Security analysis of the W-OTS+ signature scheme: Updating security bounds

Kudinov Mikhail

Russian Quantum Center, Russia
QApp, Russia

September 16, 2020

Definitions and Notations

Experiment $\mathrm{Exp}^{\mathrm{EU\ CMA}}_{\mathrm{Dss}(1^n)}(A)$

$(\mathrm{sk}; \mathrm{pk}) \quad \mathrm{Kg}(1^n)$.

$(M^?; \ ^?) \quad A^{\mathrm{sign}(\mathrm{sk}; \ )}(\mathrm{pk})$.

$f(M_i; \ _i)g_{i=1}^q$ be the query answers for $\mathrm{Sign}(\mathrm{sk}; \ )$.

Return 1 iff $\mathrm{Vf}(\mathrm{pk}; \ ^?; \mathrm{M}^?) = 1$ and $M^? \not\in fM_i g_{i=1}^q$.

Definitions and Notations

Consider a function family $F_n = ff_k : f0;1g^n \;!\; f0;1g^n g_{k2K_n}$, where K_n is some set.

$$\mathrm{Succ}^{\mathrm{OW}}_{F_n}(A) =$$

$$\Pr[k \overset{\$}{} K_n; x \overset{\$}{} f0;1g^n; y = f_k(x); x^0 \quad A(k;y) : y = f_k(x)] \quad (1)$$

$$\mathrm{Succ}^{\mathrm{SPR}}_{F_n}(A) =$$

$$\Pr[k \overset{\$}{} K_n; x \overset{\$}{} f0;1g^n; x^0 \quad A(k;x) : (x \neq x^0)\wedge(f(x) = f(x^0))]; \quad (2)$$

Definitions and Notations

Definition (Advantage)

Given two distributions X and Y we define the advantage $\mathrm{Adv}_{X;Y}(A)$ of an adversary A in distinguishing between these two distributions as follows:

$$\mathrm{Adv}_{X;Y}(A) = j\,\mathrm{Pr}\;\;1 \quad A(X) \quad \mathrm{Pr}\;\;1 \quad A(Y)\;j: \qquad (3)$$

We distinguish an element $(u;k)$, which is either generated uniformly at random of the following way: sample $k \overset{\$}{} K_n$ and $x \overset{\$}{} f0;1g^n$, and then setting $u = f_k(x)$.

Definition (Undetectability)

We call F_n undetectable, if the advantage of any adversary A against the UD property of F_n running in time t is negligible:

$$\mathrm{InSec}^{\mathrm{UD}}(F_n;t) \overset{\mathrm{def}}{=} \max_A f\mathrm{Adv}^{\mathrm{UD}}_{F_n}(A)g = \mathrm{negl}(n): \qquad (4)$$

The W-OTS$^+$ signature scheme

Let n 2 N be the security parameter, and m be the bit-length of signed messages, that is $M = f0;1g^m$. Let w 2 N be so-called Winternitz parameter, which determines a base of the representation that is used in the scheme. Let us define the following constants:

$$l_1 = \frac{m}{\log(w)} \quad ; \quad l_2 = \frac{\log(l_1(w \quad 1))}{\log(w)} \quad + 1; \quad l = l_1 + l_2: \quad (5)$$

By using the described above function family F_n, we define a chaining function $c_k^i(x;\mathbf{r})$ for x 2 $f0;1g^n$, $\mathbf{r} = (r_1;:::;r_j)$ 2 $f0;1g^{n \quad j}$, and $j \quad i \quad 0$ as follows:

$$c_k^0(x;\mathbf{r}) = x; \quad c_k^i(x;\mathbf{r}) = f_k(c_k^{i \quad 1}(x;\mathbf{r}) \quad r_i) \text{ for } i > 0: \quad (6)$$

The W-OTS$^+$ signature scheme

Key generation algorithm ($\mathrm{Kg}(1^n)$) consists of the following steps:

1. Sample the values

$$k \xleftarrow{\$} K; \quad \mathbf{r} = (r_1; \ldots; r_{w-1}) \xleftarrow{\$} \{0,1\}^{n(w-1)}. \tag{7}$$

2. Sample the secret signing key

$$\mathrm{sk} = (\mathrm{sk}_1; \ldots; \mathrm{sk}_l) \xleftarrow{\$} \{0,1\}^{nl}. \tag{8}$$

