Mitigating Multi-Target-Attacks in Hash-based Signatures

Andreas Hülsing

joint work with Joost Rijneveld, Fang Song

A brief motivation

Information Assurance

About IA at NSA
IA Client and Partner Support
IA News
IA Events
IA Mitigation Guidance
IA Academic Outreach
IA Business and Research
IA Programs
Commercial Solutions for Classified Program
Global Information Grid
High Assurance Platform
Inline Media Encryptor
Suite B Cryptography
NSA Mobility Program
National Security Cyber Assistance Program

Home > Information Assurance > Programs > NSA Suite B Cryptography

SEARCH

Cryptography Today

In the current global environment, rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Strong cryptographic algorithms and secure protocol standards are vital tools that contribute to our national security and help address the ubiquitous need for secure, interoperable communications.

Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to quantum resistant algorithms.

Background

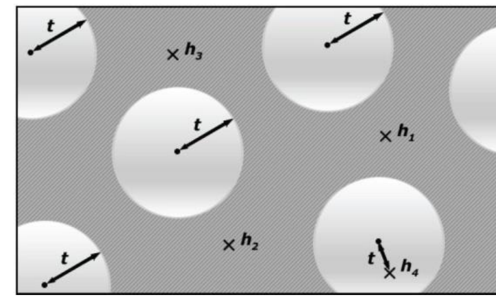
IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. Our ultimate goal is to provide cost effective security against a potential quantum computer. We are working with partners across the USG, vendors, and standards bodies to ensure there is a clear plan for getting a new suite of algorithms that are developed in an open and transparent manner that will form the foundation of our next Suite of cryptographic algorithms.

NISTIR 8105
DRAFT

Report on Post-Quantum Cryptography

Lily Chen
Stephen Jordan
Yi-Kai Liu
Dustin Moody
Rene Peralta
Ray Perlner
Daniel Smith-Tone

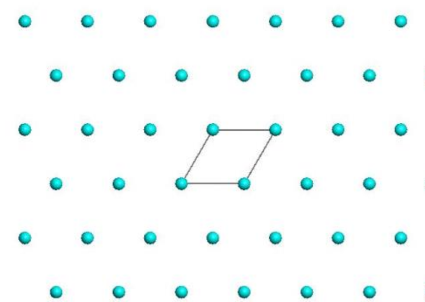
Trapdoor- / Identification Scheme-based (PQ-)Signatures



Lattice, MQ, Coding

- Signature and/or key sizes
- Runtimes
- Secure parameters

$$y_1 = x_1^2 + x_1x_2 + x_1x_4 + x_3$$
$$y_2 = x_3^2 + x_2x_3 + x_2x_4 + x_1 + 1$$
$$y_3 = \ldots$$



Hash-based Signature Schemes

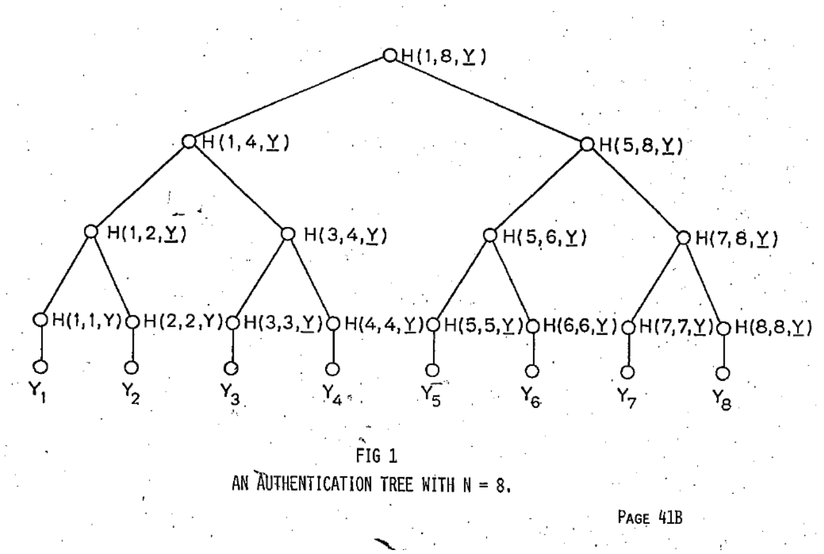
[Mer89]

