Mitigating Multi-Target-Attacks in Hash-based Signatures

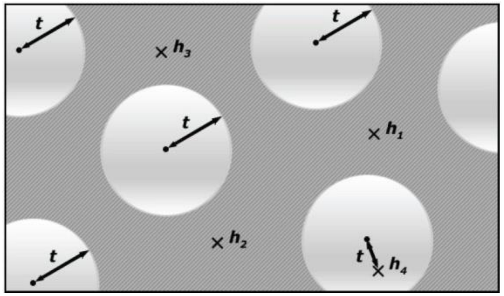
Andreas Hülsing

joint work with Joost Rijneveld, Fang Song

A brief motivation

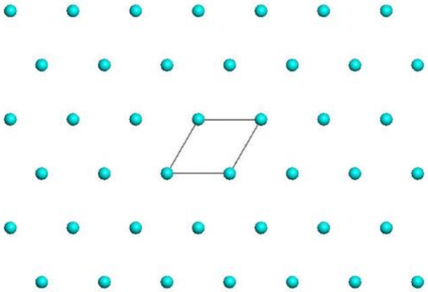
Trapdoor- / Identification Scheme-based (PQ-)Signatures

Lattice, MQ, Coding



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

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



Hash-based Signature Schemes

[Mer89]

- Post quantum
- Only secure hash function
- Security well understood
- Fast

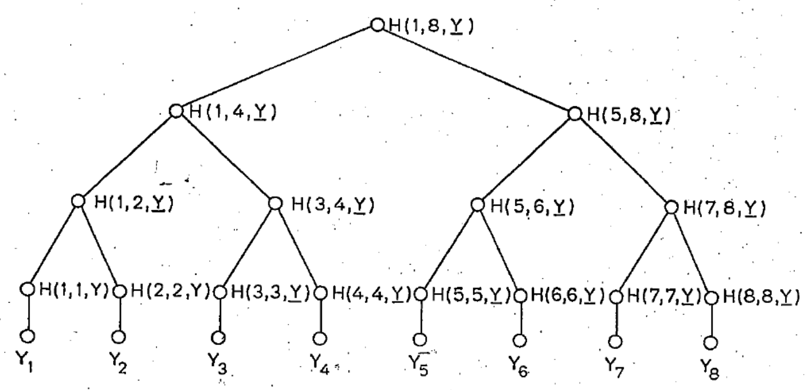
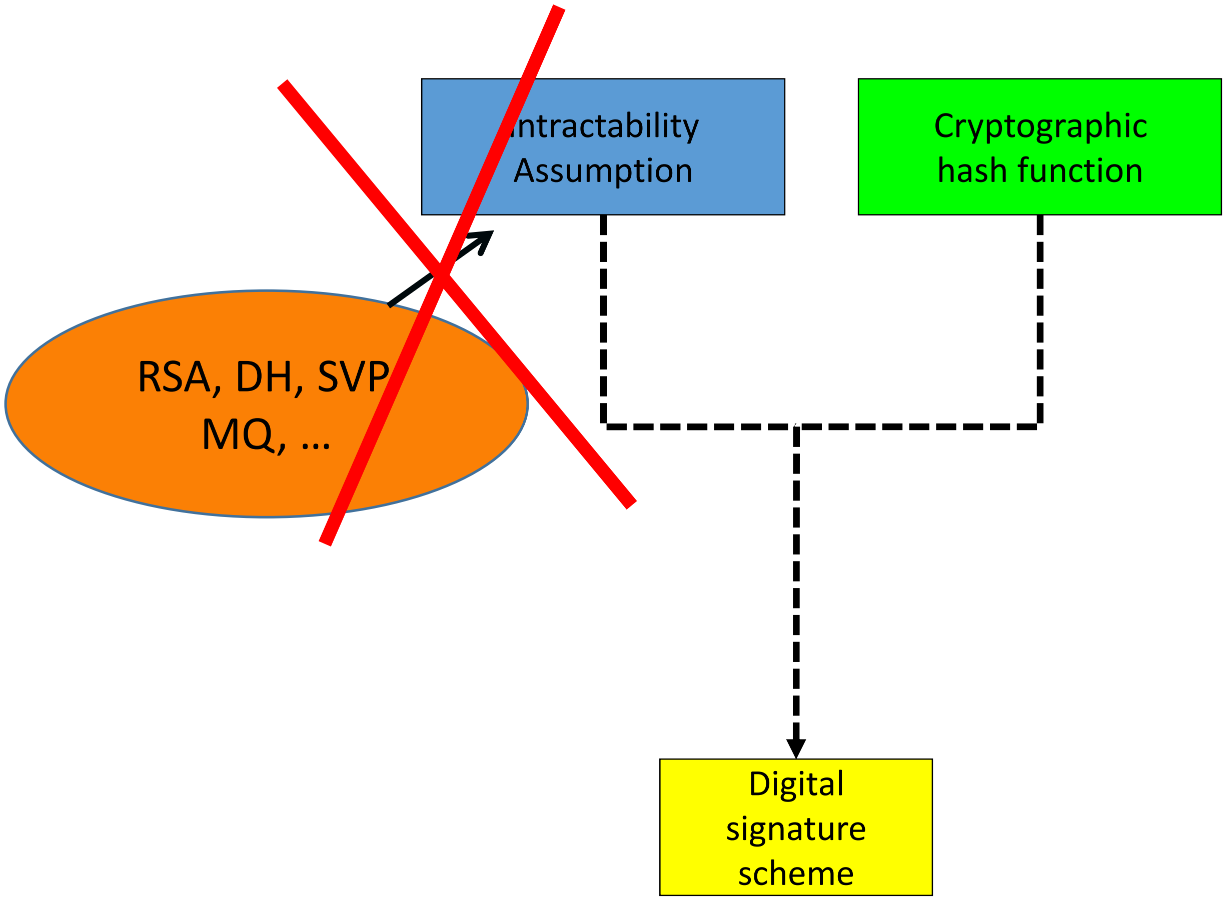
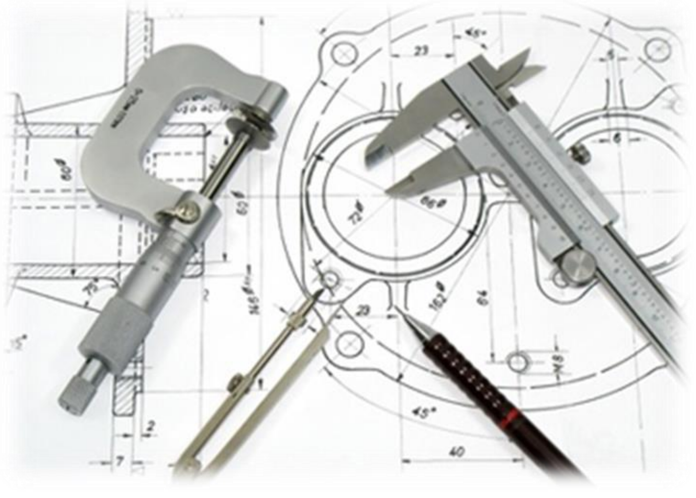


