

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 $\text{Exp}_{\text{Dss}(1^n)}^{\text{EU-CMA}}(\mathcal{A})$

$(\text{sk}, \text{pk}) \leftarrow \text{Kg}(1^n).$

$(M^*, \sigma^*) \leftarrow \mathcal{A}^{\text{sign}(\text{sk}, \cdot)}(\text{pk}).$

$\{(M_i, \sigma_i)\}_{i=1}^q$ be the query answers for $\text{Sign}(\text{sk}, \cdot).$

Return 1 iff $\forall (\text{pk}, \sigma^*, M^*) = 1$ and $M^* \notin \{M_i\}_{i=1}^q.$

Definitions and Notations

Consider a function family $\mathcal{F}_n = \{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \mathcal{K}_n}$, where $\mathcal{K}_n$ is some set.

$$\begin{aligned} \text{Succ}_{\mathcal{F}_n}^{\text{OW}}(\mathcal{A}) = \\ \Pr[k \xleftarrow{\$} \mathcal{K}_n, x \xleftarrow{\$} \{0, 1\}^n, y = f_k(x), x' \leftarrow \mathcal{A}(k, y) : y = f_k(x)] \quad (1) \end{aligned}$$

$$\begin{aligned} \text{Succ}_{\mathcal{F}_n}^{\text{SPR}}(\mathcal{A}) = \\ \Pr[k \xleftarrow{\$} \mathcal{K}_n, x \xleftarrow{\$} \{0, 1\}^n, x' \leftarrow \mathcal{A}(k, x) : (x \neq x') \wedge (f(x) = f(x'))], \quad (2) \end{aligned}$$

Definitions and Notations

Definition (Advantage)

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

$$\text{Adv}_{\mathcal{X},\mathcal{Y}}(\mathcal{A}) = |\Pr[1 \leftarrow \mathcal{A}(\mathcal{X})] - \Pr[1 \leftarrow \mathcal{A}(\mathcal{Y})]|. \quad (3)$$

We distinguish an element (u, k) , which is either generated uniformly at random of the following way: sample $k \xleftarrow{\$} \mathcal{K}_n$ and $x \xleftarrow{\$} \{0, 1\}^n$, and then setting $u = f_k(x)$.

Definition (Undetectability)

We call $\mathcal{F}_n$ undetectable, if the advantage of any adversary $\mathcal{A}$ against the UD property of $\mathcal{F}_n$ running in time $\leq t$ is negligible:

$$\text{InSec}^{\text{UD}}(\mathcal{F}_n; t) \stackrel{\text{def}}{=} \max_{\mathcal{A}} \{\text{Adv}_{\mathcal{F}_n}^{\text{UD}}(\mathcal{A})\} = \text{negl}(n). \quad (4)$$

The W-OTS⁺ signature scheme

Let $n \in \mathbb{N}$ be the security parameter, and m be the bit-length of signed messages, that is $\mathcal{M} = \{0, 1\}^m$. Let $w \in \mathbb{N}$ be so-called Winternitz parameter, which determines a base of the representation that is used in the scheme. Let us define the following constants:

$$l_1 = \left\lceil \frac{m}{\log(w)} \right\rceil, \quad l_2 = \left\lfloor \frac{\log(l_1(w-1))}{\log(w)} \right\rfloor + 1, \quad l = l_1 + l_2. \quad (5)$$

By using the described above function family $\mathcal{F}_n$, we define a chaining function $c_k^i(x, \mathbf{r})$ for $x \in \{0, 1\}^n$, $\mathbf{r} = (r_1, \dots, r_j) \in \{0, 1\}^{n \times j}$, and $j \geq i \geq 0$ as follows:

$$c_k^0(x, \mathbf{r}) = x, \quad c_k^i(x, \mathbf{r}) = f_k(c_k^{i-1}(x, \mathbf{r}) \oplus r_i) \text{ for } i > 0. \quad (6)$$

The W-OTS⁺ signature scheme

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

1. Sample the values

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

2. Sample the secret signing key

$$\text{sk} = (\text{sk}_1, \dots, \text{sk}_l) \xleftarrow{\$} \{0, 1\}^{n \times l}. \quad (8)$$

