“Oops, I did it again” – Security of One-Time Signatures under Two-Message Attacks

Leon Groot Bruinderink
joint work with Andreas Hülsing

August 17, 2017

Post-Quantum Signatures

- Multiple (lattice, MQ, coding, isogeny)-based suggestions exist, however:

Post-Quantum Signatures

- Multiple (lattice, MQ, coding, isogeny)-based suggestions exist, however:
  - Large signature and/or key sizes ☹

Post-Quantum Signatures

- Multiple (lattice, MQ, coding, isogeny)-based suggestions exist, however:
  - Large signature and/or key sizes ☹
  - Slow ☹

Post-Quantum Signatures

- Multiple (lattice, MQ, coding, isogeny)-based suggestions exist, however:
  - Large signature and/or key sizes
  - Slow
  - Secure parameters / lack of cryptanalysis

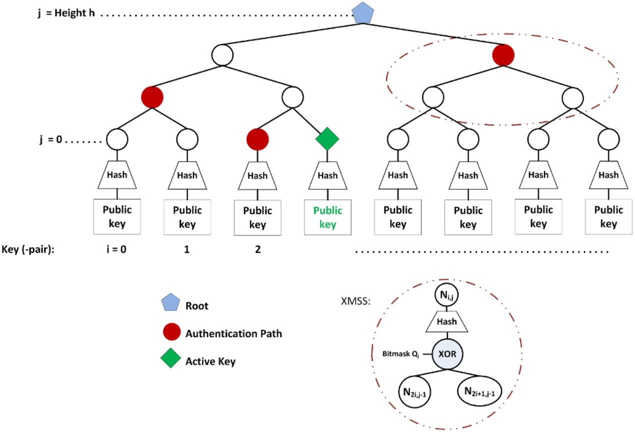
Hash-based signatures

- Only requires a secure hash-function
- Security well understood
- Fast

Hash-based one-time signatures

- First proposed already in 1979 by Leslie Lamport (LOTS)
- Later optimized by Winternitz (WOTS)
- Requires a secure hash function
- **Security only provable when keys are used to sign once!**

Merkle-based signatures



XMSS tree[1]

[1] http://www.pqsignatures.org/index/hbs.html/

Standardization

- Stateful proposals currently considered for standardization
- Stateful Merkle-tree based signatures:
  - XMSS[2]
  - LMS[3](talk by Edward Eaton)
- Stateless scheme: SPHINCS
- All of these schemes have one-time signatures (OTS) as building block.

[2] https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures/

[3] https://datatracker.ietf.org/doc/draft-mcgrew-hash-sigs/

One-time signatures - in practice?

- **Security only provable when keys are used to sign once!**
- What can happen in practice?
  - Multi-threading
  - Backups
  - Virtualization
- What can we say about attack complexities?

How one-time are One-Time Signatures?

- What can we say about attack complexities?
- In this work:
  - We assume messages are hashed before signed (but not randomized)
  - We only look at two-message attacks
  - Chosen-message and random-message attack
  - Attack goals: full break ; **existential**, selective and universal forgery

Analyzing two-message attacks

Notation

- Digest length m, security parameter n
- $F : \{0,1\}^n \rightarrow \{0,1\}^n$ one-way function
- $H : \{0,1\}^* \rightarrow \{0,1\}^m$ message hash function (modelled as RO)
- $G : \{0,1\}^m \rightarrow K \subset S$ message mapping function, where K is a subset of secret values S
- Signature σ containing secret values K

Formal security game

- Existential unforgeability under adaptively chosen-message attacks (EU-CMA)
- Game:
  - Attacker receives public key pk
  - Attacker can query H during the whole game
  - Attacker can query signing oracle twice
  - Attacker wins when outputting forgery on new message

Security games - OTS case

- We do not consider attacks against the hash function
- Security game boils down to:
    - Attacker receives public key *pk*
    - Attacker queries *H* for optimal message digests
    - Sends two optimal messages to signing oracle
    - Attacker outputs forgery
- Attack complexity equals queries to *H*
- Strong attack: pre-computation independent of public key

Security games - OTS case

- Existential unforgeability under random-message attack (EU-RMA)
- Security game boils down to:
  - Attacker gets two random messages plus signatures
  - Query H to find a third message to forge
- Attack complexity equals queries to H