FIG 1
AN AUTHENTICATION TREE WITH N = 8.
PAGE 41B

RSA – DSA – EC-DSA…

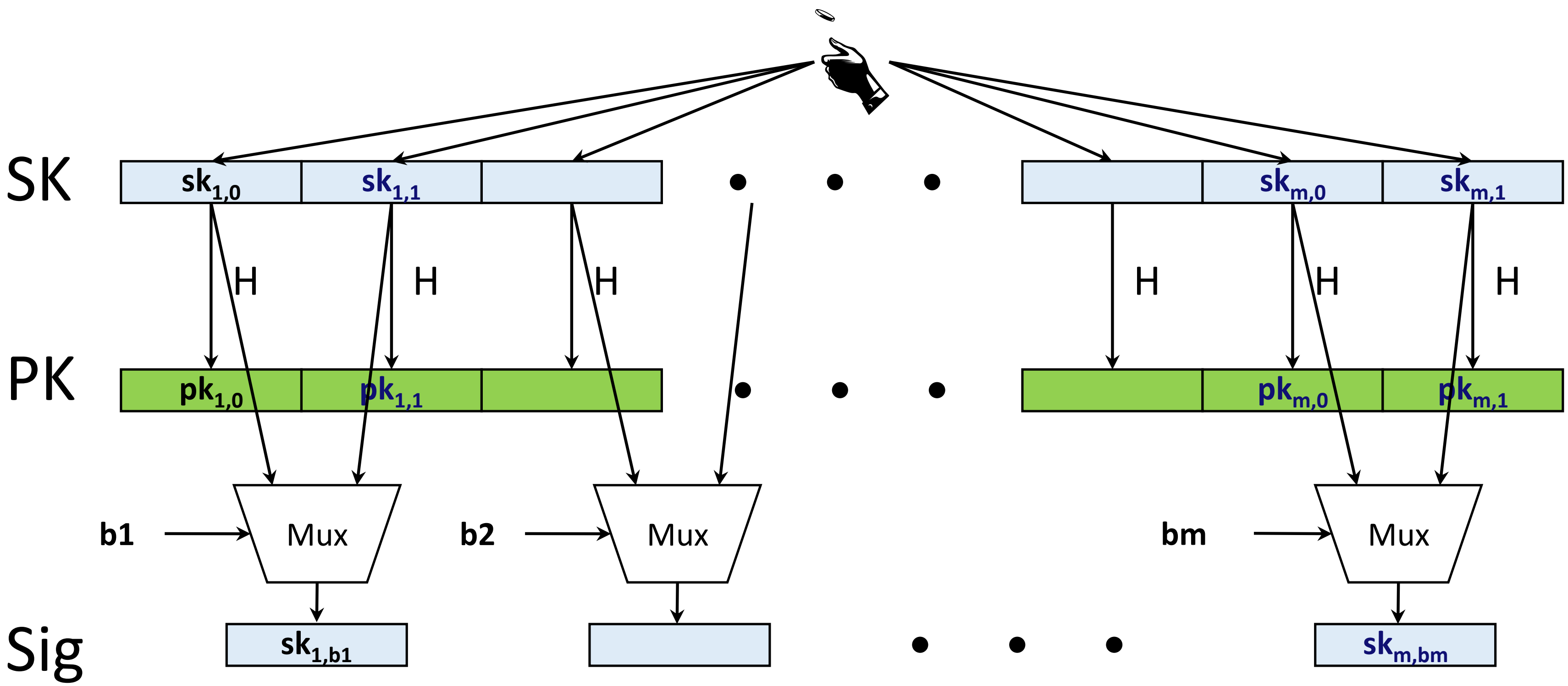


