ON THE SECURITY OF THE WOTS-PRF SIGNATURE SCHEME

PHILIP LAFRANCE AND ALFRED MENEZES

Abstract. We identify a flaw in the security proof and a flaw in the concrete security analysis of the WOTS-PRF variant of the Winternitz one-time signature scheme, and discuss the implications to its concrete security.

1. Introduction

The Winternitz one-time signature (WOTS) scheme (see [22, 8]) is an optimization of a one-time signature scheme first described by Lamport [20]; the latter is now called the Lamport-Diffie one-time signature scheme. The WOTS scheme is widely believed to be resistant to attacks by large-scale quantum computers, and therefore is a prime candidate for inclusion in emerging standards for post-quantum cryptography.

Several variants of WOTS have been proposed and studied in the literature. The original WOTS scheme used a one-way function and was analyzed by Dods et al. [6]. The Leighton and Micali scheme WOTS-LM is described in an IETF Internet-Draft [21], and has been analyzed in the random oracle model [17] and the quantum random oracle model [7]. Buchmann et al. [4] (see also [3, 11]) proposed a variant, called WOTS-PRF, that uses a pseudorandom function (PRF) instead of a hash function. Another hash-based WOTS variant, called WOTS$^+$, was proposed by Hülsing [12] and has been included in an IETF Internet-Draft [14]. In [16], a modification of WOTS$^+$ specifically designed to resist multi-target attacks was studied.

The practicality of a one-time signature scheme is enhanced by using a Merkle tree [22] to simultaneously authenticate many public keys for the one-time signature scheme. Merkle tree-based signature schemes that use a WOTS variant as the underlying one-time signature scheme include the eXtended Merkle Signature Scheme (XMSS) [5], XMSS$^+$ [13], XMSS^{MT} [15], and XMSS-T [16].

The most attractive feature of WOTS-PRF is that it has a reductionist security proof with minimal assumptions [4], namely the existence of a secure PRF whose existence in turn is guaranteed by the existence of one-way functions [9, 10]. This is unlike, say, WOTS-LM whose only known security proof assumes that the underlying hash function is a purely random function [17], or WOTS$^+$ whose security proof assumes the existence of a one-way function that is also second-preimage resistant and 'undetectable' [12].

In this paper, we show that the security proof for WOTS-PRF in [4] is flawed. Furthermore, we show that even if the flaw can be repaired, the concrete security analysis in [4] is incorrect since it underestimates the possible number of "key collisions" for the PRF by using an unconstructible reductionist argument to relate this number to PRF security. We show that this underestimation leads to a drastic overestimation of the concrete security

Date: September 24, 2017.

of WOTS-PRF and the Merkle signature schemes that employ it including XMSS and XMSS$^+$.

The remainder of the paper is organized as follows. The WOTS-PRF signature scheme is described in §2. In §3 we identify a flaw in the reductionist security proof. The flaw in the concrete security analysis and its implications are presented in §4. We make some concluding remarks in §5.

2. The WOTS-PRF signature scheme

The WOTS-PRF signature scheme [4] has the following ingredients:

1. A security parameter $n \in \mathbb{N}$.
2. The bitlength m of messages.
3. A Winternitz parameter $w \in \mathbb{N}$, which for simplicity we will take to be a power of two: $w = 2^e$.
4. A pseudorandom function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. For $(k, x) \in \{0,1\}^n \times \{0,1\}^n$, we will denote $f(k, x)$ by $f_k(x)$. The *iterates* of f are defined as follows. For $(k, x) \in \{0,1\}^n \times \{0,1\}^n$,
$$f_k^0(x) = k \quad \text{and} \quad f_k^i(x) = f_{f_k^{i-1}(x)}(x) \text{ for } i \geq 1.$$
Thus, $f_k^1(x) = f_k(x)$, $f_k^2(x) = f_{f_k(x)}(x)$, and so on.
5. A checksum C on messages defined as follows: set
$$\ell_1 = \left\lceil \frac{m}{e} \right\rceil, \quad \ell_2 = \left\lfloor \frac{\log_2(\ell_1(w-1))}{e} \right\rfloor + 1, \quad \ell = \ell_1 + \ell_2.$$
Define $C : \{0,1\}^m \to \{0,1\}^{e\ell_2}$ as follows. Let $M \in \{0,1\}^m$. Obtain M^0 by prepending M with 0's until the bitlength of M^0 is $e\ell_1$, and then write $M^0 = M_1 \| M_2 \| \cdots \| M_{\ell_1}$ where each M_i has bitlength e. Interpret each M_i as a non-negative integer and compute $c(M) = \sum_{i=1}^{\ell_1}(w - 1 - M_i)$. The checksum $C(M)$ is obtained by converting $c(M)$ to a binary string and then prepending 0's as necessary to obtain a binary string of bitlength exactly $e\ell_2$.

We next present the WOTS-PRF signature scheme.

Key generation. Each user A does the following:

1. Select $x \in_R \{0,1\}^n$.
2. Select $sk_1, sk_2, \ldots, sk_\ell \in_R \{0,1\}^n$.
3. Compute $pk_i = f_{sk_i}^{w-1}(x)$ for $i = 1, 2, \ldots, \ell$; $(sk_i, f_{sk_i}^1(x), f_{sk_i}^2(x), \ldots, f_{sk_i}^{w-1}(x))$ is called the i-th Winternitz hash chain.
4. A's public signature verification key is $pk = (pk_0, pk_1, \ldots, pk_\ell)$ where $pk_0 = x$. A's secret signature generation key is $sk = (sk_1, sk_2, \ldots, sk_\ell)$.

Signature generation. To sign a message $M \in \{0,1\}^m$, A does the following:

1. Compute the checksum $C = C(M)$, and let $B = M^0 \| C = b_1 \| b_2 \| \cdots \| b_\ell$ where each b_i has bitlength e.
2. Compute $\sigma_i = f_{sk_i}^{b_i}(x)$ for $i = 1, 2, \ldots, \ell$.
3. A's signature on M is $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_\ell)$.

Signature verification. To verify A's signed message (M, σ), the verifier does the following:

(1) Compute the checksum $C = C(M)$, and let $B = M^0 \| C = b_1 \| b_2 \| \cdots \| b_\ell$ where each b_i has bitlength e.
(2) Compute $pk_i' = f_{\sigma_i}^{w-1-b_i}(pk_0)$ for $i = 1, 2, \ldots, \ell$.
(3) Accept the signature if and only if $pk_i' = pk_i$ for all $i = 1, 2, \ldots, \ell$.

3. The WOTS-PRF security proof

This section presents the WOTS-PRF reductionist security proof from [4] and the flaw we observed in the analysis of its success probability. We begin with the definitions of a secure one-time signature scheme, a secure pseudorandom function, and the maximum and minimum number of key collisions.

Definition 1. A one-time signature scheme $\mathcal{S}$ is said to be (t, ϵ)-secure if all adversaries $\mathcal{A}_{\mathcal{S}}$ whose running times are bounded by t have success probability less than ϵ in the following game: $\mathcal{A}_{\mathcal{S}}$ is given a public key pk for $\mathcal{S}$ and can query a signing oracle (with respect to pk) for the signature σ of one message m of its choosing; $\mathcal{A}_{\mathcal{S}}$'s challenge is to generate a valid signed message (m^*, σ^*) with $m^* \neq m$. The security level of $\mathcal{S}$ is $\log_2(t/\epsilon)$ bits.

