{s \in (\{0,1\}^n)^l} |\eta(m, s)\rangle_{BE} |s^m\rangle_{S(m)} |\Phi\rangle_{S(\bar{m})}^{\otimes l} \\ &= \sum_{j=1}^{l} |\hat{\eta}(m^*, \sigma^*, j)\rangle_{BES_{\{(j, m_j^*)\}^c}} |\Phi\rangle_{S_j^{m_j^*}}, \end{aligned} \tag{16}$$

where we absorbed all registers except for $S_j^{m_j^*}$ into the first system. The remaining register $S_j^{m_j^*}$ is still in the uniform superposition $|\Phi\rangle$ since $j = i(m)$ is the smallest index such that $m_j \neq m_j^*$. Applying Q_{l+1} hence clearly maps the state to zero, and so the situation where none of the secret key sub-registers relevant for the verification of the forged signature σ^* is in state $|\Phi\rangle$ can ever occur.

Now, we execute the last part of the BlindForge experiment which consists of checking the correctness of the forged signature σ^*. For this purpose, we perform a computational basis measurement on the entire secret key register S to sample the strings s_i^j. As mentioned above, the probability of (m^*, σ^*) being valid is at most 2^{-n} as $s_i^{m_i}$ is independent of σ_i^*, where i is the outcome of the Q-measurement. Applying the pinching lemma (Lemma 3) to relate the success probabilities with and without Q-measurement, and Lemma 7 for $w = 2$ to relate the success probabilities in the Real world and the Quantum independent world (see details in the full version [23]), we arrive at

$$\Pr\left[\mathcal{A} \text{ wins } \mathsf{BlindForge}\right] \leq \frac{l+1}{2^n} + 12l^2 \cdot 2^{-n}. \tag{17}$$

Hence, the success probability of the adversary $\mathcal{A}$ in winning the BlindForge experiment game is at most $(l+1)/2^n$, which is negligible since l is polynomial in n, and n is large enough. We conclude that a Sign query does not help the adversary to get significant information about the secret key.

4.5 Hash queries after Sign query

To complete the proof of Theorem 11 and bound the success probability an adversary can achieve in the BlindForge game with a given number of queries, it remains to analyse *hash queries after* Sign *query*. In this case, it is not obvious how to track the secret key invariant (the fact that there is at least one unused part of the secret key that is relevant for the forged signature). Therefore we use a special projector P_S that projects onto the subspace of the secret key register that is consistent with a single blinded sign query and no hash queries. If the final adversary state after producing the forgery candidate is in the image of P_S, then according to Lemma 13 the outcome $l + 1$ corresponding to the situation when *none of the secret key sub-registers useful for the forged signature is in state* $|\Phi\rangle$ can never occur. We thus want to show that adversary's final state is approximately in the range of P_S.

If there are no hash queries before the Sign query, then from Lemma 14 the adversary state after the Sign query remains completely in the range of P_S, which means that the outcome $l + 1$ cannot occur. That is, $P_S|\psi_1\rangle = P_S B\, \mathsf{Sign}_{\mathrm{sk}}\, |\psi_0\rangle = B\, \mathsf{Sign}_{\mathrm{sk}}\, |\psi_0\rangle = |\psi_1\rangle$ where $|\psi_0\rangle$ and $|\psi_1\rangle$ are adversary's states immediately before and after the Sign query.

Now, assuming there are hash queries before the Sign query, since the projector P_S and the random oracle unitary U_h approximately commute by Lemma 15, it follows that hash queries before Sign query give no significant information to the adversary about the invariant of the secret key register.

Suppose there are hash queries after the Sign query and let us examine in detail what happen in this case. From the previous case, we know that the adversary's state directly after the Sign query is $|\psi_1\rangle_{M\Sigma XYES}$. Just like for hash queries before the Sign query, suppose that the adversary makes q_1 hash queries after querying the signing oracle. Let $(W^i_{XYE})_{i=1,\ldots,q_1}$ be the unitaries applied between the hash queries. Then, let

$$|\psi_1'\rangle_{M\Sigma XYES} = (U_h)_{XYS}W^{q_1}_{XYE}(U_h)_{XYS}W^{q_1-1}_{XYE}\cdots W^2_{XYE}(U_h)_{XYS}W^1_{XYE}|\psi_1\rangle_{M\Sigma XYES}$$

be the adversary's state after q_1 hash queries and before performing some unitary operation $U_{M\Sigma E}$ on the post-hash-queried state, or any measurement leading to the forgery candidate.

