33. Josef Pieprzyk, Huaxiong Wang, and Chaoping Xing. Multiple-time signature schemes against adaptive chosen message attacks. In Mitsuru Matsui and Robert Zuccherato, editors, Selected Areas in Cryptography, volume 3006 of LNCS, pages 88–100. Springer, 2004.
34. Leonid Reyzin and Natan Reyzin. Better than BiBa: Short one-time signatures with fast signing and verifying. In Lynn Batten and Jennifer Seberry, editors, Information Security and Privacy 2002 , volume 2384 of LNCS, pages 1–47. Springer, 2002.
35. Fang Song. A note on quantum security for post-quantum cryptography. In Michele Mosca, editor, Post-Quantum Cryptography , volume 8772 of LNCS, pages 246–265. Springer, 2014.
36. Kazuhiro Suzuki, Dongvu Tonien, Kaoru Kurosawa, and Koji Toyota. Birthday paradox for multi-collisions. In Min Rhee and Byoungcheon Lee, editors, Information Security and Cryptology ICISC 2006 , volume 4296 of LNCS, pages 29–40. Springer, 2006.

A Security Properties

In this appendix we give the basic definitions for security properties we use.

Existential Unforgeability under Adaptive Chosen Message Attacks. The standard security notion for digital signature schemes is existential unforgeability under adaptive chosen message attacks (EU-CMA) [24] which is defined using the following experiment. By $\text{Dss}(1^n)$ we denote a signature scheme with security parameter n.

Experiment $\mathsf{Exp}^{\text{EU-CMA}}_{\text{Dss}(1^n)}(\mathcal{A})$
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{kg}(1^n)$
$(M^\star, \sigma^\star) \leftarrow \mathcal{A}^{\mathsf{sign}(\mathsf{sk},\cdot)}(\mathsf{pk})$
Let $\{(M_i, \sigma_i)\}_1^q$ be the query-answer pairs of $\mathsf{sign}(\mathsf{sk}, \cdot)$.
Return 1 iff $\mathsf{vf}(\mathsf{pk}, M^\star, \sigma^\star) = 1$ and $M^\star \notin \{M_i\}_1^q$.

A signature scheme is called existentially unforgeable under a q adaptive chosen message attack if any PPT adversary making at most q queries, has only negligible success probability in winning the above game.

An EU-CMA secure one-time signature scheme (OTS) is a signature scheme that is existentially unforgeable under a 1-adaptively chosen message attack.

Hash Function Families. We now provide definitions of the security properties of hash function families that we use, namely one-wayness, second-preimage resistance, undetectability and pseudorandomness. In the following let $n \in \mathsf{N}$ be the security parameter, $m, k = \text{poly}(n)$, $\mathcal{H}_n = \{\text{H}_K : \{0,1\}^m \to \{0,1\}^n \mid K \in \{0,1\}^k\}$ a family of functions. (In the description of SPHINCS we actually omit the key K in many cases for readability.)

We define the security properties in terms of the success probability of an adversary $\mathcal{A}$ against the respective property. A function family $\mathcal{H}_n$ is said to provide a property if the success probability of any probabilistic polynomial-time adversary against this property is negligible. We begin with the success

probability of an adversary $\mathcal{A}$ against the one-wayness (OW) of a function family $\mathcal{H}_n$.

$$\mathrm{Succ}^{\mathrm{OW}}_{\mathcal{H}_n}(\mathcal{A}) = \mathsf{Pr}\left[\, K \xleftarrow{\$} \{0,1\}^k; M \xleftarrow{\$} \{0,1\}^m, Y \leftarrow \mathrm{H}_K(M), \right.$$
$$\left. M' \leftarrow \mathcal{A}(K,Y) : Y = \mathrm{H}_K(M') \right] .$$

We next define the success probability of an adversary $\mathcal{A}$ against second-preimage resistance (SPR).