Definition 2. A function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is said to be a (t, ϵ)-secure PRF if all adversaries $\mathcal{A}_f$ whose running times are bounded by t have advantage less than ϵ in the following game: $\mathcal{A}_f$ is given blackbox access to an oracle $O(\cdot)$ that with equal probability is either $f_k(\cdot)$ for hidden key $k \in_R \{0,1\}^n$ or else a random function $R : \{0,1\}^n \to \{0,1\}^n$; $\mathcal{A}_f$'s challenge is to determine which it is. ($\mathcal{A}_f$'s advantage is the absolute value of the differences in probabilities that $\mathcal{A}_f$ declares that $O(\cdot)$ is $f_k(\cdot)$ in the case where $O(\cdot)$ is $f_k(\cdot)$ and the case where $O(\cdot)$ is $R(\cdot)$.) The security level of f is $\log_2(t/\epsilon)$ bits.

Definition 3. Consider the function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. For each pair $(k, x) \in \{0,1\}^n \times \{0,1\}^n$, let

$$N_{k,x} = \#\{k' \in \{0,1\}^n \ : \ f_{k'}(x) = f_k(x)\},$$

and

$$T_x = \max_k \{N_{k,x}\} \quad \text{and} \quad S_x = \min_k \{N_{k,x}\}.$$

Then the maximum number κ and minimum number κ' of key collisions are

$$\kappa = \max_x \{T_x\} \quad \text{and} \quad \kappa' = \min_x \{S_x\}.$$

Observe that $N_{k,x} \geq 1$, and so $1 \leq \kappa' \leq \kappa$. We note that the definition of κ' in [4] is incorrect, as are the definitions of κ and κ' in [3]. Our definitions of κ and κ' are equivalent to those given in [11].

In [4], the following notion of a key one-way (KOW) function is introduced.

Definition 4. A function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is said to be (t, ϵ)-KOW if all adversaries $\mathcal{A}_{KOW}$ whose running times are bounded by t have advantage less than ϵ in the following game: $\mathcal{A}_{KOW}$ is given (x, y), where $x, k \in_R \{0,1\}^n$ and $y = f_k(x)$; $\mathcal{A}_{\mathrm{KOW}}$'s challenge is to find some $k' \in \{0,1\}^n$ with $f_{k'}(x) = y$.

Proposition 2.7 in [4] shows that a (t, ϵ)-secure PRF is a $(t - 2, \epsilon/(1/\kappa - 1/2^n))$-KOW. The following is the main security claim in [4]. We include a summary of the proof from [4].

Theorem 1 (Theorem 2.8 in [4]). *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a (t', ϵ')-secure PRF. Then WOTS-PRF is a (t, ϵ)-secure one-time signature scheme with*

$$t = t' - t_{\mathrm{Kg}} - t_{\mathrm{Vf}} - 2, \tag{1}$$

$$\epsilon \leq \epsilon' \ell^2 w^2 \kappa^{w-1} \frac{1}{1/\kappa - 1/2^n}, \tag{2}$$

where t_{Kg} and t_{Vf} denotes the running times of the WOTS-PRF key generation and verification algorithms, respectively.

Summary of proof from [4]. Suppose that $\mathcal{A}_{\mathrm{WOTS}}$ is a forger that runs in time t and produces a WOTS-PRF forgery with probability at least ϵ. We construct an adversary $\mathcal{A}_{\mathrm{KOW}}$ that uses $\mathcal{A}_{\mathrm{WOTS}}$ to solve the KOW challenge.

The adversary $\mathcal{A}_{\mathrm{KOW}}$ is given a KOW challenge (x, y). It begins by generating a WOTS-PRF key pair as specified in §2 with one exception. It selects random indices $\alpha \in_R [1, \ell]$ and $\beta \in_R [1, w-1]$. Instead of selecting the secret key component sk_α and computing $pk_\alpha = f_{sk_\alpha}^{w-1}(x)$, $\mathcal{A}_{\mathrm{KOW}}$ sets $pk_\alpha = f_y^{w-1-\beta}(x)$; i.e., it inserts y at position β in the Winternitz hash chain used to compute pk_α.

