Quantum-access security of the Winternitz one-time signature scheme

Christian Majenz[1], Chanelle Matadah Manfouo[2] and Maris Ozols[3]

[1] Centrum Wiskunde & Informatica and QuSoft, The Netherlands
[2] African Institute for Mathematical Science & Quantum Leap Africa, Rwanda
[3] Institute for Logic, Language, and Computation, Korteweg-de Vries Institute for Mathematics, and Institute for Theoretical Physics, University of Amsterdam and QuSoft, The Netherlands

arXiv:2103.12448

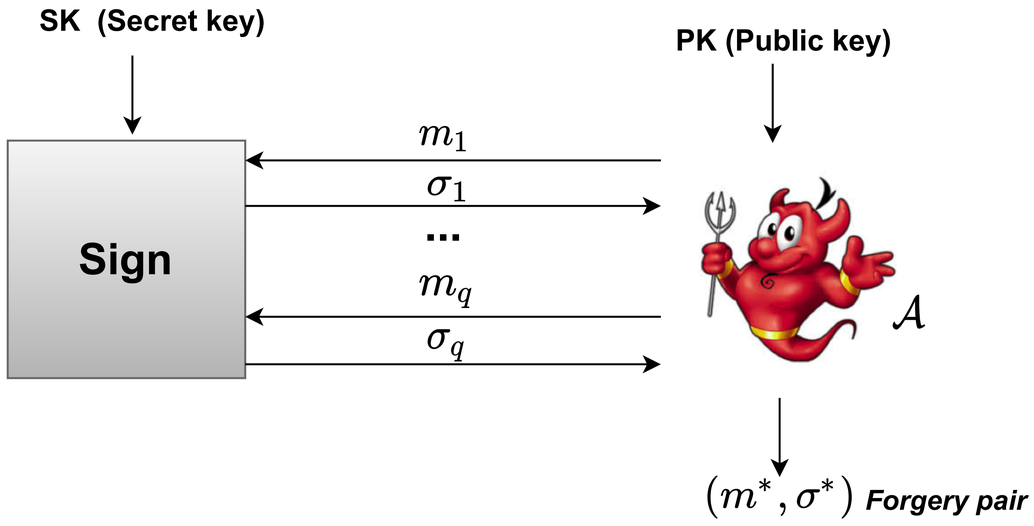
Abstract

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.

Security of digital signature schemes

Digital signature scheme $S = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Ver})$, triple of polynomial time algorithms

Classical security: **Forge game**



Adversary $\mathcal{A}$ wins if $m^* \neq m_i$ for all $i \in \{1, \ldots, q\}$ and $\mathsf{Sign}_{\mathrm{sk}}(m^*) = \sigma^*$.

Definition 1 (Existential Unforgeability under adaptative Chosen Message Attack (EU-CMA))**.** *A digital signature scheme is* EU-CMA *secure if no adversary can win the forge game with non-negligible probability.*

Quantum security?

The adversary queries in superposition and the forgery pair is classical.

Several problems:

- No-cloning prevents the signer from keeping a record of the queried messages and that of their corresponding signatures.
- Difficulty to distinguish queried messages and forged message.
- Measure to compare $\Rightarrow$ disturbance!

A promising approach: Blind Unforgeability (generalization of EU-CMA to quantum adversaries)

- Grant an adversary with a Sign oracle blinded in a subset B of the message space, i.e.,

$$B\,\mathsf{Sign}_{\mathrm{sk}}(m) = \begin{cases} \perp & \text{if } m \in B, \\ \mathsf{Sign}_{\mathrm{sk}}(m) & \text{otherwise} \end{cases}$$

  where $\perp$ is the *blinding symbol*
- Ask the adversary to forge in the blinded region

Under this approach, an adversary wins the previous forge game for quantum queries if $m^* \in B$ and $\mathsf{Sign}_{\mathrm{sk}}(m^*) = \sigma^*$ for classical pair (m^*, σ^*).

Prior work, our work, and motivation

Prior work: Alagic et al. [1] analyzed the security of the Lamport One-time Signature (OTS) in the quantum random oracle model (QROM) based on the blind-unforgeability definition. More precisely, a proof of one-time blind-unforgeability in the QROM is provided.