Post quantum

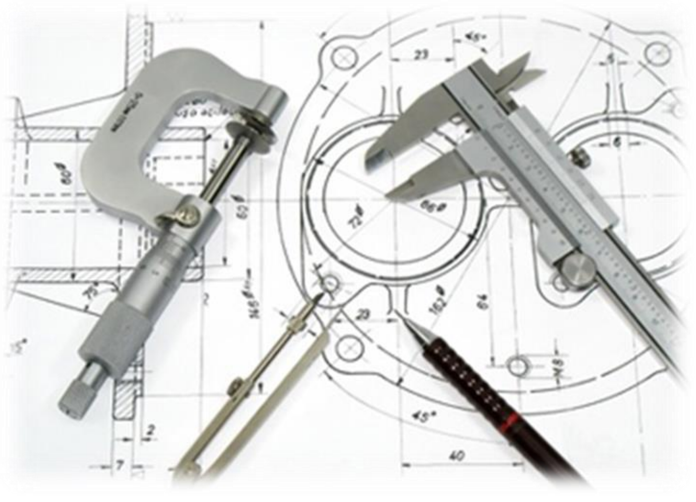
Only secure hash function

Security well understood

Fast

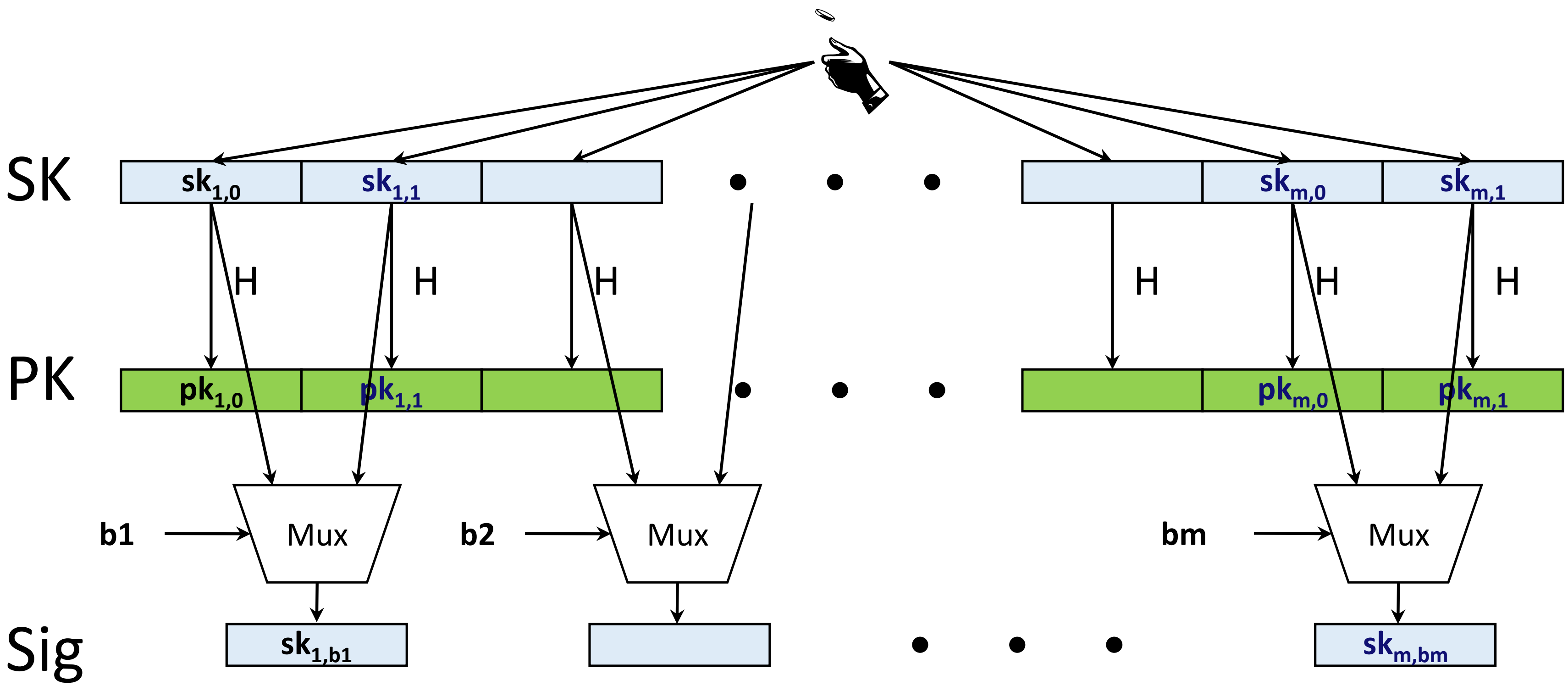


Basic Construction

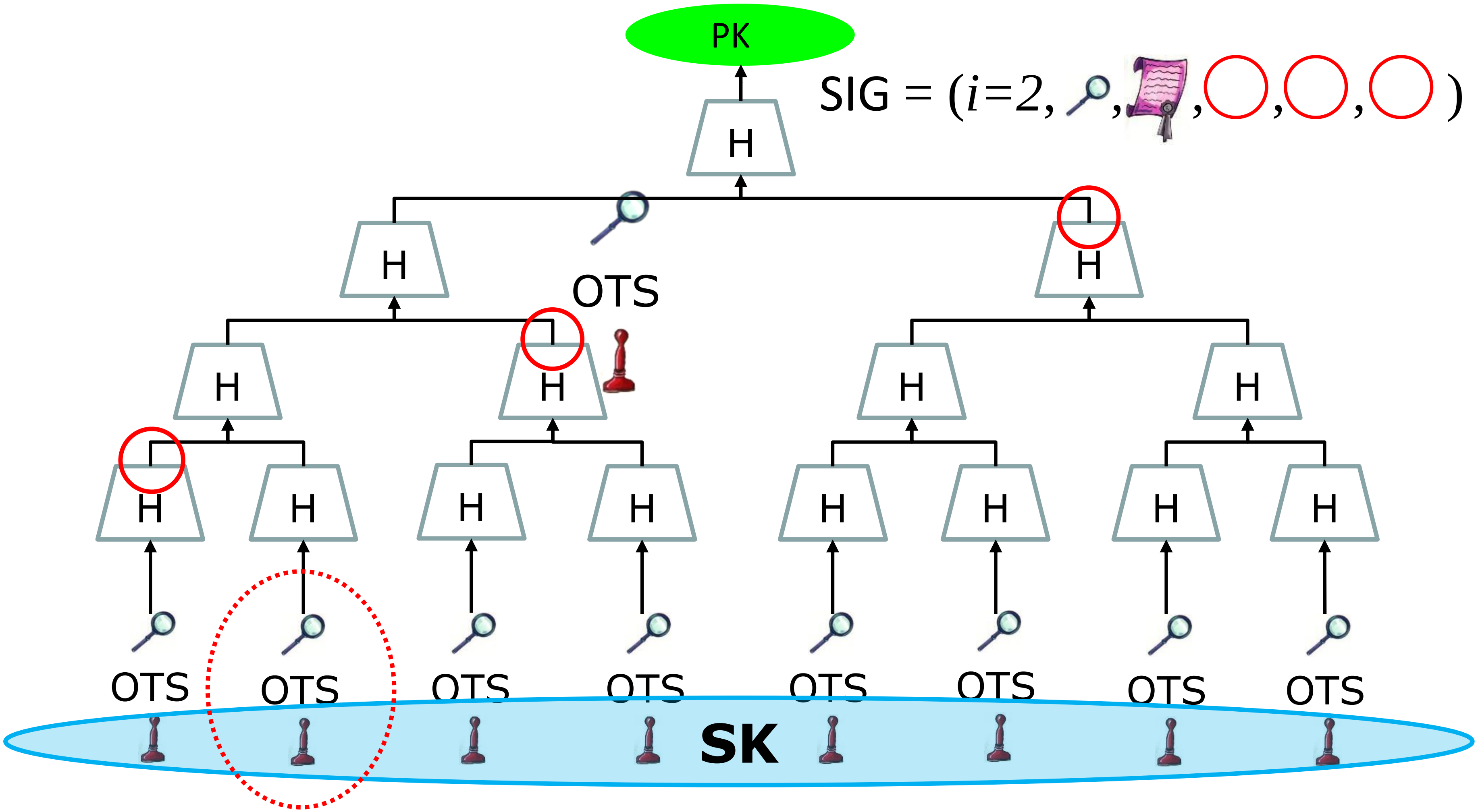


Lamport-Diffie OTS [Lam79]

Message M = b1,…,bm, OWF H   * = n bit



Merkle's Hash-based Signatures



Minimizing security assumptions…

[BHH+15,BDE+11,BDH11, DOTV08,Hül13,HRB13]