Next, $\mathcal{A}_{\mathrm{KOW}}$ invokes $\mathcal{A}_{\mathrm{WOTS}}$ with public key pk and answers its signing oracle query as follows. If $b_\alpha < \beta$, then $\mathcal{A}_{\mathrm{KOW}}$ terminates the experiment since it doesn't know the first β entries of the α'th Winternitz hash chain. Otherwise, if $b_\alpha \geq \beta$, then $\mathcal{A}_{\mathrm{WOTS}}$ produces the required signature as specified in §2. If $\mathcal{A}_{\mathrm{WOTS}}$ produces a valid forger (M', σ') within its allotted time, and if $b'_\alpha < \beta$, then $\mathcal{A}_{\mathrm{WOTS}}$ computes $k' = f_{\sigma'_\alpha}^{\beta-1-b'_\alpha}(x)$ and outputs k' if $f_{k'}(x) = y$; otherwise $\mathcal{A}_{\mathrm{WOTS}}$ terminates with failure. See Figure 1.

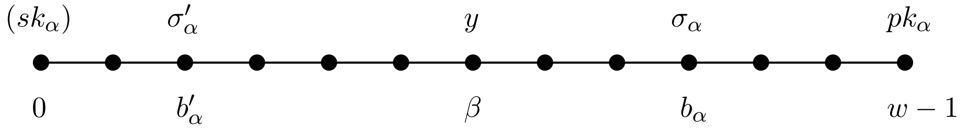

FIGURE 1. The α'th Winternitz hash chain in $\mathcal{A}_{\mathrm{KOW}}$'s experiment.

$\mathcal{A}_{\mathrm{KOW}}$'s success probability ϵ_{KOW} is assessed as follows. The probability that $b_\alpha \geq \beta$ is at least $(\ell w)^{-1}$. The probability that $\mathcal{A}_{\mathrm{WOTS}}$ succeeds is at least ϵ subject to the condition that pk is a valid public key, i.e., there exists $sk_\alpha \in \{0,1\}^n$ such that $f_{sk_\alpha}^{\beta}(x) = y$. This happens with probability at least $1/\kappa^\beta$ according to Definition 3. The probability that $b'_\alpha < \beta$ is at least $(\ell w)^{-1}$. The probability that $y = f_{k'}(x)$ holds where $k' = f_{\sigma'_\alpha}^{\beta-1-b'_\alpha}(x)$ is at least $1/\kappa^{w-1-\beta}$. This is because there exists at most κ^{w-1} keys mapping x to pk_α after $w-1$ iterations of f and only κ^β of these keys maps x to y after β iterations.

In summary we have $\epsilon_{\mathrm{KOW}} \geq \epsilon/(\ell^2 w^2 \kappa^\beta \kappa^{w-1-\beta})$ and $t_{\mathrm{KOW}} = t + t_{\mathrm{Kg}} + t_{\mathrm{Vf}}$. This yields a PRF forger $\mathcal{A}_{\mathrm{PRF}}$ with $\epsilon_{\mathrm{PRF}} \geq \epsilon(1/\kappa - 1/2^n)/(\ell^2 w^2 \kappa^{w-1})$ and $t_{\mathrm{PRF}} = t + t_{\mathrm{Kg}} + t_{\mathrm{Vf}} + 2$. □

We observe a flaw in the proof of Theorem 1, which pertains to the probability analysis of the reduction. To aid in our explanations, we introduce the notion of a *keychain*.

Definition 5. Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF, and fix $x \in \{0,1\}^n$. For any $\gamma \in \mathbb{N}$ and $y \in \{0,1\}^n$, a γ-*keychain to* y is an ordered tuple $(k_1, k_2, \ldots, k_\gamma)$ of n-bit keys such that $k_{i+1} = f_{k_i}(x)$ for $i = 1, 2, \ldots, \gamma - 1$ and $k_\gamma = y$.