▶ **Lemma 17.** *In the* Quantum independent world*, the state* $|\psi_1'\rangle_{M\Sigma XYES}$ *right before the adversary's measurement determining the forgery is applied is approximately in the range of* P_S*:*

$$\left\|P_S|\psi_1'\rangle_{M\Sigma XYES} - |\psi_1'\rangle_{M\Sigma XYES}\right\|_2 \leq q_1\delta_L(n) + 4lq_1\epsilon_L(n) = q_1(\delta_L(n) + 4l\epsilon_L(n)). \quad (18)$$

The proof uses commutator arguments via Lemma 15 akin to the ones used in the proof of Lemma 16, and can be found in the full version [23].

Recall that, just like in Section 4.4, we want to analyze the modified BlindForge experiment where the Q-measurement is applied after the adversary has output a forgery, but before the secret key register is measured to sample the secret key and verify the forgery. It thus remains to show that due to the fact that $|\psi_1'\rangle$ is approximately in the range of P_S, the outcome $l+1$ only occurs with small probability.

To that end, we define a new measurement given by projectors $\tilde{Q}_i$ that performs the Q-measurement controlled on the content of the M-register, i.e., $\tilde{Q}_i = \sum_m |m\rangle\langle m|_M \otimes Q_i^m$. Now, observe that applying the Q-measurement after the adversary has output a forgery is equivalent to applying the $\tilde{Q}$-measurement right before the adversary's measurement that produces the forgery. If $m^* \in B$, the outcome $l+1$ occurs only with small probability in the modified BlindForge experiment and it suffices to prove the following lemma.

▶ **Lemma 18.** *In the* Quantum independent world*, for blinded messages, the outcome* $l+1$ *occurs with small probability:* $\left\|\tilde{Q}_{l+1}\Pi^B_M|\psi_1'\rangle_{M\Sigma XYES}\right\|_2 \leq q_1(\delta_L(n) + 4l\epsilon_L(n))$*,* $\Pi^B = \sum_{m\in B}|m\rangle\langle m|$*.*

The proof is a simple application of Lemma 13 and can be found in the full version [23]. We are now ready to combine our lemmas and prove Theorem 11.

Proof of Theorem 11. We begin by bounding the success probability of the adversary in the modified BlindForge experiment, in the Quantum independent world. Abbreviating the modified BlindForge experiment as MBF and writing "outcome i" to denote the event that the Q-measurement yields outcome i,

$$\begin{aligned}
&\Pr_{QI,MBF}[\mathcal{A}\text{ succeeds}] = \sum_{i=1}^{l+1}\Pr_{QI,MBF}[\mathcal{A}\text{ succeeds} \wedge \text{outcome } i] \\
&= \sum_{i=1}^{l}\Pr_{QI,MBF}[\mathcal{A}\text{ succeeds} \wedge \text{outcome } i] + \Pr_{QI,MBF}[\mathcal{A}\text{ succeeds} \wedge \text{outcome } l+1] \\
&\leq \sum_{i=1}^{l}\Pr_{QI,MBF}[\text{outcome } i] \times 2^{-n} + \Pr_{QI,MBF}[\text{outcome } l+1] \leq 2^{-n} + q^2(\delta_L(n) + 4l\epsilon_L(n))^2,
\end{aligned}$$

where the first inequality uses the fact that σ^* and $s_i^{m_i^*}$ are independent conditioned on outcome i, and the last inequality uses the square of the inequality from Lemma 18.