XMSS

Tree: Uses bitmasks

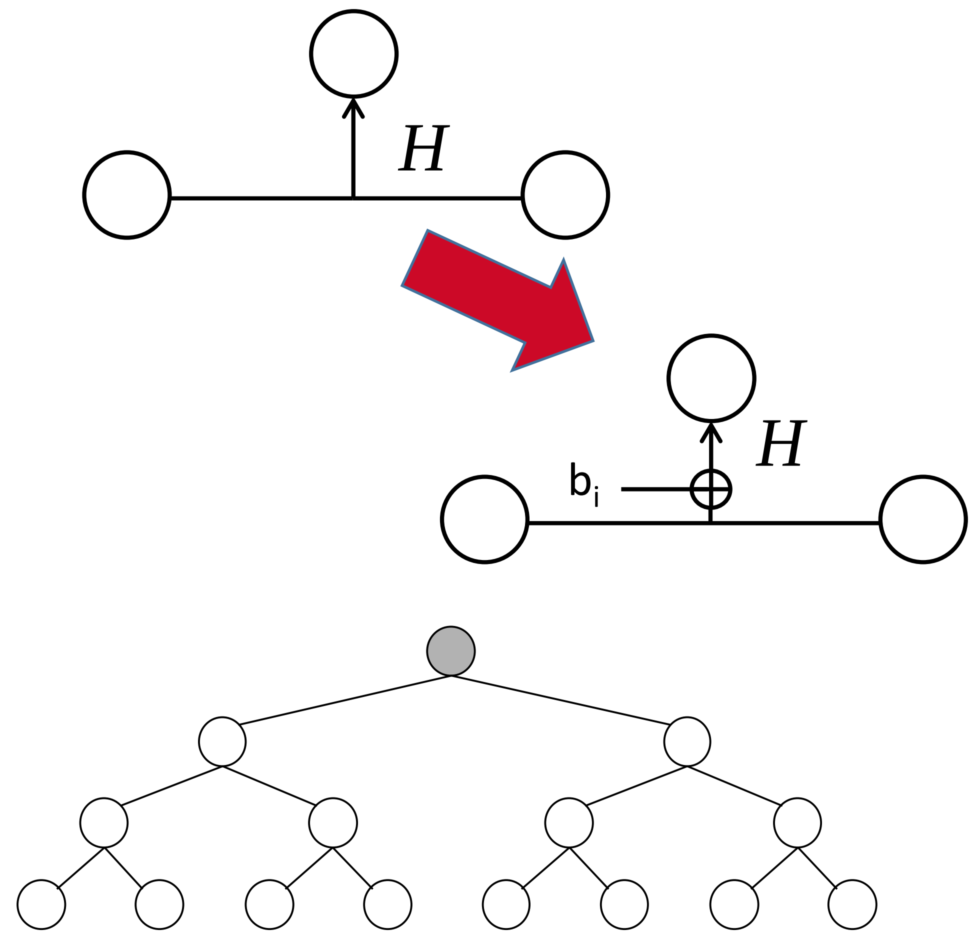
Leafs: Use binary tree with bitmasks

OTS: WOTS$^+$

Message digest: Randomized hashing

Collision-resilient

-> signature size halved

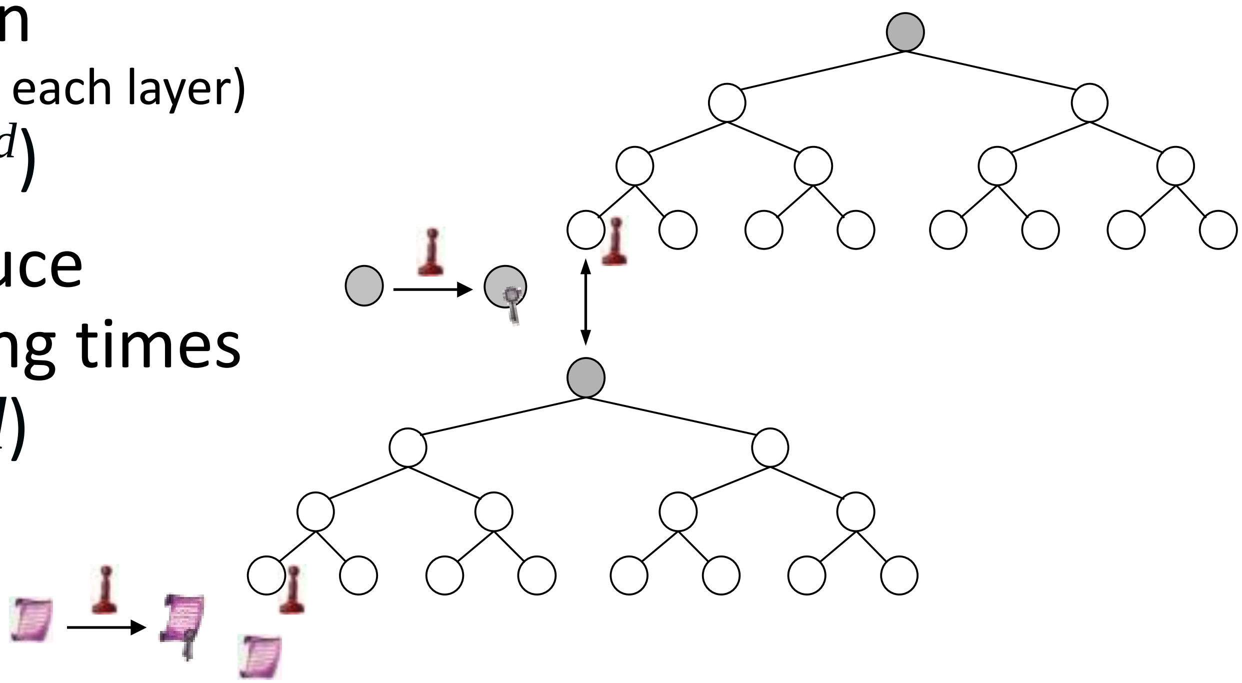


Multi-Tree XMSS

Uses multiple layers of trees

-> Key generation
(= Building first tree on each layer)
$\Theta(2^h) \longrightarrow \Theta(d*2^{h/d})$

-> Allows to reduce worst-case signing times
$\Theta(\mathrm{h}/2) \longrightarrow \Theta(h/2d)$



…and dealing with the consequences

Multi-target attacks

What is the bit security of a protocol using a $n = 256$ bit hash function that requires one-wayness?

256 bit?

Not necessarily!

Multi-target attacks

- Consider $H_n := \{h_k: \{0,1\}^m \rightarrow \{0,1\}^n | k \in \{0,1\}^n\}$
- Assume protocol Π that uses h_k p times
- Break Π $\Leftarrow$ invert h_k on <u>one out of p</u> different values.