The flaw is in the claim that the probability that $y = f_{k'}(x)$ holds is at least $1/\kappa^{w-1-\beta}$. Consider the tree of all w-keychains to pk_α; see Figure 2. By definition of κ, there exist at most $\kappa^{w-1-\beta}$ $(w-\beta)$-keychains to pk_α. Note that y is the first coordinate of one of these keychains. Now, since $b'_\alpha < \beta$, the keychain to pk_α beginning at σ'_α must connect with one of the $(w-\beta)$-keychains to pk_α. If the connecting keychain is selected uniformly at random, then the probability that the connecting keychain begins with y (and thus $y = f_{k'}(x)$) is indeed at least $1/\kappa^{w-1-\beta}$. However, there is no justification for assuming that $\mathcal{A}_{\text{WOTS}}$ selects a connecting chain uniformly at random. Indeed, since $\mathcal{A}_{\text{WOTS}}$ knows σ_α, it is conceivable that it always selects σ'_α so that the keychain beginning at σ'_α does not pass through σ_α, and thus never connects with y; in this event, the probability that $y = f_{k'}(x)$ holds is zero.

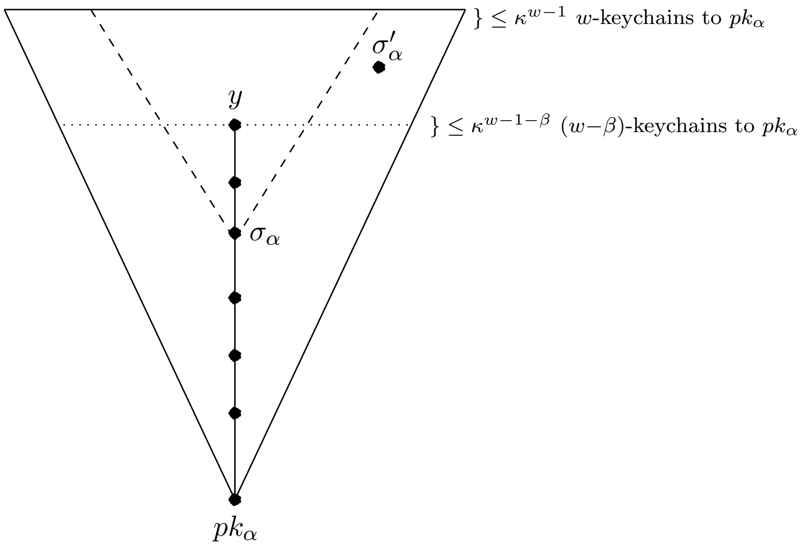
$\} \leq \kappa^{w-1}$ w-keychains to pk_α
σ'_α
y
$\} \leq \kappa^{w-1-\beta}$ $(w-\beta)$-keychains to pk_α
σ_α
pk_α

FIGURE 2. The tree of w-keychains to pk_α.

4. Concrete security of WOTS-PRF

In [4], the following relationship between the security level of the PRF f and the maximum number of key collisions κ for f is proven.

Lemma 2. *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a (t,ϵ)-secure PRF with security level $b = \log_2(t/\epsilon)$. Then $\kappa \leq 2^{n-b} + 1$.*

Proof, paraphrased from [4]. Suppose that $\kappa > 2^{n-b}+1$ and let $(x,y) \in \{0,1\}^n \times \{0,1\}^n$ be a pair for which there exist κ keys k for which $f_k(x) = y$. We construct a PRF-adversary $\mathcal{A}_f$ as follows. $\mathcal{A}_f$ queries its oracle $O(\cdot)$ with x. If $O(x) = y$ then $\mathcal{A}_f$ declares that $O(\cdot)$ is $f_k(\cdot)$; otherwise it declares that $O(\cdot)$ is $R(\cdot)$. Clearly $\mathcal{A}_f$'s runs in time $t' = 1$. Furthermore,

$$\Pr[\mathcal{A}_f \text{ declares that } O(\cdot) \text{ is } f_k(\cdot) \mid O(\cdot) \text{ is indeed } f_k(\cdot)] = \frac{\kappa}{2^n} > 2^{-b} + 2^{-n}$$

and

$$\Pr[\mathcal{A}_f \text{ declares that } O(\cdot) \text{ is } f_k(\cdot) \mid O(\cdot) \text{ is indeed } R(\cdot)] = 2^{-n}.$$