3. Compute the public key as follows:

$$\mathrm{pk} = (\mathrm{pk}_0; \mathrm{pk}_1; \ldots; \mathrm{pk}_l) = ((\mathbf{r}; k); c_k^{w-1}(\mathrm{sk}_1; \mathbf{r}); \ldots; c_k^{w-1}(\mathrm{sk}_l; \mathbf{r})). \tag{9}$$

The W-OTS$^+$ signature scheme

Signature algorithm (Sign(M; sk; $\mathbf{r}$)) consists of the following steps:

1. Convert M to the base w representation: $M = (M_1; : : : ; M_{l_1})$ with M_i 2 $f0; : : : ; w \quad 1g$.
2. Compute the checksum $C = \sum_{i=1}^{l_1} (w \quad 1 \quad M_i)$ and its base w representation $C = (C_1; : : : ; C_{l_2})$.
3. Set $B = (b_1; : : : ; b_l) = MjjC$ as the concatenation of the base w representations of M and C.
4. Compute the signature on M as follows:

$$= (\ _1; : : : ;\ _l) = (c_k^{b_1}(\mathrm{sk}_1; \mathbf{r}); : : : ; c_k^{b_l}(\mathrm{sk}_l; \mathbf{r})): \qquad (10)$$

The W-OTS$^+$ signature scheme

Veri cation algorithm (Vf(M; ; pk)) consists of the following steps:

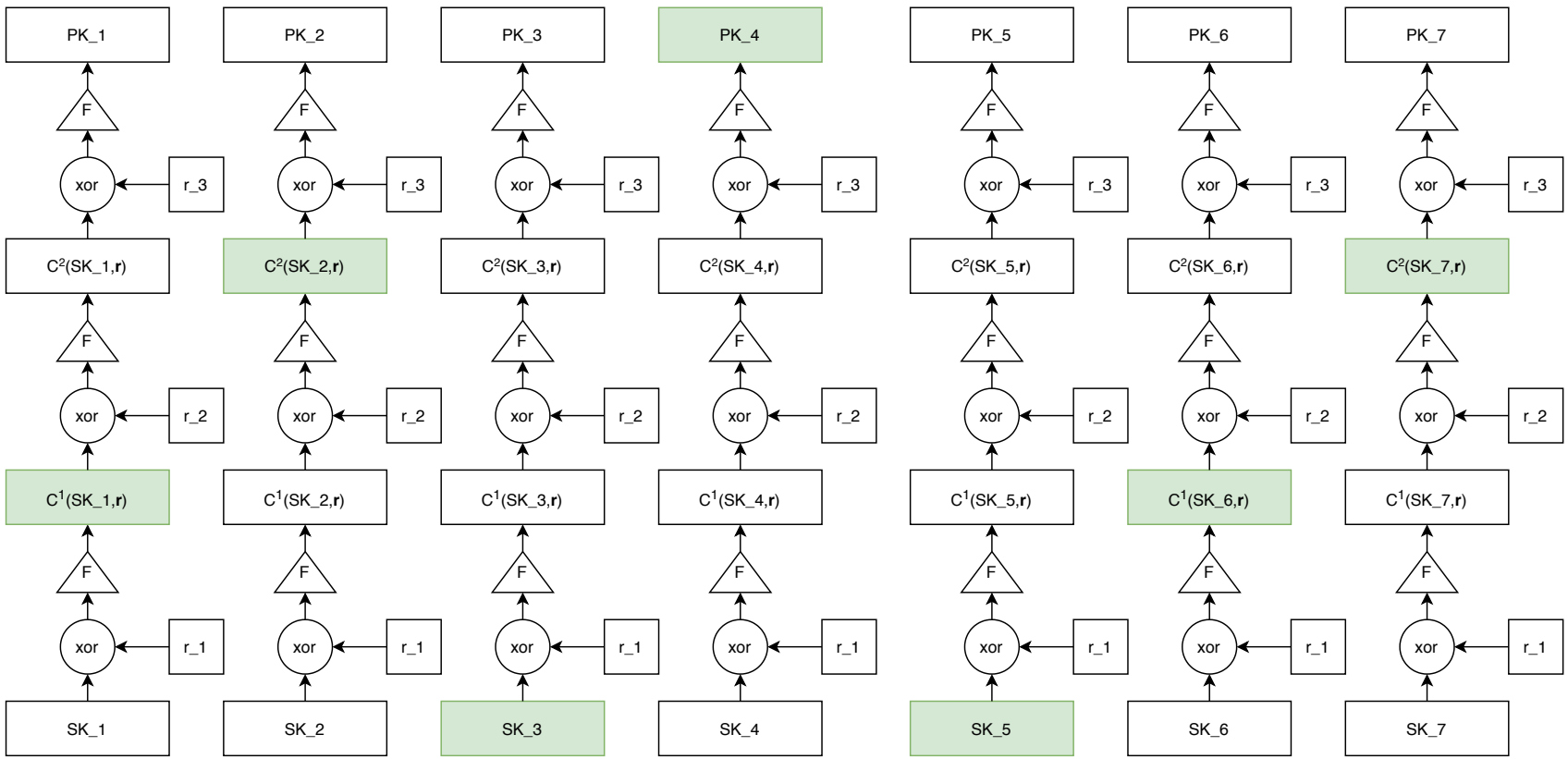
1. Compute $(b_1; : : : ; b_l)$ as it is described in steps 1-3 of the signature algorithm.
2. Do the following comparison:

$$\mathrm{pk}_i \stackrel{?}{=} c_k^{w \quad 1 \quad b_i}(\quad _i; \mathbf{r}_{b_i+1;w \quad 1}); \quad i \ 2 \ f1; : : : ; lg: \qquad (11)$$

If the comparison holds for all i, return 1, otherwise return 0.

The W-OTS$^+$ signature scheme

Consider an example with the following parameters: $n = 8$, $w = 4$. Then $l_1 = 4$, $l_2 = 3$ and $l = 7$. We will sign a message $M = 01; 10; 00; 11$. The checksum will be $C = 00; 01; 10$.



Security of W-OTS$^+$

Theorem

Let $n; w; m \; 2 \; \mathbb{N}$ and $w; m = \mathrm{poly}(n)$. Let $F_n = f f_k : f0; 1g^n \;\; ! \;\; f0; 1g^n g_{k\,2\,K_n}$ be a one-way, second preimage resistant, and undetectable function family. Then, the insecurity of the W-OTS$^+$ scheme against an EU-CMA attack is bounded by

$$\begin{aligned} &\mathrm{InSec}^{\mathrm{EU}\;\;\mathrm{CMA}}(\text{W-OTS}^+(1^n; w; m); t; 1) \\ &< lw \;\; w \;\; \mathrm{InSec}^{\mathrm{UD}}(F_n; \mathbf{t}) + \mathrm{InSec}^{\mathrm{OW}}(F_n; \mathbf{t}) + w \;\; \mathrm{InSec}^{\mathrm{SPR}}(F_n; \mathbf{t}) \end{aligned} \tag{12}$$

with $\mathbf{t} = t + 3lw + w \quad 2$, where time is given in number of evaluation function from F.

Security of W-OTS$^+$

$$p \quad e_A \qquad \mathrm{InSec}^{\mathrm{OW}}(F_n; t e) : \tag{13}$$

$$(1 \quad p)\frac{e_A}{w} < \mathrm{InSec}^{\mathrm{SPR}}(F_n; t e) : \tag{14}$$

$$e_A < \mathrm{InSec}^{\mathrm{OW}}(F_n; t e) + w \quad \mathrm{InSec}^{\mathrm{SPR}}(F_n; t e) : \tag{15}$$

Security of W-OTS$

Consider two distributions D_M and D_{Kg} over $\{1,\ldots,w-1\} \times \{0,1\}^n \times \{0,1\}^{n(w-1)} \times K_n$. An element (i, u, r, k) is obtained from D_M by generating all subelements, u, r, and k uniformly at random from the corresponding sets. At the same time, an element (i, u, r, k) is obtained from D_{Kg} by generating i, r, and k uniformly at random, but setting $u = c_k^i(x, r)$ with $x \xleftarrow{\$} \{0,1\}^n$. One can see that D_{Kg} corresponds to the generation of elements in W-OTS$ signature chain from the secret key element up to the ith level.

We construct a machine M^A to break the undetectability of F_n.