$$\mathrm{Succ}^{\mathrm{SPR}}_{\mathcal{H}_n}(\mathcal{A}) = \mathsf{Pr}\left[\, K \xleftarrow{\$} \{0,1\}^k; M \xleftarrow{\$} \{0,1\}^m, M' \leftarrow \mathcal{A}(K,M) : \right.$$
$$\left. (M = M') \wedge (\mathrm{H}_K(M) = \mathrm{H}_K(M')) \right] .$$

To define undetectability, assume the following two distributions over $\{0,1\}^n \times \{0,1\}^k$. A sample (U,K) from the first distribution $\mathcal{D}_{\mathrm{UD},\mathcal{U}}$ is obtained by sampling $U \xleftarrow{\$} \{0,1\}^n$ and $K \xleftarrow{\$} \{0,1\}^k$ uniformly at random from the respective domains. A sample (U,K) from the second distribution $\mathcal{D}_{\mathrm{UD},\mathcal{H}}$ is obtained by sampling $K \xleftarrow{\$} \{0,1\}^k$ and then evaluating H_K on a uniformly random bit string, i.e., $\mathcal{U}_m \xleftarrow{\$} \{0,1\}^m, U \leftarrow \mathrm{H}_K(\mathcal{U}_m)$. The success probability of an adversary $\mathcal{A}$ against the undetectability of $\mathcal{H}_n$ is defined as:

$$\mathrm{Succ}^{\mathrm{UD}}_{\mathcal{H}_n}(\mathcal{A}) = \left| \mathsf{Pr}[\mathcal{A}^{\mathcal{D}_{\mathrm{UD},\mathcal{U}}} = 1] - \mathsf{Pr}[\mathcal{A}^{\mathcal{D}_{\mathrm{UD},\mathcal{H}}} = 1] \right| ,$$

where $\mathcal{A}^{\mathrm{dist}}$ denotes that $\mathcal{A}$ has oracle access to some oracle that outputs samples from distribution dist.

The fourth notion we use is pseudorandomness of a function family (PRF). In the definition of the success probability of an adversary against pseudorandomness the adversary gets black-box access to an oracle Box. Box is either initialized with a function from $\mathcal{H}_n$ or a function from the set $\mathcal{G}(m,n)$ of all functions with domain $\{0,1\}^m$ and range $\{0,1\}^n$. The goal of the adversary is to distinguish both cases:

$$\mathrm{Succ}^{\mathrm{PRF}}_{\mathcal{H}_n}(\mathcal{A}) = \left| \mathsf{Pr}[\mathsf{Box} \xleftarrow{\$} \mathcal{H}_n : \mathcal{A}^{\mathsf{Box}(\cdot)} = 1] - \mathsf{Pr}[\mathsf{Box} \xleftarrow{\$} \mathcal{G}(m,n) : \mathcal{A}^{\mathsf{Box}(\cdot)} = 1] \right| .$$

Subset-Resilient Functions. We now recall the definition of subset resilience from [34]. Let $\mathcal{H} = \{\mathrm{H}_{i,t,k}\}$ be a family of functions, where $\mathrm{H}_{i,t,k}$ maps a bit string of arbitrary length to an subset of size at most k of the set $[t-1]$. (As for hash functions in the description of SPHINCS we omit the key and assume the used function is randomly selected from a family using the uniform distribution.) Moreover, assume that there is a polynomial-time algorithm that, given $i, 1^t, 1^k$ and M, computes $\mathrm{H}_{i,t,k}(M)$. Then $\mathcal{H}$ is called γ-subset resilient if the following success probability is negligible for any probabilistic polynomial-time adversary $\mathcal{A}$:

$$\mathrm{Succ}^{\gamma\text{-sr}}_{\mathcal{H}}(\mathcal{A}) = \mathsf{Pr}_i\Big[(M_1, M_2, \ldots, M_{\gamma+1}) \leftarrow \mathcal{A}(i, 1^t, 1^k)$$
$$\text{s.t. } \mathrm{H}_{i,t,k}(M_{\gamma+1}) \subseteq \bigcup_{j=1}^{\gamma} \mathrm{H}_{i,t,k}(M_j)\Big]$$