Exactly as in the simplified case in Section 4.4, we can bound the success probability in the actual BlindForge experiment using the pinching lemma (Lemma 3):

$$\Pr_{QI,\mathsf{BlindForge}}[\mathcal{A} \text{ succeeds}] \leq (l+1)\left(2^{-n} + q^2\left(\delta_L(n) + 4l\epsilon_L(n)\right)^2\right).$$

Finally, plugging in the functions $\epsilon_L(n)$ and $\delta_L(n)$ from Lemmas 12 and 15, and applying Lemma 7 for $w = 2$, we obtain

$$\begin{aligned}\Pr_{\mathsf{BlindForge}}[\mathcal{A} \text{ succeeds}] &\leq (l+1)\left(2^{-n} + q^2\left(\frac{32l}{2^{n/2}} + 4l\frac{6}{2^{n/2}}\right)^2\right) + 12l^2 2^{-n}\\ &\leq l^2 \cdot 2^{-n}\left(3137q^2(l+1) + 12\right). \end{aligned}$$ ◀

5 One-time BU security of the Winternitz OTS

The Lamport OTS that we analyzed in the last section is, in some sense, a special case of the Winternitz OTS. Indeed, the Winternitz scheme for $w = 2$ is fairly similar to the Lamport OTS, except that the public key is used to sign the bits that are equal to 1, which is compensated for by the checksum encoding. As a result, the analysis of the Winternitz OTS in the QROM is, in a similar sense, a generalization of the one of the Lamport OTS.

Before getting started, we give and overview of our strategy. In this section, we use the same register labels as in Table 1, except that the secret key register S is now replaced by the hash chain register Γ. The security proof follows a similar outline as in the Lamport case. Some differences are as follows. After a Winternitz signing query, the adversary does not have any information about the part of the hash chain below the queried position, and this represents the invariant of the hash chain. Quantumly, this invariant has to be tracked in superposition like for the Lamport scheme, requiring the definition of a new and slightly more involved invariant projector (see details in the full version [23]).

▶ **Theorem 19.** *The Winternitz OTS is 1-*BU *secure if the function chain $\mathcal{C}$ is modeled as a quantum-accessible random oracle. More precisely, let $\mathcal{A}$ be an adversary that plays the* BlindForge *game for the Winternitz OTS, making a total of q queries to the random oracle. Then $\mathcal{A}$ succeeds with a probability bounded as*

$$\begin{aligned}\Pr[\mathcal{A} \textit{ wins } \mathsf{BlindForge}] &\leq 2^{-n}\left[\left(1 + q^2l^2(w-1)^2(20w-4)^2\right)(l+1) + 3w^2l^2\right] && (19)\\ &\leq 800w^4q^2l^3 \cdot 2^{-n}. && (20)\end{aligned}$$

Here, l is the length of the encoded message in w-ary, see Equation (2)*, $w \geq 2$ is the Winternitz parameter, and the simplified bound in the last line holds for $q > 0$.*

The main difference between the analyses of the Lamport and Winternitz OTS is as follows. For the Lamport OTS, the public key is obtained from the private key by applying a hash function once. For the Winternitz OTS, on the other hand, the secret and public keys consist of the start and end points of length-w hash chains, respectively. Thus, while following the same proof strategy, the Q projectors as well as the invariant projector P needs to be defined differently. Thus, we start our analysis by describing the Q projectors and the invariant projector for the Winternitz OTS.

The Q-measurement for the Winternitz OTS. The Winternitz signature of a message consists of l hash chain elements. In complete analogy to Equation (5) in Section 4.1, we define a measurement whose projectors correspond, respectively, to the events that *the i-th hash chain element relevant for the forged signature is in state $|\Phi\rangle$* and *none of them is in state $|\Phi\rangle$*:

$$Q^{b^*}_{i^*} = \Phi^{\perp}_{\Gamma_1^{b_1^*}} \otimes \cdots \otimes \Phi^{\perp}_{\Gamma_{i^*-1}^{b^*_{i^*-1}}} \otimes \Phi_{\Gamma_{i^*}^{b^*_{i^*}}}, \qquad Q^{b^*}_{l+1} = \bigotimes_{i=1}^{l} \Phi^{\perp}_{\Gamma_i^{b_i^*}} \tag{21}$$

where $i^* \in \{1, \ldots, l\}$, $b_i^* = b_i(m^*)$ and l is the number of blocks of the message and the checksum, see Equation (2). These operators act as I on all other registers Γ_i^j not specified.

