Recovering the tight security proof of SPHINCS+

Kudinov Mikhail
joint work with Andreas Hülsing

December 7, 2022

Outline

SPHINCS$^+$

- Hash-based post-quantum signature scheme;
- Only requires a secure hash function;
- Chosen for standardization by NIST.

NIST IR 8413-upd1 Third Round Status Report

Table 4. Algorithms to be Standardized

Public-Key Encryption/KEMs	**Digital Signatures**
CRYSTALS–KYBER	CRYSTALS–Dilithium
	FALCON
	SPHINCS$^+$

Table 5. Candidates advancing to the Fourth Round

Public-Key Encryption/KEMs	**Digital Signatures**
BIKE	
Classic McEliece	
HQC	
SIKE	

Security flaw

- During third round of the NIST competition a flaw in the proof of security was found.
- The flaw did not lead to an attack;
- A non tight proof was applicable ($\sim$60 bits of security loss);

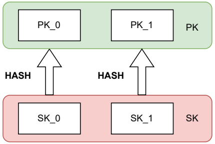
From:	pqc-forum@list.nist.gov on behalf of Mikhail Kudinov <mkudinov@qapp.tech>
Sent:	Thursday, July 23, 2020 11:10 AM
To:	pqc-forum
Subject:	[pqc-forum] ROUND 3 OFFICIAL COMMENT: SPHINCS+

Dear all,

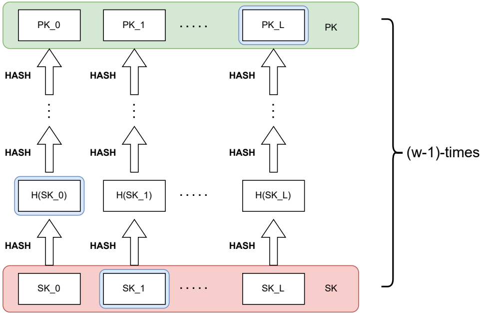
In this comment, we would like to point out a flaw of existing security proofs of the SPHINCS+ hash-based scheme. Particularly, we would like to pay attention to security proofs of the underlying WOTS+ scheme with preimage resistance (PRE) requirement replaced by second preimage resistance (SPR) + “at least two preimages for every image” requirements [see eq. (14) in Round 2 submission] or decisional second preimage resistance (DSPR) + SPR requirements [see Bernstein et al. “The SPHINCS+ signature framework” 2019].

Building blocks: OTS

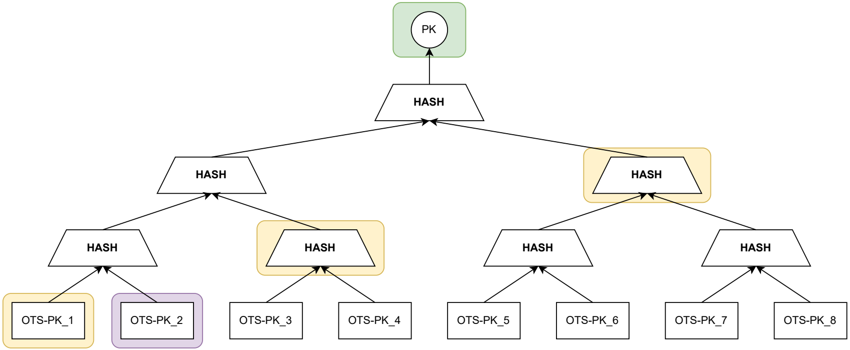
Lamport One-time signature
1-bit



Winternitz One-time signature
n-bit

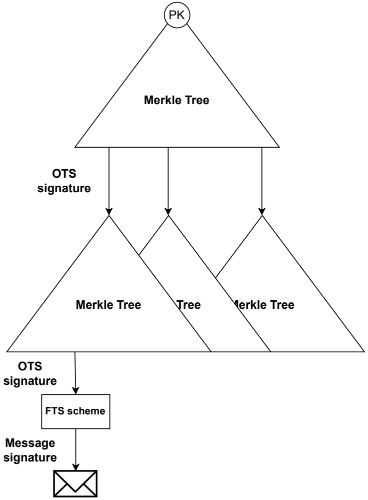


Building blocks: Merkle Tree



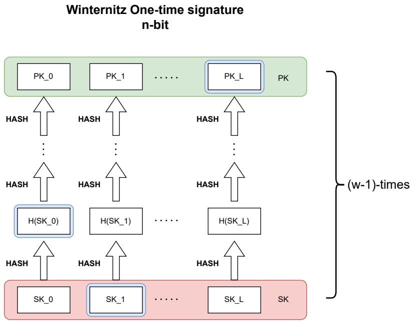
SPHINCS+ construction

- Multiple layers of Merkle trees;
- Last layer used for signing messages;
- The last layer uses Winternitz OTS (WOTS) to sign few-time signature scheme (FTS) public key, which then used to sign the message.
- The signature contains a FTS signature, WOTS signatures and authentication paths for each layer.