3. Compute the public key as follows:

$$\text{pk} = (\text{pk}_0, \text{pk}_1, \dots, \text{pk}_l) = ((\mathbf{r}, k), c_k^{w-1}(\text{sk}_1, \mathbf{r}), \dots, c_k^{w-1}(\text{sk}_l, \mathbf{r})). \quad (9)$$

The W-OTS⁺ signature scheme

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

1. Convert M to the base w representation: $M = (M_1, \dots, M_{l_1})$ with $M_i \in \{0, \dots, w-1\}$.
2. Compute the checksum $C = \sum_{i=1}^{l_1} (w-1-M_i)$ and its base w representation $C = (C_1, \dots, C_{l_2})$.
3. Set $B = (b_1, \dots, b_l) = M \parallel C$ as the concatenation of the base w representations of M and C .
4. Compute the signature on M as follows:

$$\sigma = (\sigma_1, \dots, \sigma_l) = (c_k^{b_1}(\text{sk}_1, \mathbf{r}), \dots, c_k^{b_l}(\text{sk}_l, \mathbf{r})). \quad (10)$$

The W-OTS⁺ signature scheme

Verification algorithm ($\text{Vf}(M, \sigma, \text{pk})$) consists of the following steps:

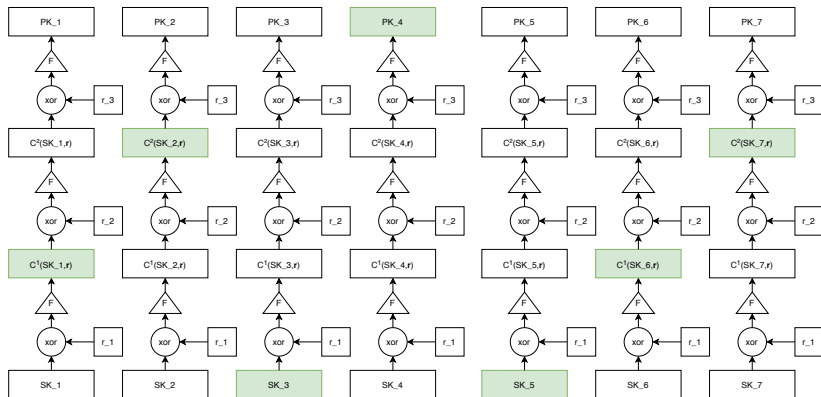
1. Compute $(b_1, \dots, b_l)$ as it is described in steps 1-3 of the signature algorithm.
2. Do the following comparison:

$$\text{pk}_i \stackrel{?}{=} c_k^{w-1-b_i}(\sigma_i, \mathbf{r}_{b_i+1, w-1}), \quad i \in \{1, \dots, l\}. \quad (11)$$

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⁺

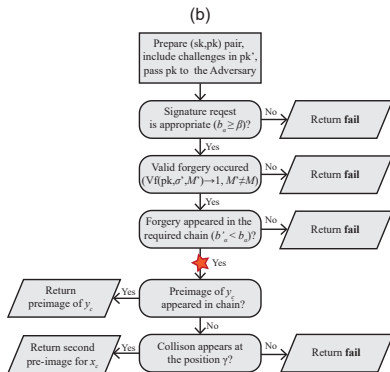
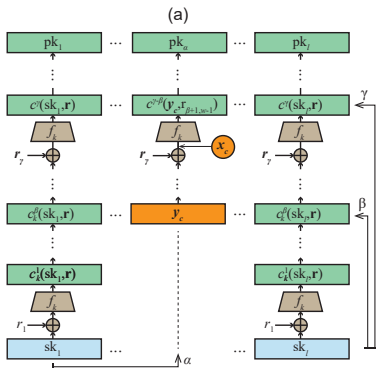
Theorem