The Invariant projector for the Winternitz OTS. In this section, we define the invariant projector P_Γ, the analogue of P_S for the Winternitz OTS. We also state several of its properties. Just like in Section 4.2, for any string $\alpha = (\alpha_i^j)_{i=1,\ldots,l}^{j=0,\ldots,w-2}$ we define an associated projector $\Phi(\alpha)$ on the whole hash chain (except for the last) register Γ. This is a complete set of projectors: $\sum_{\alpha \in \{0,1\}^{l(w-1)}} \Phi(\alpha)_\Gamma = I_\Gamma$.

Since we are interested in the unused part of the hash chain register, we need to filter those α's for which Γ_i^j is in state $|\Phi\rangle$. By construction of the checksum, if a block b of a message m is computed, then in the block b' of any other message m' there exists at least one position i at which $b'_i < b_i$, $1 \le i \le l$. Therefore, since the blinded signing oracle signs at most a single un-blinded message $m \in B^c$, the state after the signing oracle call can be written as a superposition of states where, for some un-blinded message $m' \in B^c$, $b'_i < b_i$ for all i. The latter implies that the hash chain registers corresponding to those b'_i are still in the uniform superposition $|\Phi\rangle$, for all i. Thus, we collect all strings α that are consistent with no blinded messages having been signed in the set

$$\widehat{B^c} = \bigcup_{m \in B^c} \left\{ \alpha \in \{0,1\}^{l(w-1)} \;\middle|\; \alpha_i^j = 0 \text{ for all } i = 1, \ldots, l \text{ and } j < b_i(m) \right\}. \tag{22}$$

Finally, we define the invariant projector as $P_\Gamma = \sum_{\alpha \in \widehat{B^c}} \Phi(\alpha)_\Gamma$.

Using these definitions of the Q_i and P_Γ, a set of lemmas similar to Lemmas 12–15 forms the basis of the BU security proof for the Winternitz OTS. In fact, Lemma 12 is a special case of Lemma 20 where the register Γ is replaced by S and we set $w = 2$ (see Appendix A.1 of [23] for proof). Lemma 13 holds for the new projectors Q_{l+1} and P_Γ by construction. Finally, Lemmas 14 and 15 need to be changed slightly for the Winternitz OTS and are stated below. Lemmas 21–23 are proved in the full version [23].

▶ **Lemma 20.** *Let U_h be the random oracle unitary for any given function h (see Section 3) and let $\Phi = |\Phi\rangle\langle\Phi|$ denote the projector onto the uniform superposition $|\Phi\rangle$. Furthermore, let $\Gamma_i^{\le j} = \Gamma_i^0 \ldots \Gamma_i^j$ and $\Phi_{\Gamma_i^{\le j}} = \left(\Phi^{\otimes j}\right)_{\Gamma_i^{\le j}}$. Then, for any $i' \in \{1, \ldots, l\}$ and $j' \in \{0, \ldots, w-2\}$, $\left\| \left[(U_h)_{XY\Gamma}, \Phi_{\Gamma_{i'}^{\le j'}} \right] \right\|_\infty \le 6(w-1)/2^{n/2} = \epsilon_W(n)$ is negligible in n.*

▶ **Lemma 21.** *Let $B\,\mathsf{Sign}_{\mathsf{sk}}$ be the blinded signing oracle for the Winternitz OTS, and let $|\psi_0\rangle$ be the adversary's state before the* Sign *query. If there are no hash queries, then after making a single* Sign *query the adversary's state $|\psi_1\rangle = B\,\mathsf{Sign}_{\mathsf{sk}}\,|\psi_0\rangle$ is completely in the range of the invariant projector P_Γ defined below Equation (22). That is, $P_\Gamma B\,\mathsf{Sign}_{\mathsf{sk}}\,|\psi_0\rangle = B\,\mathsf{Sign}_{\mathsf{sk}}\,|\psi_0\rangle$.*

▶ **Lemma 22.** *Let $m^* \in B$ and $b^* = b(m^*)$ the concatenation of m^* and its checksum in w-ary. Then the projectors $Q^{b^*}_{l+1}$ defined in Equation (21) and P_Γ are orthogonal, that is $Q^{b^*}_{l+1} P_\Gamma = 0$.*

▶ **Lemma 23.** *Let P_Γ and U_h be, respectively, the invariant projector for the Winternitz OTS and the random oracle unitary defined with respect to the* Quantum independent world*. If there are hash queries after the* Sign *query, then $\left\|[U_h, P_\Gamma]\right\|_\infty \leq \delta_W(n)$ where $\delta_W(n) = 8l(w+1)(w-1)/2^{n/2}$.*

The proof of Theorem 19 is based on the preceding lemmas and follows the same outline as the proof for the Lamport OTS. It can be found in the full version [23].