Hence $\mathcal{A}_f$'s advantage is $\epsilon' > 2^{-b}$, which contradicts the assumed PRF security level of b for f. □

Since the only way for the adversary of a good PRF f to gain an advantage is to guess the hidden key, the authors of [4] conclude that f can be expected to have security level $b = n$, whence $\kappa \leq 2$. However, we will argue that $\kappa = 2$ is a severe underestimation of the maximum number of key collisions for f. The problem with the proof of Lemma 2 is that the adversary $\mathcal{A}_f$ described is *non-constructive* since no efficient method for determining the pair (x, y) for f is known. On the other hand, the security level b of the PRF f is usually assessed by considering all known *constructible* algorithms for the PRF security game in Definition 2. Thus, $\mathcal{A}_f$'s advantage $\epsilon' > 2^{-b}$ in the proof does not contradict the assumed security level of f.

We show in §4.1 that κ can be expected to be considerably larger than 2 even for 'good' PRFs. The implications of the underestimation of κ to the concrete security guarantees for WOTS-PRF are explored in §4.2.

Remark 1. As argued in [18, 19] (see also [2]), the security level of a PRF f against attacks that might be unconstructible is expected to be significantly lower that when only constructible attacks are considered. In particular, if f is a good PRF with security level n against constructible attacks, then f can be expected to have security level no more than $n/2$ against unconstructible attacks. Furthermore, determining the exact security level of f against unconstructible attacks is expected to be a very challenging problem. The significance of the difference in the constructible and unconstructible security levels of f to the concrete security guarantees of Bellare's security proof [1] for the HMAC authentication scheme is discussed in [18, 19].

Remark 2. A one-time signature scheme $\mathcal{S}$ is said to be (t, ϵ)-strongly secure if, in addition to satisfying Definition 1, it is required that the signed message (m^*, σ^*) produced by the adversary $\mathcal{A}_{\mathcal{S}}$ satisfies $(m^*, \sigma^*) \neq (m, \sigma)$. Theorem 3.5 of [4] proves that WOTS-PRF is strongly secure assuming that the underlying PRF f is second-key resistant (SKR) or key-collision resistant (KCR). Furthermore, it is assumed that the minimum number of key collisions κ' for f (see Definition 3) satisfies $\kappa' \geq 2$. However, since

$$\kappa' = \min_{(k,x)} \{N_{k,x}\},$$

it is highly unlikely that $\kappa' \neq 1$ for PRFs f used in practice. Indeed, one would expect with overwhelming probability that $N_{k,x} = 1$ for at least one pair (k, x) for a function f selected uniformly at random from the space of all functions from $\{0,1\}^n \times \{0,1\}^n$ to $\{0,1\}^n$. Thus, the claim that WOTS-PRF is strongly secure if $\kappa' \geq 2$ is vacuous for common constructions of PRFs.

4.1. **Balls and bins.** Consider an experiment wherein N balls are thrown, independently and uniformly at random, into N bins. Of interest is the expected maximum number of balls in any bin. This study is analogous to the determination of the expected value of T_x for a fixed $x \in \{0,1\}^n$ (cf. Definition 3) for a uniform random function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. Here, the balls are the keys $k \in \{0,1\}^n$ (so $N = 2^n$), the bins are the elements of the codomain $\{0,1\}^n$, and ball k is placed in bin $f_k(x)$. Then the expected maximum number M of balls in a bin is equal to the expected value of T_x, which in turn is at most the expected value of κ.