Attack complexity: $\Theta(2^{n-\log p})$ (generic attacks)

Bit security: $n - \log p$

Similar problem applies for SPR, eTCR,....

Formalizing the issue

One-wayness:

$$\mathrm{Succ}^{\mathrm{OW}}_{\mathcal{H}_n}(\mathcal{A}) = \mathsf{Pr}\,[\,K \xleftarrow{\$} \{0,1\}^k; M \xleftarrow{\$} \{0,1\}^m, Y \longleftarrow \mathrm{H}_K(M);$$
$$M' \xleftarrow{\$} \mathcal{A}(K,Y) : Y = \mathrm{H}_K(M')\,] \;. \qquad (1)$$

$\mathrm{Succ}^{\mathrm{OW}}_{\mathcal{H}_n}(\mathcal{A}) = \left(\frac{q+1}{2^n}\right)$, for any classical q-query A

Single-function, multi-target one-wayness

$$\mathrm{Succ}^{\text{SM-OW}}_{\mathcal{H}_n,p}(\mathcal{A}) = \mathsf{Pr}\,[\,K \xleftarrow{\$} \{0,1\}^k; M_i \xleftarrow{\$} \{0,1\}^m, Y_i \longleftarrow \mathrm{H}_K(M_i), 0 < i \leq p;$$
$$M' \xleftarrow{\$} \mathcal{A}(K,(Y_1,\ldots,Y_p)) : \exists 0 < i \leq p, Y_i = \mathrm{H}_K(M')\,] \;. \qquad (2)$$

$$\mathrm{Succ}^{\text{SM-OW}}_{\mathcal{H}_n,p}(\mathcal{A}) = \left(\frac{(q+1)p}{2^n}\right),$$

Solution?

Use different elements from function family for each hash.

- Makes problems independent
- Each hash query can only be used for one target!

Multi-function, multi-target OW

$$\mathrm{Succ}^{\text{MM-OW}}_{\mathcal{H}_n,p}(\mathcal{A}) = \mathsf{Pr}\left[\, K_i \xleftarrow{\$} \{0,1\}^k, M_i \xleftarrow{\$} \{0,1\}^m, Y_i \longleftarrow \mathrm{H}_{K_i}(M_i), 0 < i \leq p; \right.$$
$$\left. (j, M') \xleftarrow{\$} \mathcal{A}((K_1,Y_1),\ldots,(K_p,Y_p)) : Y_j = \mathrm{H}_{K_j}(M') \right]. \quad (3)$$

$$\mathrm{Succ}^{\text{MM-OW}}_{\mathcal{H}_n,p}(\mathcal{A}) = \left(\frac{q+1}{2^n}\right),$$

Seems trivial, right?

What about the quantum case? Still trivial?

Technique for quantum bounds

- Define hard avg. case search problem:

Definition 1. *Let* $\mathcal{F} := \{f : \{0,1\}^m \to \{0,1\}\}$ *be the collection of all boolean functions on* $\{0,1\}^m$. *Let* $\lambda \in [0,1]$ *and* $\varepsilon > 0$. *Define a family of distributions* D_λ *on* $\mathcal{F}$ *such that* $f \leftarrow_R D_\lambda$ *satisfies*

$$f : x \mapsto \begin{cases} 1 & \textit{with prob. } \lambda, \\ 0 & \textit{with prob. } 1 - \lambda \end{cases}$$

for any $x \in \{0,1\}^m$.

- Reduce this to OW (SPR,....) of random function family

Results

	OW, MM-OW, SPR, MM-SPR	SM-OW, SM-SPR	eTCR	M-eTCR
Classical	$\frac{q+1}{2^n}$	$\frac{(q+1)p}{2^n}$	$\frac{(q+1)}{2^n} + \frac{q}{2^k}$	$\frac{(q+1)p}{2^n} + \frac{qp}{2^k}$
Quantum	$\Theta(\frac{(q+1)^2}{2^n})$	$\Theta(\frac{(q+1)^2 p}{2^n})$	$\Theta(\frac{(q+1)^2}{2^n})$	$\Theta(\frac{(q+1)^2 p}{2^n})$

Table 1. Security against generic classical and quantum attacks. Entries represent the success probability of a q-query adversary.