6 Tightness

The notion of blind-unforgeability does not have as close of a relation to the intuitive security property it strives to model as EU-CMA.[4] The concrete security bounds, however, arguably nevertheless provide an indication of concrete security levels. It is hence an interesting question whether the bounds proven in Section 4 above and in Section 5 of the full version [23] are tight. In the following, we present an attack against the BU security of the Lamport scheme in the QROM and analyze its success probability to show that the bound in Theorem 11 is tight up to a factor l in the number of queries. The attack generalizes to the Winternitz scheme in a straight-forward manner.

We begin by describing a straightforward classical attack based on search. To attack the BU security of the Lamport scheme, choose a blinding probability of 1/2. Now make q distinct queries to the random oracle to search for a preimage of one of the $2l$ public key strings. This succeeds with probability

$$p_{\text{search}}(q) = 1 - (1 - 2l \cdot 2^{-n})^q \geq 2ql \cdot 2^{-n}. \tag{23}$$

Suppose this search succeeded, finding a preimage y^* of $p_{i^*}^{j^*}$. Then chose $m \in \{0,1\}^l$ such that $m_{i^*} = \bar{j}^*$ and query the oracle to obtain a signature for m. This succeeds with probability 1/2. Now output m' obtained from m by flipping the i^*th bit, and σ' obtained from σ by replacing σ_{i^*} with y^*. Note that m' is blinded with probability 1/2, and y^* is equal to the correct secret key string $s_{i^*}^{j^*}$ with constant probability. In summary, the entire attack succeeds with constant probability if $q = \Omega(2^n \cdot l^{-1})$.

This search step can now be replaced by a Grover search in the QROM. Using the analysis of Grover's algorithm for multiple targets from [9], together with a basic analysis of the number of targets (which follows a binomial distribution), a constant success probability can be achieved if $q = \Omega(2^{n/2} \cdot l^{-1/2})$. To compare this result with Theorem 11, note that the inequality in Equation (4), implies that to achieve a constant success probability, at least $q \geq C \cdot 2^{n/2} \cdot l^{-3/2}$ are necessary for some constant C, i.e. the upper and lower bounds on the number of queries the optimal attack requires indeed differ by a factor of l up to constant factors. For the Winternitz scheme, the bounds differ by a factor of $w^2 l$.

References

1 Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, et al. Status report on the second round of the NIST post-quantum cryptography standardization process. *US Department of Commerce, NIST*, 2020. doi:10.6028/NIST.IR.8309.

[4] Indeed, it is a nice exercise to show that an adversary against (say, q-time) EU-CMA with success probability ϵ can be used to construct a BU-adversary with success probability $\Theta(\epsilon/q)$, and this reduction is tight for efficient adversaries if one-way functions exists.

2 Gorjan Alagic, Christian Majenz, Alexander Russell, and Fang Song. Quantum-access-secure message authentication via blind-unforgeability. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 788–817. Springer, 2020. doi:10.1007/978-3-030-45727-3_27.

3 Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM conference on Computer and communications security*, pages 62–73. ACM, 1993. doi:10.1145/168588.168596.

4 Daniel J. Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe. The SPHINCS+ signature framework. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS'19, pages 2129–2146, New York, NY, USA, 2019. Association for Computing Machinery. doi:10.1145/3319535.3363229.

5 Jeremiah Blocki, Seunghoon Lee, and Samson Zhou. On the security of proofs of sequential work in a post-quantum world, 2020. arXiv:2006.10972.

6 Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 41–69. Springer, 2011. doi:10.1007/978-3-642-25385-0_3.

7 Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013*, pages 361–379, Berlin, Heidelberg, 2013. Springer. doi:10.1007/978-3-642-40084-1_21.