Basic Construction

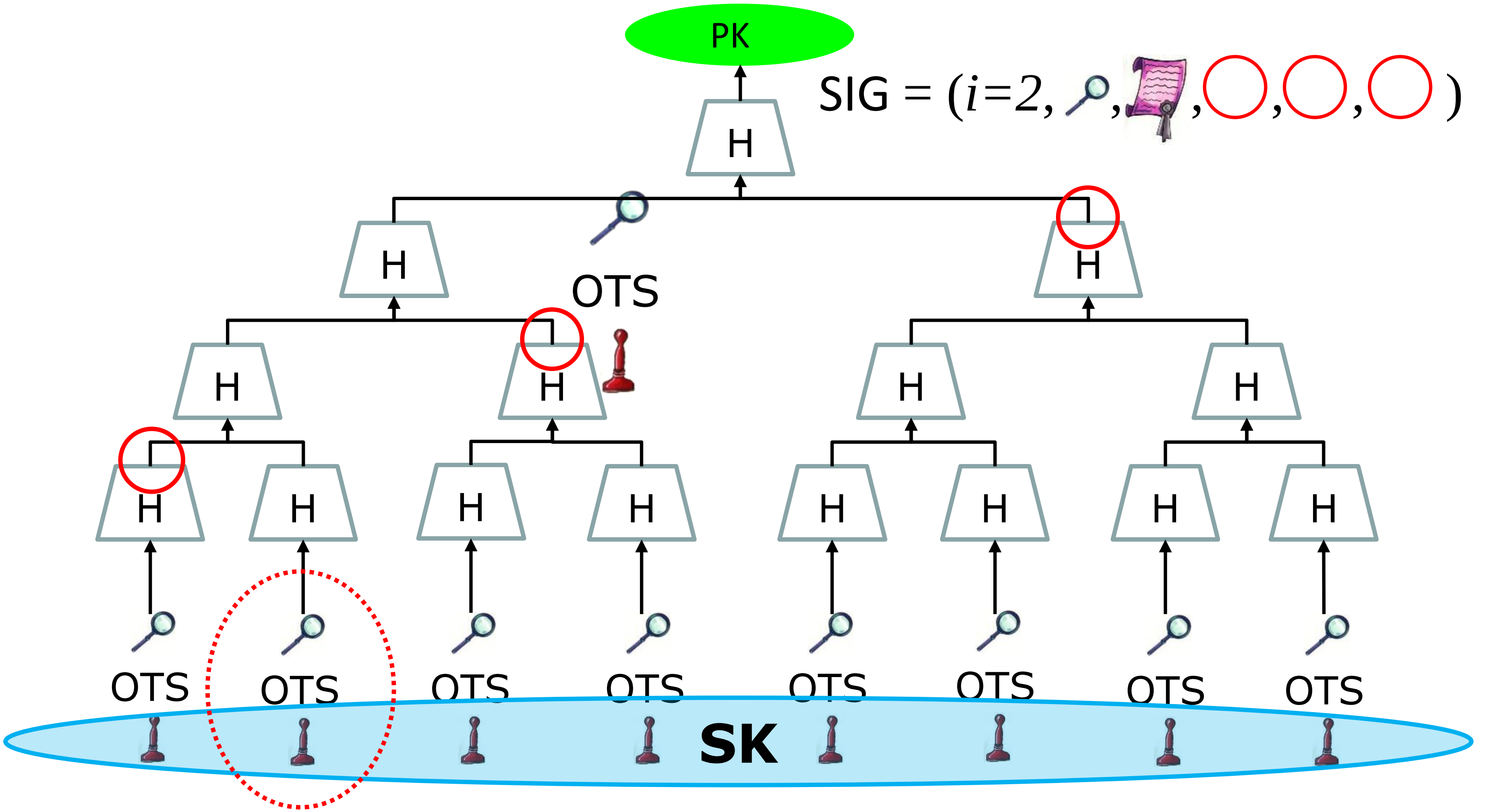


Lamport-Diffie OTS [Lam79]