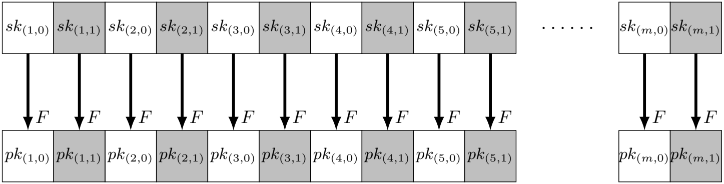
Security games - OTS case

- Existential unforgeability under random-message attack (EU-RMA)
- Security game boils down to:
  - Attacker gets two random messages plus signatures
  - Query H to find a third message to forge
- Attack complexity equals queries to H
- **Important note: with randomized hashing, EU-CMA equals EU-RMA**

Lamport Signature Scheme

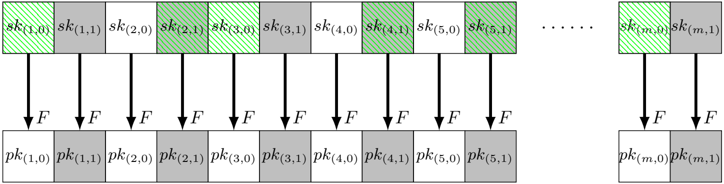
Lamport

- Key generation:
  - Secret key: $2m$ random n-bit strings: $sk = (sk_{1,0}, sk_{1,1}, \ldots, sk_{m,0}, sk_{m,1})$
  - Public key: $pk = (pk_{1,0}, pk_{1,1}, \ldots, pk_{m,0}, pk_{m,1}) = (F(sk_{1,0}), F(sk_{1,1}), \ldots, F(sk_{m,0}), F(sk_{m,1}))$



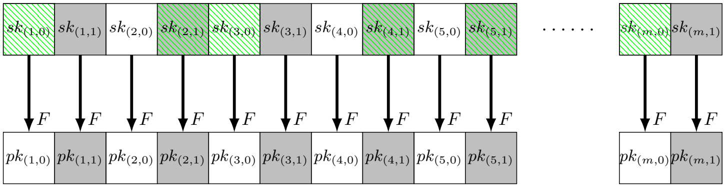
Lamport

- Key generation:
  - Secret key: $2m$ random n-bit strings: $sk = (sk_{1,0}, sk_{1,1}, \ldots, sk_{m,0}, sk_{m,1})$
  - Public key: $pk = (pk_{1,0}, pk_{1,1}, \ldots, pk_{m,0}, pk_{m,1}) = (F(sk_{1,0}), F(sk_{1,1}), \ldots, F(sk_{m,0}), F(sk_{m,1}))$
- Signature generation for $H(m_1) = (0, 1, 0, 1, 1, \ldots, 0)$:



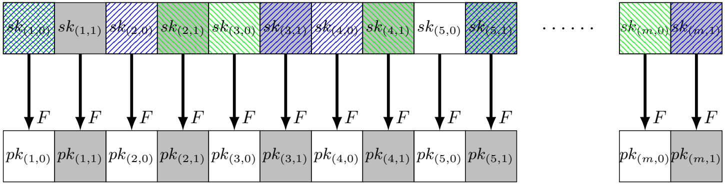
Two-message attack analysis Lamport

- First signature ($G(H(m_1)) = (0, 1, 0, 1, 1, \ldots, 0)$)



Two-message attack analysis Lamport

- First signature $(G(H(m_1)) = (0,1,0,1,1,\ldots,0))$
- Second signature $(G(H(m_2)) = (0,0,1,0,1,\ldots,1))$



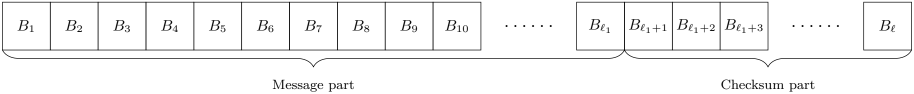
Two-message attack analysis Lamport

- Probability $H(m_3)$ being covered: $(\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2}) = 3/4$ (single bit)
- Asymptotic complexities:
  - CMA (optimize all three messages) : $(4/3)^{m/3}$
  - RMA: $(4/3)^m$
- For $n = m = 256$, CMA complexity of 2^{36} and RMA still 2^{106}