8 Xavier Bonnetain, Akinori Hosoyamada, María Naya-Plasencia, Yu Sasaki, and André Schrottenloher. Quantum attacks without superposition queries: The offline Simon's algorithm. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019*, pages 552–583, Cham, 2019. Springer. doi:10.1007/978-3-030-34578-5_20.

9 Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum cryptanalysis of hash and claw-free functions. In Cláudio L. Lucchesi and Arnaldo V. Moura, editors, *LATIN'98: Theoretical Informatics*, pages 163–169, Berlin, Heidelberg, 1998. Springer. doi:10.1007/BFb0054319.

10 Johannes Buchmann, Erik Dahmen, and Andreas Hülsing. XMSS - a practical forward secure signature scheme based on minimal security assumptions. In Bo-Yin Yang, editor, *Post-Quantum Cryptography*, pages 117–129, Berlin, Heidelberg, 2011. Springer. doi:10.1007/978-3-642-25405-5_8.

11 Kai-Min Chung, Serge Fehr, Yu-Hsuan Huang, and Tai-Ning Liao. On the compressed-oracle technique, and post-quantum security of proofs of sequential work, 2020. arXiv:2010.11658.

12 Shimon Even, Oded Goldreich, and Silvio Micali. On-line/off-line digital signatures. *Journal of Cryptology*, 9(1):35–67, 1996. doi:10.1007/0-387-34805-0_24.

13 Tommaso Gagliardoni, Andreas Hülsing, and Christian Schaffner. Semantic security and indistinguishability in the quantum world. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016*, pages 60–89, Berlin, Heidelberg, 2016. Springer. doi:10.1007/978-3-662-53015-3_3.

14 Tommaso Gagliardoni, Juliane Krämer, and Patrick Struck. Quantum indistinguishability for public key encryption, 2020. arXiv:2003.00578.

15 Sumegha Garg, Henry Yuen, and Mark Zhandry. New security notions and feasibility results for authentication of quantum data. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017*, pages 342–371, Cham, 2017. Springer. doi:10.1007/978-3-319-63715-0_12.

16 Shafi Goldwasser, Silvio Micali, and Ronald L Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on computing*, 17(2):281–308, 1988. doi:10.1137/0217017.

17 Alex B. Grilo, Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz. Tight adaptive reprogramming in the QROM, 2020. arXiv:2010.15103.

18 Masahito Hayashi. Optimal sequence of quantum measurements in the sense of Stein's lemma in quantum hypothesis testing. *Journal of Physics A: Mathematical and General*, 35(50):10759, 2002. doi:10.1088/0305-4470/35/50/307.

19 Andreas Hülsing, Denise Butin, Stefan-Lukas Gazdag, Joost Rijneveld, and Aziz Mohaisen. XMSS: Extended hash-based signatures. RFC 8391, 2018. doi:10.17487/RFC8391.

20 Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016*, pages 207–237, Berlin, Heidelberg, 2016. Springer. doi:10.1007/978-3-662-53008-5_8.

21 Leslie Lamport. Constructing digital signatures from a one way function. Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, 1979. URL: http://lamport.azurewebsites.net/pubs/dig-sig.pdf.

22 Qipeng Liu and Mark Zhandry. On finding quantum multi-collisions. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 189–218, Cham, 2019. Springer. doi:10.1007/978-3-030-17659-4_7.

23 Christian Majenz, Chanelle Matadah Manfouo, and Maris Ozols. Quantum-access security of the Winternitz one-time signature scheme, 2021. arXiv:2103.12448.

24 Ralph C. Merkle. A certified digital signature. In *Conference on the Theory and Application of Cryptology*, pages 218–238. Springer, 1989. doi:10.1007/0-387-34805-0_21.

25 Michael A. Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002. doi:10.1023/A:1012603118140.

26 Thomas Santoli and Christian Schaffner. Using Simon's algorithm to attack symmetric-key cryptographic primitives. *Quantum Info. Comput.*, 17(1–2):65–78, 2017. doi:10.26421/QIC17.1-2-4.

27 Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. IEEE, 1994. doi:10.1109/SFCS.1994.365700.

28 Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019*, pages 239–268, Cham, 2019. Springer. doi:10.1007/978-3-030-26951-7_9.