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



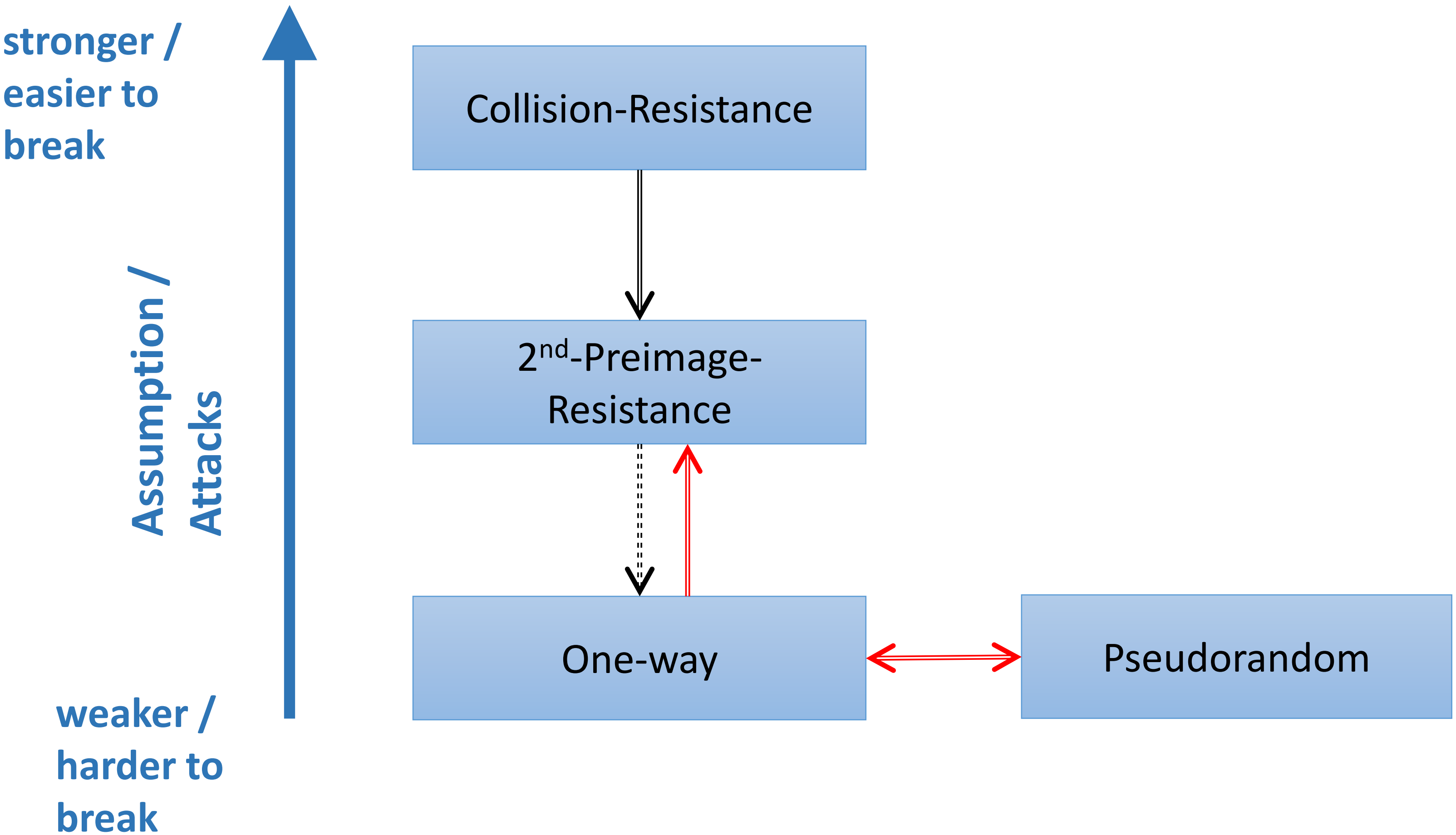
Merkle's Hash-based Signatures



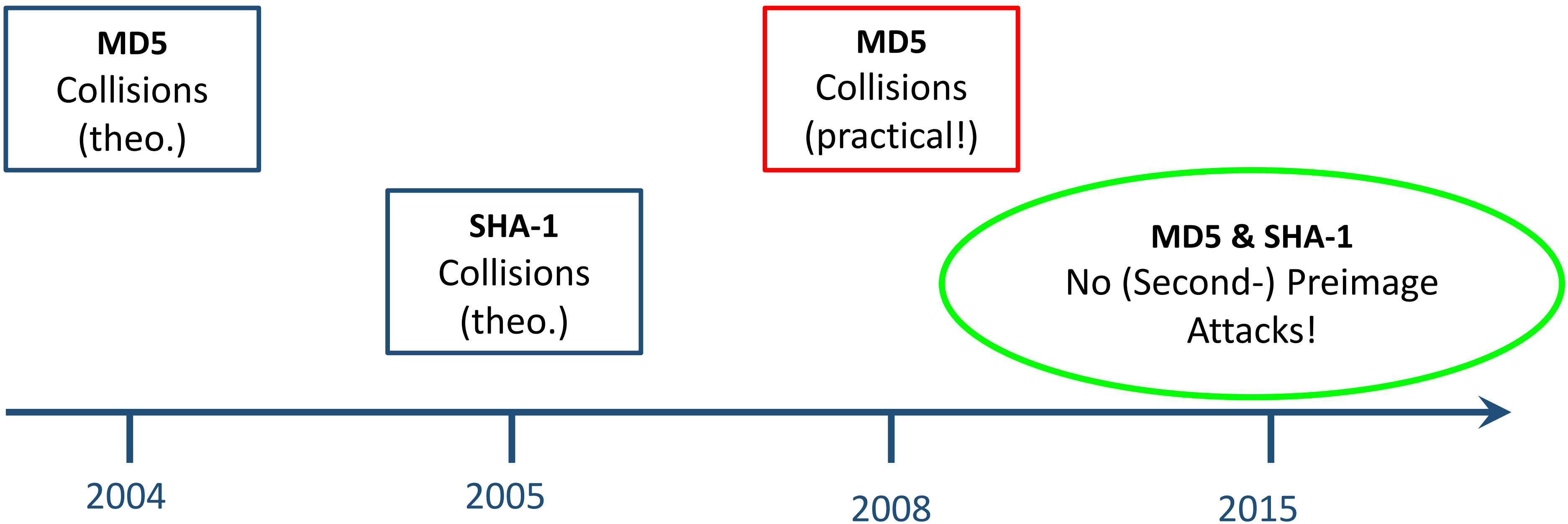
Minimizing security assumptions…

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

Hash-function properties



Attacks on Hash Functions



…and dealing with the consequences

[HRS16]

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 $\Pi \Leftarrow$ 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:

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

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

Single-function, multi-target one-wayness

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

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

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

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

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

Seems trivial, right?