Security flaw

- During third round of the NIST competition a flaw in the proof of security was found.
- The flaw was in the security of WOTS;
- The flaw did not lead to an attack;
- A non tight proof was applicable ($\sim$60 bits of security loss);



Preliminaries

Definition 1 (Tweakable hash function). *Let $n, m \in \mathbb{N}$, $\mathcal{P}$ the public parameters space and $\mathcal{T}$ the tweak space. A tweakable hash function is an efficient function*

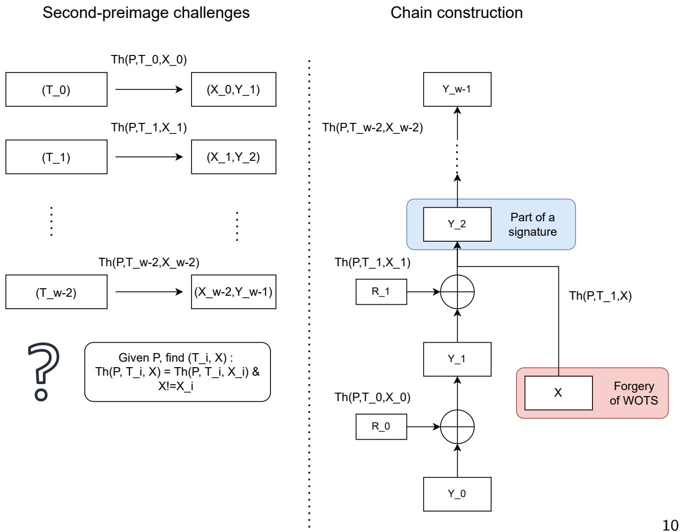
$$\mathbf{Th} : \mathcal{P} \times \mathcal{T} \times \{0,1\}^m \to \{0,1\}^n, \ \mathrm{MD} \leftarrow \mathbf{Th}(P, T, M)$$

mapping an m-bit message M to an n-bit hash value MD *using a function key called public parameter $P \in \mathcal{P}$ and a tweak $T \in \mathcal{T}$.*

- Same public parameter for every **Th** call
- Different Tweak for every **Th** call
- Mitigation of multi-target attacks
- Multi-user security

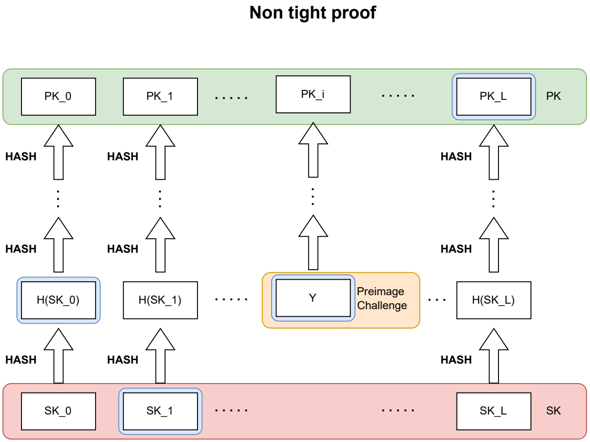
Intuition behind the flaw

- $\mathbf{Th}(P, T, X) = y$:
  X is information-theoretically hidden among all preimages of y;
- $\mathbf{Th}(P, T, X) = y$, where $X = \mathbf{Th}(P, T', X')$:
  X is not information-theoretically hidden among all preimages of y.



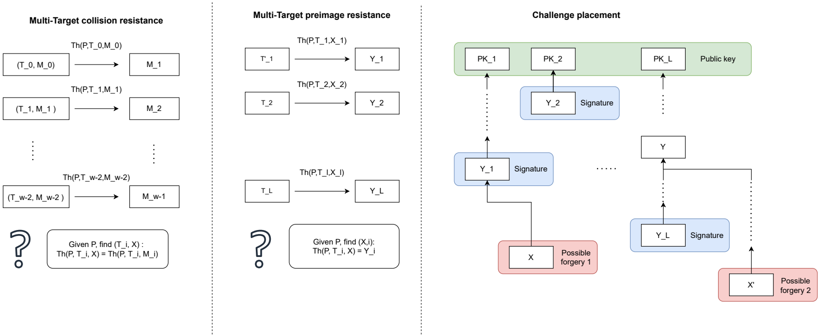
Recovering the security: Non tight proof