Let $n, w, m \in \mathbb{N}$ and $w, m = \text{poly}(n)$. Let $\mathcal{F}_n = \{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \mathcal{K}_n}$ 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

$$\begin{aligned} & \text{InSec}^{\text{EU-CMA}}(\text{W-OTS}^+(1^n, w, m); t, 1) \\ & < lw \cdot (w \cdot \text{InSec}^{\text{UD}}(\mathcal{F}_n; \tilde{t}) + \text{InSec}^{\text{OW}}(\mathcal{F}_n; \tilde{t}) + w \cdot \text{InSec}^{\text{SPR}}(\mathcal{F}_n; \tilde{t})) \end{aligned} \quad (12)$$

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

Security of W-OTS⁺



$$p \cdot \tilde{\epsilon}_{\mathcal{A}} \leq \text{InSec}^{\text{OW}}(\mathcal{F}_n; \tilde{t}). \quad (13)$$

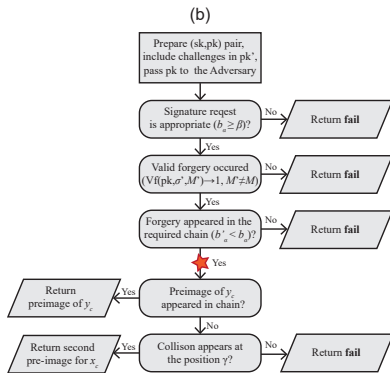
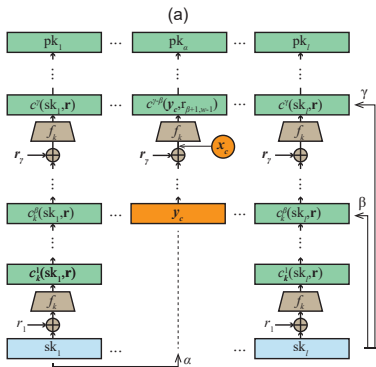
$$(1-p)\frac{\tilde{\epsilon}_A}{W} < \text{InSec}^{\text{SPR}}(\mathcal{F}_n; \tilde{t}). \quad (14)$$

$$\tilde{\epsilon}_{\mathcal{A}} < \text{InSec}^{\text{OW}}(\mathcal{F}_n; \tilde{t}) + w \cdot \text{InSec}^{\text{SPR}}(\mathcal{F}_n; \tilde{t}). \quad (15)$$

Security of W-OTS⁺

Consider two distributions $\mathcal{D}_{\mathcal{M}}$ and $\mathcal{D}_{\text{Kg}}$ over $\{1, \dots, w-1\} \times \{0, 1\}^n \times \{0, 1\}^{n \times (w-1)} \times \mathcal{K}_n$. An element $(\beta, u, \mathbf{r}, k)$ is obtained from $\mathcal{D}_{\mathcal{M}}$ by generating all subelements β , u , $\mathbf{r}$, and k uniformly at random from the corresponding sets. At the same time, an element $(\beta, u, \mathbf{r}, k)$ is obtained from $\mathcal{D}_{\text{Kg}}$ by generating β , $\mathbf{r}$, and k uniformly at random, but setting $u = c_k^\beta(x, \mathbf{r})$ with $x \xleftarrow{\$} \{0, 1\}^n$. One can see that $\mathcal{D}_{\text{Kg}}$ corresponds to the generation of elements in W-OTS⁺ signature chain from the secret key element up to the β th level. We construct a machine $\mathcal{M}'^{\mathcal{A}}$ to break the undetectability of $\mathcal{F}_n$.

Security of W-OTS⁺



$$\begin{aligned}\hat{\epsilon}_{\mathcal{A}} &\equiv \Pr[b_{\alpha} \geq \beta \wedge \text{“Forgery is valid”} \wedge b'_{\alpha} < b_{\alpha}] \\ &= \epsilon_{\mathcal{A}} \cdot \Pr[b_{\alpha} \geq \beta \wedge b'_{\alpha} < b_{\alpha} | \text{“Forgery is valid”}] \\ &\geq \epsilon_{\mathcal{A}} \cdot \Pr[b_{\alpha} = \beta \wedge b'_{\alpha} < b_{\alpha} | \text{“Forgery is valid”}].\end{aligned}\quad (16)$$