What about the quantum case? Still trivial?

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.

→ New function (key) for each call.

→ New bitmask too for SPR

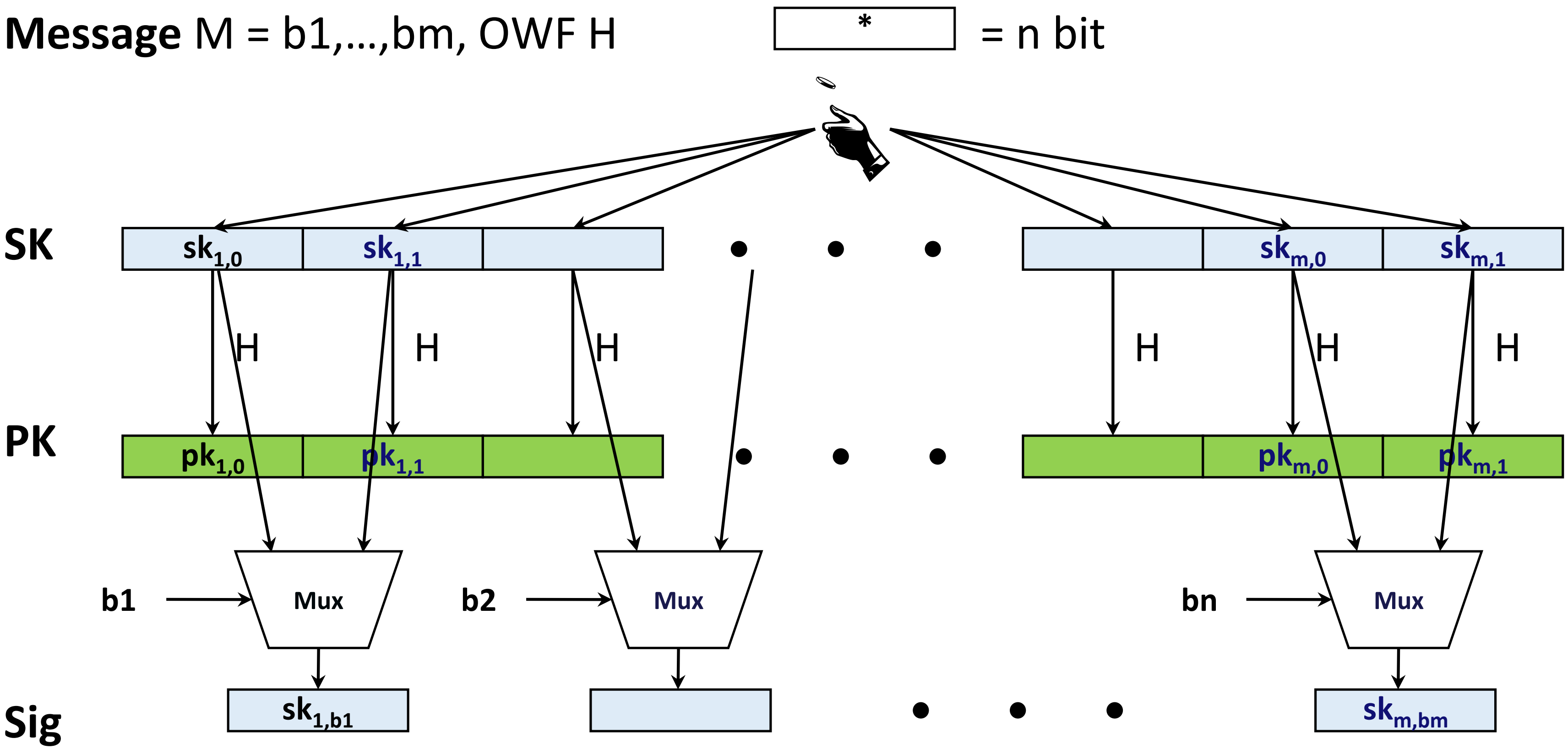
→ No solution for message digest, yet (see eTCR)

Part II: Details on Hash-based signatures

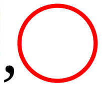
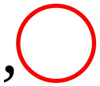
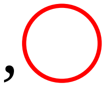
Winternitz-OTS

[Mer90,BDE+11,Hül13]

Recap LD-OTS [Lam79]



LD-OTS in MSS

SIG = (i=2, , , , , )