- Not knowing the message we have to guess a position for preimage placement.
- Probability of good placement: $\frac{1}{lw}$
- Having 2^h WOTS instances makes it $\frac{1}{2^h \cdot l \cdot w}$



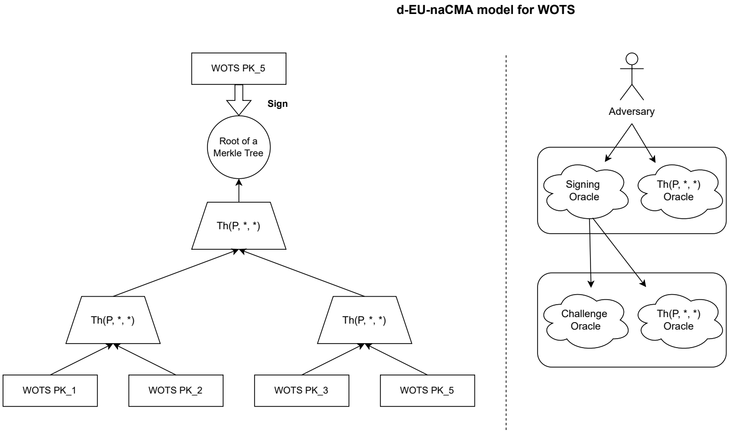
Recovering the security: new proof

- **Key observation**: Only EU-naCMA security of WOTS is necessary, which means that the reduction knows the message when preparing the public key;
- We either break PRE or TCR;
- We need undetectability to deal with the change in the distribution.



Dealing with multiple instances of WOTS

- Since we have to do all the challenge queries before obtaining the public parameter we use $\mathbf{Th}_\lambda$ oracle;
- The adversary is not allowed to query $\mathbf{Th}_\lambda$ with tweaks corresponding to the WOTS instances.
- The signing oracle queries the challenge oracle and $\mathbf{Th}_\lambda$, but can not query $\mathbf{Th}_\lambda$ with the tweaks used for the challenge queries



Final theorems

Theorem 2. *Let n, $w \in \mathbb{N}$ and $w = poly(n)$. Let $\mathbf{F} := \mathbf{Th}_1 : \mathcal{P} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ be a* SM-TCR, SM-PRE, SM-UD THF *as a member of a collection. Let $\mathbf{PRF} : \mathcal{S} \times \mathcal{T} \to \{0,1\}^n$ be a* KHF*. Then the following inequality holds:*

$$\begin{aligned}\mathrm{InSec}^{\text{d-EU-naCMA}}(\text{WOTS-TW}; t, d) < \\ \mathrm{InSec}^{\mathrm{PRF}}(\mathbf{PRF}; \widetilde{t}, d \cdot l) + \mathrm{InSec}^{\mathrm{SM\text{-}TCR}}(\mathbf{F} \in \mathbf{Th}; \widetilde{t}, d \cdot lw) + \\ \mathrm{InSec}^{\mathrm{SM\text{-}PRE}}(\mathbf{F} \in \mathbf{Th}; \widetilde{t}, d \cdot l) + w \cdot \mathrm{InSec}^{\mathrm{SM\text{-}UD}}(\mathbf{F} \in \mathbf{Th}; \widetilde{t}, d \cdot l) \quad (3)\end{aligned}$$

with $\widetilde{t} = t + d \cdot lw$, where time is given in number of **Th** *and* **PRF** *evaluations.*

Theorem 3. *For parameters n, w, h, d, m, t, k as described in [BHK+19] and l be the number of chains in WOTS-TW instances the following bound can be obtained:*

$$\begin{aligned}&\mathrm{InSec}^{\mathrm{EU-CMA}}(\mathrm{SPHINCS}^+; \xi, q_s) \leq \\ &\mathrm{InSec}^{\mathrm{PRF}}(\mathbf{PRF}, \xi, q_1) + \mathrm{InSec}^{\mathrm{PRF}}(\mathbf{PRF}_{\mathbf{msg}}, \xi, q_s) + \\ &\mathrm{InSec}^{\mathrm{ITSR}}(\mathbf{H}_{\mathbf{msg}}, \xi, q_s) + w \cdot \mathrm{InSec}^{\mathrm{SM\text{-}UD}}(\mathbf{F} \in \mathbf{Th}; \xi, q_2) + \\ &\mathrm{InSec}^{\mathrm{SM\text{-}TCR}}(\mathbf{F} \in \mathbf{Th}; \xi, q_3 + q_7) + \mathrm{InSec}^{\mathrm{SM\text{-}PRE}}(\mathbf{F} \in \mathbf{Th}; \xi, q_2) + \\ &\mathrm{InSec}^{\mathrm{SM\text{-}TCR}}(\mathbf{H} \in \mathbf{Th}; \xi, q_4) + \mathrm{InSec}^{\mathrm{SM\text{-}TCR}}(\mathbf{Th}_k \in \mathbf{Th}; \xi, q_5) + \\ &\mathrm{InSec}^{\mathrm{SM\text{-}TCR}}(\mathbf{Th}_l \in \mathbf{Th}; \xi, q_6) + \\ &3 \cdot \mathrm{InSec}^{\mathrm{SM\text{-}TCR}}(\mathbf{F} \in \mathbf{Th}; \xi, q_8) + \mathrm{InSec}^{\mathrm{SM\text{-}DSPR}}(\mathbf{F} \in \mathbf{Th}; \xi, q_8)\,,\end{aligned}$$