Theorem 3 ([23]). *Consider an experiment wherein N balls are randomly assigned to N bins. Let M be the random variable that counts the maximum number of balls in a bin. Then*

$$E[M] = \frac{\ln N}{\ln \ln N}(1 + o(1)) \textit{ with probability } 1 - o(1).$$

Moreover,

$$\Pr[\textit{ there is at least one bin with } \geq \alpha \frac{\ln N}{\ln \ln N} \textit{ balls }] = \begin{cases} 1 - o(1), & \textit{if } 0 < \alpha < 1, \\ o(1), & \textit{otherwise.} \end{cases}$$

Clearly the value $\ln N / \ln \ln N$ can be made arbitrarily large. Hence, for any $t \in \mathbb{N}$ one can produce values $0 < \alpha < 1$ and $N \in \mathbb{N}$ such that $\alpha \ln N / \ln \ln N \geq t$. Thus, even though the PRF f is not uniformly random, this gives strong evidence that $\kappa \leq 2$ is in general false.

4.2. Concrete security assurances of WOTS-PRF and XMSS.

The tightness gap in the security reduction of Theorem 1 is

$$\ell^2 w^2 \kappa^{w-1} \frac{1}{1/\kappa - 1/2^n} \approx \ell^2 w^2 \kappa^w,$$

which is sensitive to the value to κ. For example, suppose that the PRF f is instantiated using AES with 128-bit keys, whereby it is reasonable to assume that it has a security level of 128 bits. The authors of [4], take $\kappa = 2$, $m = 128$, $w = 16$ and conclude that Theorem 1 guarantees a security level of at least 91 bits for WOTS-PRF. However, since one expects that

$$\kappa \geq \frac{\ln(2^{128})}{\ln(\ln(2^{128}))} \approx 20,$$

Theorem 1 can guarantee a security level of at most 39 bits for WOTS-PRF, which is insufficient in practice.

As a second example, consider XMSS when instantiated with WOTS-PRF. The security proof in [11] yields an XMSS security level of

$$b > n - h - 3 - \max\{h + 1, w \log_2(\kappa) + \log_2(\ell w)\}, \tag{3}$$

where h is the height of the XMSS tree. Taking $n = m = 256$, $w = 64$, $\kappa = 2$ and $h = 16$, Table 7.1 concludes that XMSS has a security level of at least 161 bits. However, since one expects that

$$\kappa \geq \frac{\ln(2^{256})}{\ln(\ln(2^{256}))} \approx 34.3,$$

the security bound (3) can at best guarantee that $b > -100$, which is vacuous.

Similar conclusions can be drawn about the concrete security levels given for XMSS in [5] and XMSS$^+$ in [13].

5. Concluding remarks

We emphasize that our observations on the WOTS-PRF security proof have no bearing on the security proofs for variants of WOTS such as WOTS-LM and WOTS$^+$. Furthermore, our remarks in §4.2 on the concrete security bounds for XMSS and XMSS$^+$ only apply when these signature schemes are instantiated with WOTS-PRF. In particular, they are not applicable to XMSS as described in the IETF Internet-Draft [14] where WOTS$^+$ is the underlying one-time signature scheme.

An open problem is to devise a (tight) reductionist security proof for WOTS-PRF (or a variant of it) under the sole assumption that f is a secure PRF.

Acknowledgements

We thank Andreas Hülsing for his comments on an earlier draft of this paper.

References

[1] M. Bellare, "New proofs for NMAC and HMAC: Security without collision resistance", *Advances in Cryptology — CRYPTO 2006*, LNCS 4117 (2006), 602–619.

[2] D. Bernstein and T. Lange, "Non-uniform cracks in the concrete: the power of free computation", *Advances in Cryptology — ASIACRYPT 2013*, LNCS 8270 (2013), 321–340.

[3] J. Buchmann, E. Dahmen, S. Ereth, A. Hülsing and M. Rückert, "On the security of the Winternitz one-time signature scheme", *Progress in Cryptology — AFRICACRYPT 2011*, LNCS 6737 (2011), 363–378.

[4] J. Buchmann, E. Dahmen, S. Ereth, A. Hülsing and M. Rückert, "On the security of the Winternitz one-time signature scheme", *International Journal of Applied Cryptography*, 3 (2013), 84–96.