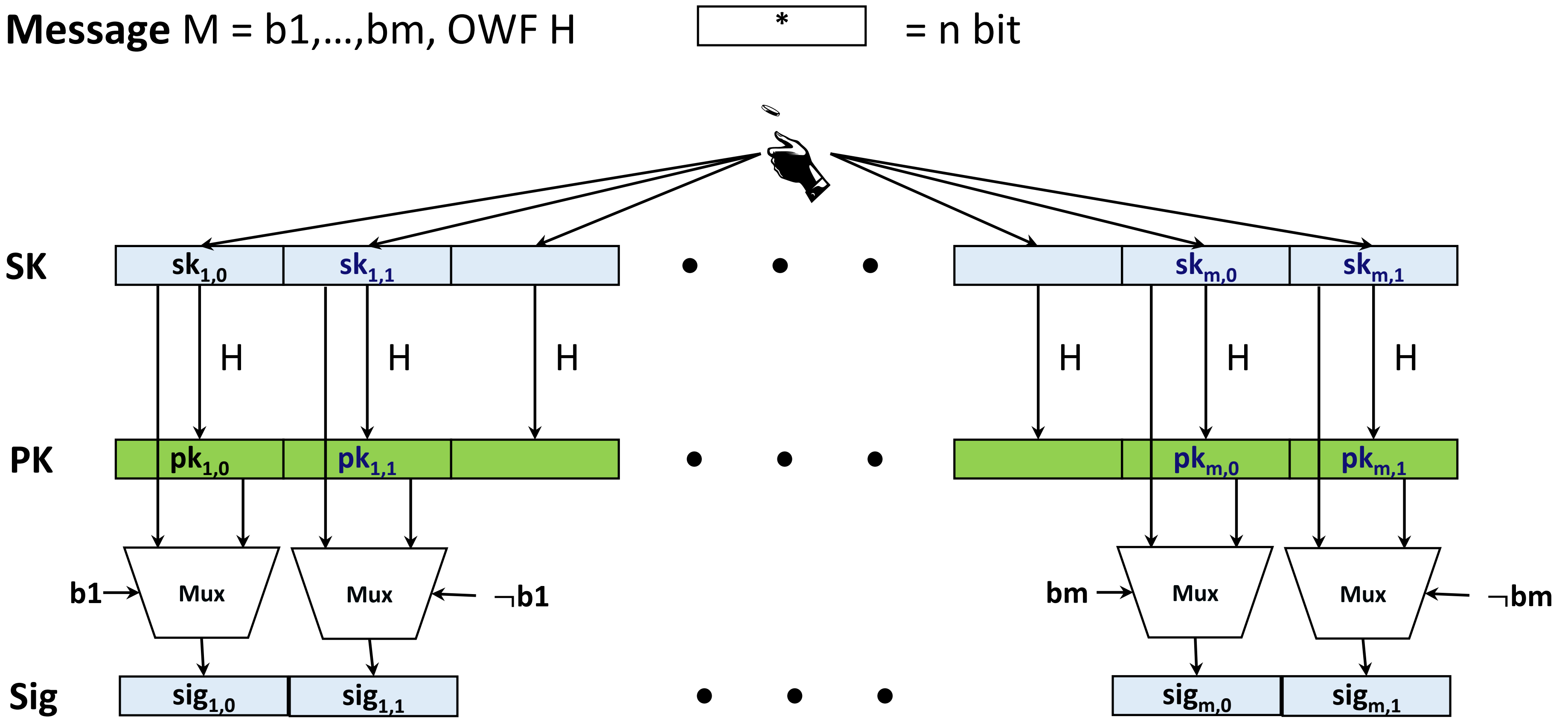
Verification:

1. Verify 
2. Verify authenticity of 

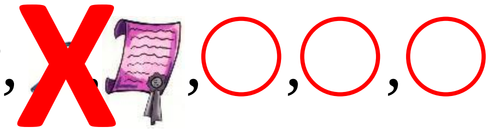
We can do better!

Trivial Optimization

Message M = b1,…,bm, OWF H



Optimized LD-OTS in MSS

SIG = (i=2, )

Verification:

1. Compute  from 
2. Verify authenticity of 

Steps 1 + 2 together verify 

Let‘s sort this!

Message $M = b_1,\ldots,b_m$, OWF H

SK: $sk_1,\ldots,sk_m,sk_{m+1},\ldots,sk_{2m}$

PK: $H(sk_1),\ldots,H(sk_m),H(sk_{m+1}),\ldots,H(sk_{2m})$

Encode M: $M' = M || \neg M$ **=** $b_1,\ldots,b_m,\neg b_1,\ldots,\neg b_m$
(instead of $b_1, \neg b_1,\ldots,b_m,\neg b_m$)

Sig: sig_i **=** $\begin{cases} sk_i & \text{, if } b_i = 1 \\ H(sk_i) & \text{, otherwise} \end{cases}$

Checksum with bad performance!

Optimized LD-OTS [Mer90]

Message $M = b_1,\ldots,b_m$, OWF H

SK: $sk_1,\ldots,sk_m,sk_{m+1},\ldots,sk_{m+1+\log m}$

PK: $H(sk_1),\ldots,H(sk_m),H(sk_{m+1}),\ldots,H(sk_{m+1+\log m})$

Encode M: $M' = b_1,\ldots,b_m,\sum_1^m \neg b_i$

Sig: sig_i **=**
$$sig_i = \begin{cases} sk_i & \text{, if } b_i = 1 \\ H(sk_i) & \text{, otherwise} \end{cases}$$

IF one b_i is flipped from 1 to 0, another b_j will flip from 0 to 1

Function chains

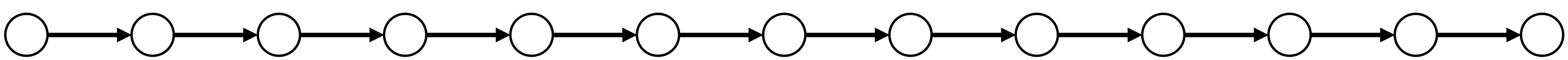
Function family: $H_n := \{h_k : \{0,1\}^n \rightarrow \{0,1\}^n\}$