where $q_1 < 2^{h+1}(kt + l)$, $q_2 < 2^{h+1} \cdot l$, $q_3 < 2^{h+1} \cdot l \cdot w$, $q_4 < 2^{h+1}k \cdot 2t$, $q_5 < 2^h$, $q_6 < 2^{h+1}$, $q_7 < 2^{h+1}kt$, $q_8 < 2^h \cdot kt$ and q_s denotes the number of signing queries made by $\mathcal{A}$.

Analyzing Quantum Generic Security

Table 1: Success probability of generic attacks – In the “Success probability” column we give the bound for a quantum adversary $\mathcal{A}$ that makes q quantum queries to the function and p classical queries to the challenge oracle. The security parameter n is the output length of **Th**. We use $X = \sum_\gamma \left(1 - \left(1 - \frac{1}{t}\right)^\gamma\right)^k \binom{p}{\gamma} \left(1 - \frac{1}{2^h}\right)^{p-\gamma} \frac{1}{2^{h\gamma}}$.

Property	Success probability	Status
SM-TCR	$\Theta((q+1)^2/2^n)$	proven (this work, [BHK+19, HRS16])
SM-DSPR	$\Theta((q+1)^2/2^n)$	conjectured ([BHK+19])
SM-PRE	$\Theta((q+1)^2/2^n)$	based on conjecture ([BH19a, BHK+19])
PRF	$\Theta(12q/\sqrt{2^n})$	proven ([XY19])
SM-UD	$\Theta(12q/\sqrt{2^n})$	proven (this work)
ITSR	$\Theta((q+1)^2 \cdot X)$	conjectured ([BHK+19])

Constructions of tweakable hash functions

Construction 1 ([BHK+19]) *Given two hash functions* $H_1 : \{0,1\}^{2n} \times \{0,1\}^{\alpha} \to \{0,1\}^n$ *with* $2n$*-bit keys, and* $H_2 : \{0,1\}^{2n} \to \{0,1\}^{\alpha}$ *we construct* **Th** *with* $\mathcal{P} = \mathcal{T} = \{0,1\}^n$*, as*

$$\mathbf{Th}(P,T,M) = H_1(P||T, M^{\oplus}), \ \textit{with}\ M^{\oplus} = M \oplus H_2(P||T)$$

Construction 2 ([BHK+19]) *Given a hash function* $H : \{0,1\}^{2n+\alpha} \to \{0,1\}^n$*, we construct* **Th** *with* $\mathcal{P} = \mathcal{T} = \{0,1\}^n$*, as*

$$\mathbf{Th}(P,T,M) = H(P||T||M)$$

Theorem 7. *Let* H_1 *and* H_2 *be hash functions as in Construction 1 and* **Th** *the* THF *constructed by Construction 1. Then the success probability of any time-*ξ *(quantum) adversary* $\mathcal{A}$ *against* SM-PRE *of* **Th** *with tweak advice is bounded by*

$$\mathrm{Succ}^{\text{SM-PRE}}_{\mathbf{Th},p}(\mathcal{A}) \leq \mathrm{InSec}^{\text{DM-PRE}}(H_1; \xi, p)\,.$$

Theorem 8. *Let* H_1 *and* H_2 *be hash functions as in Construction 1 and* **Th** *the* THF *constructed by Construction 1. Then the following equality holds:*

$$\mathrm{InSec}^{\text{SM-UD}}(\mathbf{Th}; \xi, p) \leq \mathrm{InSec}^{\text{DM-UD}}(H_1; \xi, p).$$

Conclusion

This work:

- We recovered the proof of security of SPHINCS+
- We updated the quantum generic security of the used properties (SM-TCR, SM-UD)
- We analyzed the constructions of tweakable hash functions and the connection between the properties

Future work:

- Computer aided proof of security
- Analysis of the used properties regarding the hash functions constructions

The End
Questions?