Implications

→ Tight security for MSS that rely on multi-function properties (works for stateful & stateless).

→ New function (key) for each call.

→ New bitmask too for SPR.

→ No solution for message digest, yet (see eTCR)

XMSS / XMSS-T Implementation (same parameters)

C Implementation, using OpenSSL [HRS16]

	Sign (ms)	Signature (kB)	Public Key (kB)	Secret Key (kB)	Bit Security classical/ quantum	Comment
XMSS	3.24	2.8	1.3	2.2	212 / 106	h = 20, d = 1,
XMSS-T	9.48	2.8	**0.064**	2.2	**190 / 95**	h = 20, d = 1
XMSS	3.59	8.3	1.3	14.6	170 / 85	h = 60, d = 3
XMSS-T	10.54	8.3	**0.064**	14.6	**190 / 95**	h = 60, d = 3

Intel(R) Core(TM) i7 CPU @ 3.50GHz
All using SHA2-256, w = 16 and k = 2

XMSS / XMSS-T Implementation
(same security)

C Implementation, using OpenSSL [HRS16]

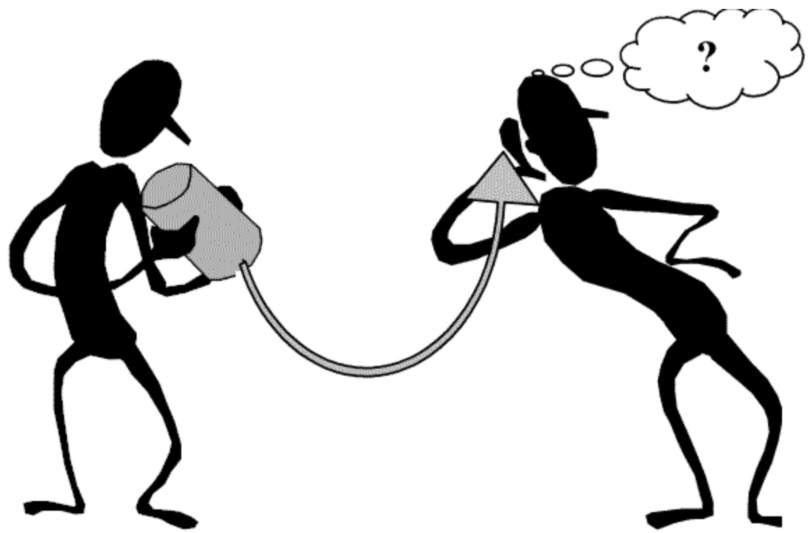
	Sign (ms)	Signature (kB)	Public Key (kB)	Secret Key (kB)	Bit Security classical/ quantum	Comment
XMSS	4.98	3.5	1.5	2.6	256/ 128	$h = 20$, $d = 1$, $m = 276$, $n =$ **300**
XMSS-T	10.14	2.9	0.064	2.2	256/ 128	$h = 20$, $d = 1$, $m = 276$, $n =$ **256**
XMSS	6.43	13.7	1.7	21.4	256/ 128	$h = 60$, $d = 3$, $m = 316$, $n =$ **342**
XMSS-T	12.82	8.8	0.064	14.6	256/ 128	$h = 60$, $d = 3$, $m = 316$, $n =$ **256**

Intel(R) Core(TM) i7 CPU @ 3.50GHz
All using SHA2-256 or SHA2-512, $w = 16$ and $k = 2$

In paper

- XMSS-T
  (== draft-irtf-cfrg-xmss-hash-based-signatures-02)
- Tight security reduction for XMSS-T
- Implementation of XMSS & XMSS-T

Thank you!
Questions?



For references & further literature see
https://huelsing.wordpress.com/hash-based-signature-schemes/literature/