Our work: In this work, we generalize the approach in [1] to prove the security of the Winternitz OTS when an adversary has both quantum access to the signing oracle, and to a random oracle. In our variant of the Winternitz OTS, the KeyGen routine computes the pair of keys as a *hash chain*, i.e. sequences of strings obtained by iteratively applying a hash function, where the head is the secret key and the tail, the public key.

Motivation: With the development of quantum computers, it becomes increasingly important to analyze the security of cryptographic protocols against quantum adversaries.

Our main results

Blind unforgeability of the Lamport OTS

We revisit the analysis of the Lamport OTS in the QROM presented in [1] and give a complete proof of blind unforgeability, i.e.,

Theorem 2 (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* $\Pr[\mathcal{A} \text{ succeeds}] \leq C_L q^2 l^3 \cdot 2^{-n}$,
where C_L is a constant, n is the security parameter of the Lamport OTS and l is the message length.

Compared to [1], our security proof features the following improvements:

- We make use of the superposition oracle technique of Zhandry [2]. In particular, we uses (a variant of) the superposition oracle technique to sample the secret key, and reprogram *in superposition*, the standard random oracle at inputs contained in the secret key.
- We give a full analysis of the adversarial success probability considering the impact of the auxiliary measurement (idea from [1]).

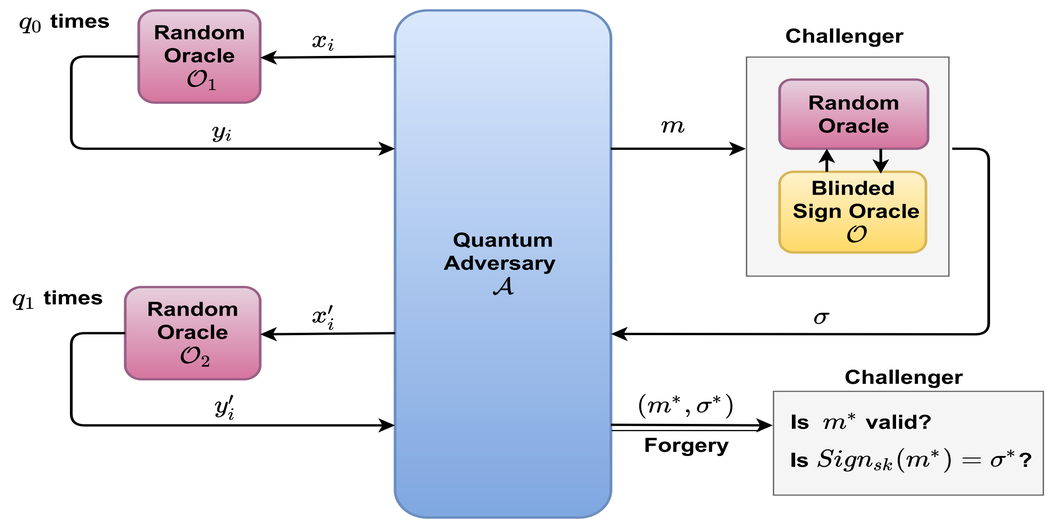
Blind unforgeability of the Winternitz OTS

Theorem 3 (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*

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

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

Overview of the technique



Outline of the Proof

Construct our Quantum independent world for our analysis

1. Develop the superposition hash chain
   - Prepare the secret key and all the intermediate hash chain elements initially in uniform superposition state $|\Phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$
   - Sample each string of the public key (tail of the hash chain) uniformly at random in the domain $\{0,1\}^n$.
   - Reprogram the standard random oracle in superposition
2. Modify the Random oracle and signing oracle algorithms with respect to the new hash chain.

We show that our ideal world and the Real world are indistinguishable, i.e.,

Lemma 4. *Let p and q be the output distributions over n-bit strings of an algorithm $\mathcal{A}$ interacting with the* Real world *and the* Quantum independent world*, respectively. Then* $\left\|p - q\right\|_1 \leq \frac{3(wl)^2}{2^n}$.

Examine the adversarial success probability

- We show that the final adversary-oracle state is approximately unchanged.
  $\Rightarrow$ the adversary learns insignificant information about the hash chain, thus it has negligible probability to produce a valid forgery pair.

References

[1] 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.

[2] 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.