Winternitz Signature Scheme

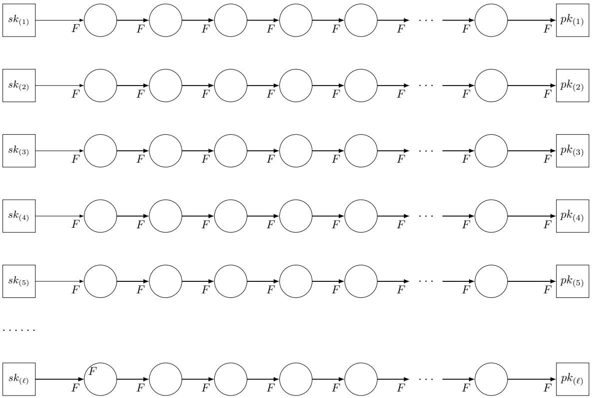
Winternitz Signature Scheme

- WOTS parameter w
- Mapping function G that maps message to:
  - Message part: base-w representation of message (size $\ell_1 = \lceil \frac{m}{\log(w)} \rceil$)
  - Checksum part: (negated) base-w representation of hamming weight (size $\ell_2 = \lfloor \frac{\log(\ell_1(w-1))}{\log(w)} \rfloor + 1$)
- Signature and key size $\ell = \ell_1 + \ell_2$
- Uses $w - 1$ iterations of hash-chains based on F: $F^k(x) = F(F^{k-1}(x)), F^0(x) = x$



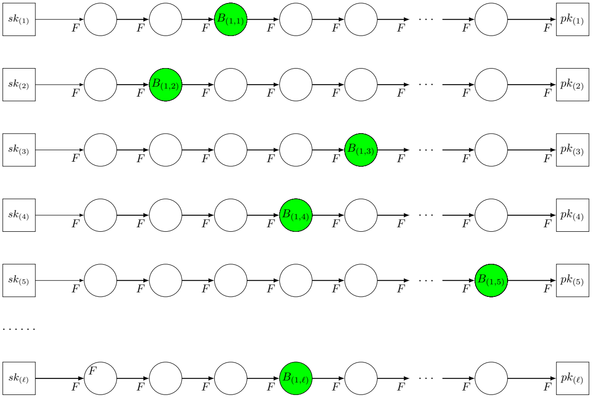
Winternitz Signature Scheme

- Key generation:
  - Secret key: ℓ random n-bit strings: $sk = (sk_1, sk_2, \ldots, sk_\ell)$
  - Public key:
    $pk = (pk_1, pk_2, \ldots, pk_\ell) = (F^{w-1}(sk_1), F^{w-1}(sk_2), \ldots, F^{w-1}(sk_\ell))$



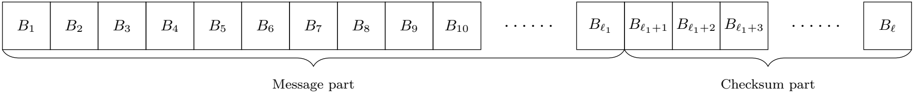
Winternitz Signature Scheme

- Signature generation $(G(H(m_1)) = (3, 2, 5, 4, w-2, \ldots, 4))$



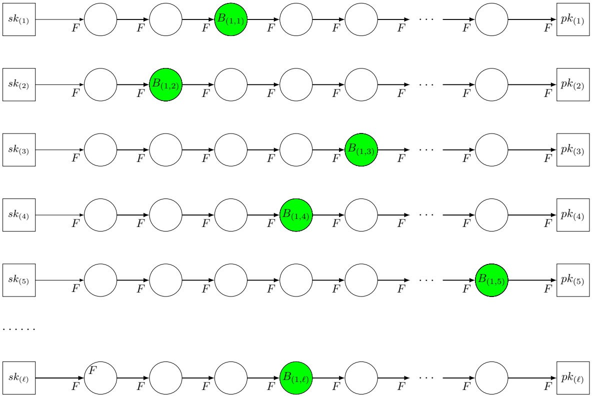
Two-message attack analysis WOTS

- Message part fixes checksum part
- What is the probability that both are covered?
- Difficult to analyze exactly. What happens "approximately"?
- Simplified model: independent random variables $U[0, w-1]$