Security of W-OTS⁺

$$\Pr[b_\alpha = \beta \wedge b'_\alpha < b_\alpha | \text{“Forgery is valid”}] = \Pr[b_\alpha = \beta | \text{“Forgery is valid”}] \cdot \Pr[b'_\alpha < b_\alpha | b_\alpha = \beta \wedge \text{“Forgery is valid”}] \quad (17)$$

$$\Pr[b_\alpha = \beta | \text{“Forgery is valid”}] = \frac{X}{l(w-1)} > \frac{X}{lw}. \quad (18)$$

$$\Pr[b'_\alpha < b_\alpha | b_\alpha = \beta \wedge \text{“Forgery is valid”}] \geq \frac{1}{X}. \quad (19)$$

$$\hat{\epsilon}_{\mathcal{A}} > \frac{\epsilon_{\mathcal{A}}}{lw}. \quad (20)$$

$$\text{Adv}_{\mathcal{D}_{\mathcal{M}}, \mathcal{D}_{\text{Kg}}}(\mathcal{M}'^{\mathcal{A}}) = |\tilde{\epsilon}_{\mathcal{A}} - \hat{\epsilon}_{\mathcal{A}}|. \quad (21)$$

$$\epsilon_{\mathcal{A}} < lw \cdot (\text{Adv}_{\mathcal{D}_{\mathcal{M}}, \mathcal{D}_{\text{Kg}}}(\mathcal{M}'^{\mathcal{A}}) + \tilde{\epsilon}_{\mathcal{A}}). \quad (22)$$

Security of W-OTS⁺

As we noticed earlier $\mathcal{M}'^{\mathcal{A}}$ distinguishes $u = c_k^\beta(x, \mathbf{r})$ and $u \xleftarrow{\$} \{0, 1\}^n$ with probability $\text{Adv}_{\mathcal{D}_{\mathcal{M}}, \mathcal{D}_{\text{Kg}}}(\mathcal{M}'^{\mathcal{A}})$. By a classic hybrid $\mathcal{M}'^{\mathcal{A}}$ can distinguish $u = c_k^1(x, \mathbf{r})$ and $u \xleftarrow{\$} \{0, 1\}^n$ with probability at least $\text{Adv}_{\mathcal{D}_{\mathcal{M}}, \mathcal{D}_{\text{Kg}}}(\mathcal{M}'^{\mathcal{A}})/w$. Hence,

$$\text{Adv}_{\mathcal{D}_{\mathcal{M}}, \mathcal{D}_{\text{Kg}}}(\mathcal{M}'^{\mathcal{A}}) < w \cdot \text{InSec}^{\text{UD}}(\mathcal{F}_n; \tilde{t}). \quad (23)$$

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

$$\epsilon_{\mathcal{A}} < lw \cdot (w \cdot \text{InSec}^{\text{UD}}(\mathcal{F}_n; \tilde{t}) + \tilde{\epsilon}_{\mathcal{A}}) \quad (24)$$

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

$$\begin{aligned} & \text{InSec}^{\text{EU-CMA}}(\text{W-OTS}^+(1^n, w, m); t, 1) \\ & < lw \cdot (w \cdot \text{InSec}^{\text{UD}}(\mathcal{F}_n; \tilde{t}) + \text{InSec}^{\text{OW}}(\mathcal{F}_n; \tilde{t}) + w \cdot \text{InSec}^{\text{SPR}}(\mathcal{F}_n; \tilde{t})) \end{aligned}$$

Difference from the previous version of the proof

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

$$\begin{aligned} \text{InSec}^{\text{EU-CMA}}(\text{W-OTS}^+(1^n, w, m); t, 1) \\ \leq wl \cdot \max \{ \text{InSec}^{\text{OW}}(\mathcal{F}_n; t'), w \cdot \text{InSec}^{\text{SPR}}(\mathcal{F}_n; t') \} + \\ w \cdot \text{InSec}^{\text{UD}}(\mathcal{F}_n; t'), \quad (25) \end{aligned}$$

	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 flaws in the proof. You can find the analysis of this new approach in the comments to round 3 Nist candidate SPHINCS⁺.

We are now working on a tighter proof of W-OTS⁺, taking into account 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