Security of W-OTS

$$
\begin{aligned}
b_A \quad & \Pr[b \quad \wedge \text{\Forgery is valid"} \wedge b' < b \,] \\
= \; & {}_A \Pr[b \quad \wedge b' < b \mid \text{\Forgery is valid"} \,] \\
& {}_A \Pr[b = \quad \wedge b' < b \mid \text{\Forgery is valid"} \,]: \quad (16)
\end{aligned}
$$

Security of W-OT$

$$\Pr[b = \ ^\ b^0 < b \ j\backslash\text{Forgery is valid"} \ ] =$$
$$\Pr[b = \ j\backslash\text{Forgery is valid"} \ ] \Pr[b^0 < b \ jb = \ ^\backslash\text{Forgery is valid"} \ ] \quad (17)$$

$$\Pr[b = \ j\backslash\text{Forgery is valid"} \ ] = \frac{X}{l(w \ \ 1)} > \frac{X}{lw}: \quad (18)$$

$$\Pr[b^0 < b \ jb = \ ^\backslash\text{Forgery is valid"} \ ] \quad \frac{1}{X}: \quad (19)$$

$$b_A > \frac{A}{lw}: \quad (20)$$

$$\text{Adv}_{D_M ;D_{Kg}}(M^{0A}) = je_A \quad b_A j: \quad (21)$$

$$_A < lw \quad \text{Adv}_{D_M ;D_{Kg}}(M^{0A}) + e_A \ : \quad (22)$$

Security of W-OTS$^+$

As we noticed earlier, M^{0A} distinguishes $u = c_k(x; r)$ and $u \xleftarrow{\$} \{0,1\}^n$ with probability $\mathrm{Adv}_{D_M, D_{Kg}}(M^{0A})$. By a classic hybrid M^{0A} can distinguish $u = c_k^1(x; r)$ and $u \xleftarrow{\$} \{0,1\}^n$ with probability at lest $\mathrm{Adv}_{D_M, D_{Kg}}(M^{0A})/w$. Hence,

$$\mathrm{Adv}_{D_M, D_{Kg}}(M^{0A}) < w \cdot \mathrm{InSec}^{UD}(F_n; t, \epsilon). \qquad (23)$$

Then putting this result into Eq. (22) we arrive at

$$\epsilon_A < l \cdot w \cdot w \cdot \mathrm{InSec}^{UD}(F_n; t, \epsilon) + \epsilon_A \qquad (24)$$

Finally, taking into account Eq. (15) we obtain the desired upper bound.

$$\mathrm{InSec}^{EU\text{-}CMA}(\text{W-OTS}^+(1^n; w; m); t; 1)$$
$$< l \cdot w \cdot w \cdot \mathrm{InSec}^{UD}(F_n; t, \epsilon) + \mathrm{InSec}^{OW}(F_n; t, \epsilon) + w \cdot \mathrm{InSec}^{SPR}(F_n; t, \epsilon)$$

Difference from the previous version of the proof

The original proof had the following equation for the security level:

$$\mathrm{InSec}^{\mathrm{EU\text{-}CMA}}(\text{W-OTS}^{+}(1^{n}; w; m); t; 1) \leq l \cdot w \cdot \max\left\{ \mathrm{InSec}^{\mathrm{OW}}(F_n; t'); w \cdot \mathrm{InSec}^{\mathrm{SPR}}(F_n; t') + w \cdot \mathrm{InSec}^{\mathrm{UD}}(F_n; t') \right\}; \quad (25)$$

	Bound from original proof			Bound from present work		
C	$b > n$	$\log w$	$\log(lw + 1)$	$b > n$	$\log(lw)$	$\log(2w + 1)$
Q	$b > \frac{n}{2}$	$\log w$	$\log(lw + 1)$	$b > \frac{n}{2}$	$\log(lw)$	$\log(2w + 1)$

Table: Comparison of security levels for the W-OTS^{+} scheme.

Conclusion and outlook

Recently, a new approach for the security analysis of hash-based signature was introduced. It suggests a novel property of hash functions, namely the decisional second-preimage resistance, but this approach had also some aws in the proof. You can nd the analysis of this new approach int he comments to round 3 Nist candidate SPHINCS+.
We are now working on a tighter proof of W-OT$^+$S taking into accaunt that it is a part of SPHINCS+ and used to sign hypertree's roots.

Security analysis of the W-OTS+ signature scheme: Updating security bounds

Thank you for your attention.

Kudinov Mikhail.
mkudinov@qapp.tech