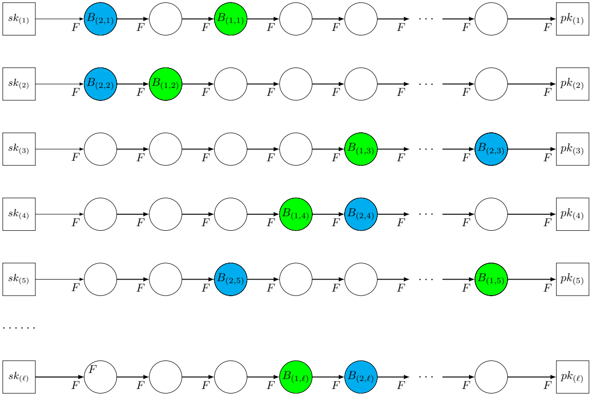
Two-message attack analysis WOTS

- Simplified model: independent random variables $U[0, w-1]$
- First signature $(G(H(m_1)) = (3, 2, 5, 4, w-2, \ldots, 4))$



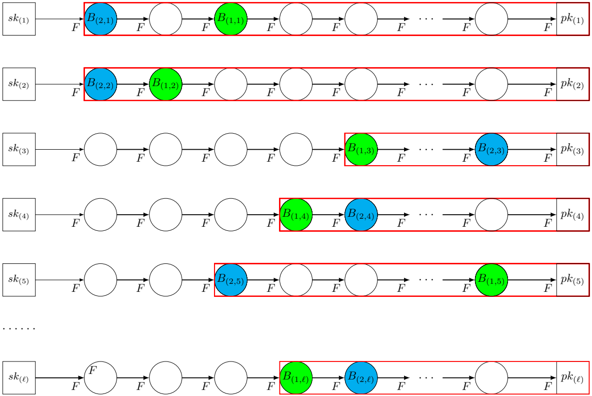
Two-message attack analysis WOTS

- Simplified model: independent random variables $U[0, w-1]$
- First signature $(G(H(m_1)) = (3, 2, 5, 4, w-2, \ldots, 4))$
- Second signature $(G(H(m_2)) = (1, 1, w-2, 4, 3, \ldots, 5))$



Two-message attack analysis WOTS

- Simplified model: independent random variables $U[0, w-1]$
- First signature $(G(H(m_1)) = (3, 2, 5, 4, w-2, \ldots, 4))$
- Second signature $(G(H(m_2)) = (1, 1, w-2, 4, 3, \ldots, 5))$



Two-message attack analysis WOTS

- Probability $H(m_3)$ being covered (single index): $\frac{(w+1)(4w-1)}{6w^2}$
- Asymptotic complexities:
  - CMA (optimize all three messages) : $\left(\frac{6w^2}{(w+1)(4w-1)}\right)^{\ell/3}$
  - RMA: $\left(\frac{6w^2}{(w+1)(4w-1)}\right)^{\ell}$
  - For $n = m = 256$ and $w = 16$, CMA complexity of 2^{11} and RMA only 2^{34}

Two-message attack analysis WOTS

- Probability $H(m_3)$ being covered (single index): $\frac{(w+1)(4w-1)}{6w^2}$
- Asymptotic complexities:
  - CMA (optimize all three messages) : $\left(\frac{6w^2}{(w+1)(4w-1)}\right)^{\ell/3}$
  - RMA: $\left(\frac{6w^2}{(w+1)(4w-1)}\right)^{\ell}$
  - For $n = m = 256$ and $w = 16$, CMA complexity of 2^{11} and RMA only 2^{34}
- *"Not that innocent"*

Experimental verification of WOTS model

- Verifying WOTS model by doing CMA
- Take list of τ messages, search for existential forgery
- From analysis: WOTS with $m = n = 256$ and $w = 16$ means $\tau \approx 2^{12}$ for $Pr[\text{Success}] = 1/2$

Table 1: WOTS with $w = 16$ and digest length $m = 256$

τ	$Pr[\text{Succes}]$
2^{11}	0.1
2^{12}	0.49
2^{13}	0.94
2^{14}	1.0
2^{15}	1.0

Conclusions

- Asymptotically, schemes still secure under two-message attacks
- However, typical parameters do not provide reasonable security level
- Future work: improve the analysis of WOTS
- More details in *http://eprint.iacr.org/2016/1042*
- **We do not advocate signing twice with any OTS**

Questions?