[5] J. Buchmann, E. Dahmen and A. Hülsing, "XMSS – a practical forward secure signature scheme based on minimal security assumptions", *Post-Quantum Cryptography — PQCrypto 2011*, LNCS 7071 (2011), 117–129.

[6] C Dods, N. Smart and M. Stam, "Hash based digital signature schemes", *Cryptography and Coding*, LNCS 3796 (2005), 96–115.

[7] E. Eaton, "Leighton-Micali hash-based signatures in the quantum random-oracle model", *Selected Areas in Cryptography — SAC 2017*, to appear. Available at eprint.iacr.org/2017/607.

[8] S. Even, O. Goldreich and S. Micali, "On-line/off-line digital signatures", *Journal of Cryptology*, 9 (1996), 35–67.

[9] O. Goldreich, S. Goldwasser and S. Micali, "How to construct random functions", *Journal of the ACM*, 33 (1986), 792–807.

[10] J. Håstad, R. Impagliazzo, L. Levin and M. Luby, "A pseudorandom generator from any one-way function", *SIAM Journal on Computing*, 28 (1999), 1364–1396.

[11] A. Hülsing, "Practical forward secure signatures using minimal security assumptions", Ph.D. thesis, Technical University of Darmstadt, 2013.

[12] A. Hülsing, "W-OTS$^+$ — Shorter signatures for hash-based signature schemes", *Progress in Cryptology — AFRICACRYPT 2013*, LNCS 7918 (2013), 173–188.

[13] A. Hülsing, C. Busold and J. Buchmann, "Forward secure signatures on smart cards", *Selected Areas in Cryptography — SAC 2012*, LNCS 7707 (2013), 66–80.

[14] A. Hülsing, D. Butin, S. Gazdag, J. Rijneveld and A. Mohaisen, "XMSS: Extended hash-based signatures", Internet Draft, July 24, 2017; available at https://tools.ietf.org/html/draft-irtf-cfrg-xmss-hash-based-signatures-10.

[15] A. Hülsing, L. Rausch and J. Buchmann, "Optimal parameters for XMSS^{MT}", *Availability, Reliability, and Security in Information Systems and HCI — CD-ARES 2013*, LNCS 8128 (2013), 194–208.

[16] A. Hülsing, J. Rijneveld and F. Song, "Mitigating multi-target attacks in hash-based signatures", *Public-Key Cryptography — PKC 2016*, LNCS 9614 (2016), 387–416.

[17] J. Katz, "Analysis of a proposed hash-based signature scheme", *Security Standardisation Research — SSR 2016*, LNCS 10074 (2016), 261–273.

[18] N. Koblitz and A. Menezes, "Another look at HMAC", *Journal of Mathematical Cryptology*, 7 (2013), 225–251.

[19] N. Koblitz and A. Menezes, "Another look at non-uniformity", *Groups Complexity Cryptology*, 5 (2013), 117–140.

[20] L. Lamport, "Constructing digital signatures from a one way function", Technical Report CSL-98, SRI International, 1979.

[21] D. McGrew, M. Curcio and S. Fluhrer, "Hash-based signatures", Internet Draft, June 20, 2017; available at https://tools.ietf.org/html/draft-mcgrew-hash-sigs-07.

[22] R. Merkle, "A digital signature based on a conventional encryption function", *Advances in Cryptology — CRYPTO '87*, LNCS 293 (1988), 369–378.

[23] M. Raab and A. Steger, ""Balls into bins" – a simple and tight analysis", *Randomization and Approximation Techniques in Computer Science – RANDOM 1998*, LNCS 1518 (1998), 159–170.

ISARA Corporation, Waterloo, Canada
E-mail address: philip.lafrance@isara.com

Department of Combinatorics & Optimization, University of Waterloo, Canada
E-mail address: ajmeneze@uwaterloo.ca