$h_k \xleftarrow{\$} H_n$

Parameter w

Chain: $c^i(x) = h_k(c^{i-1}(x)) = \underbrace{h_k \circ h_k \circ \ldots \circ h_k(x)}_{i-times}$

$c^0(x) = x$



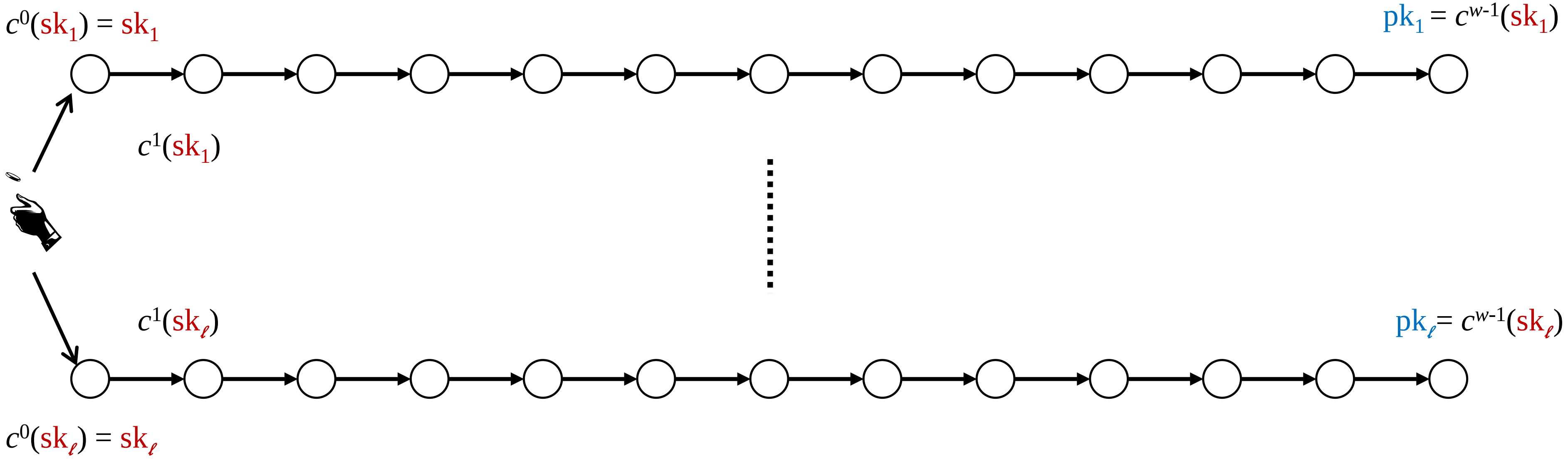
$c^1(x) = h_k(x)$

$\boldsymbol{c^{w-1}}(x)$

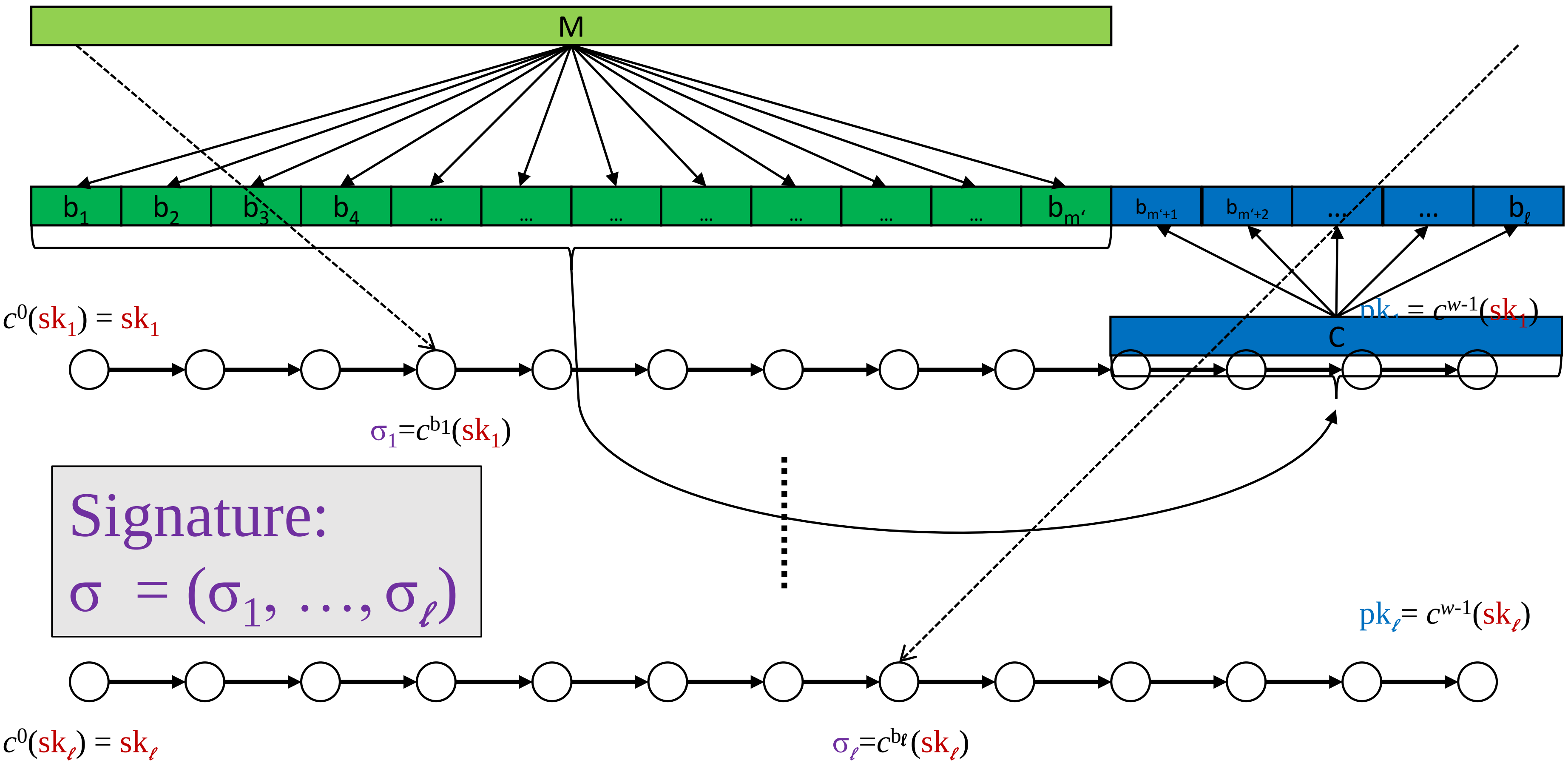
WOTS

Winternitz parameter $\boldsymbol{w}$, security parameter $\boldsymbol{n}$, message length $\boldsymbol{m}$, function family H_n

Key Generation: Compute l, sample h_k

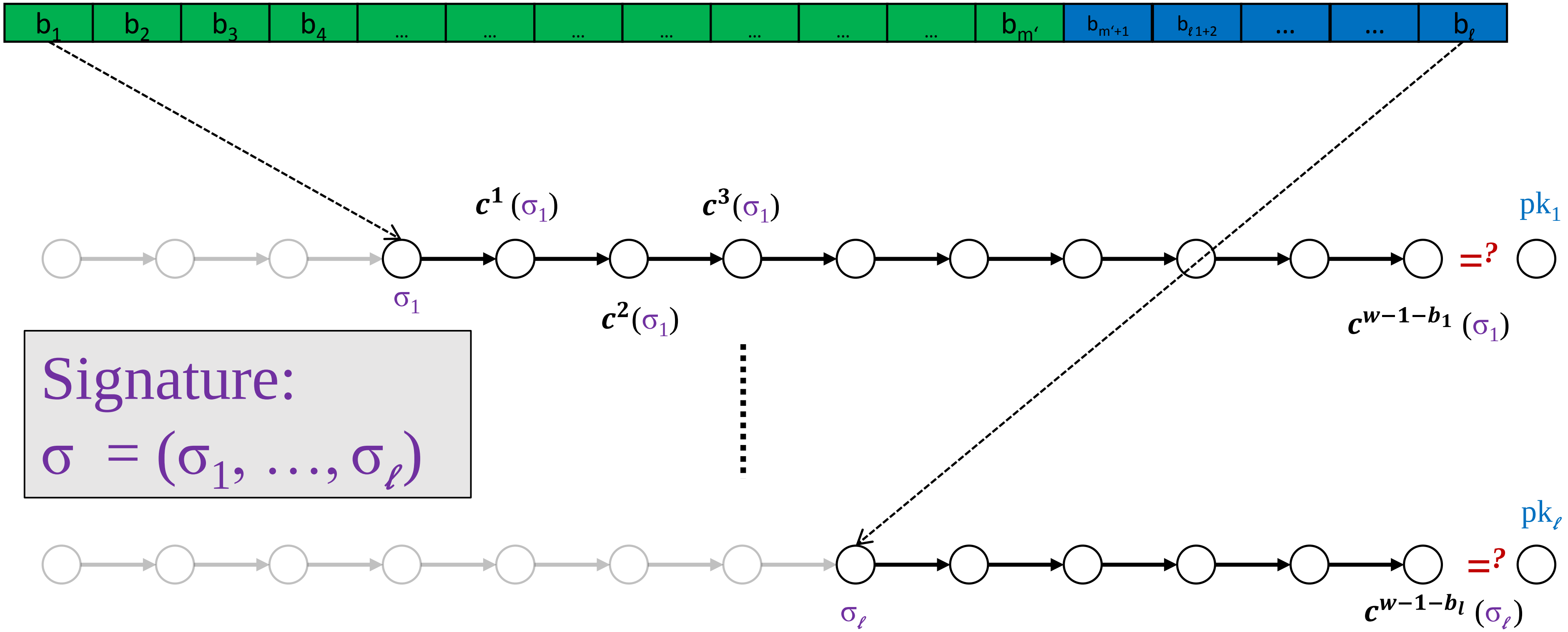


WOTS Signature generation



WOTS Signature Verification

Verifier knows: M, w



WOTS Function Chains

For $x \in \{0,1\}^n$ define $c^0(x) = x$ and

- WOTS: $c^i(x) = h_k(c^{i-1}(x))$
- WOTS$: $c^i(x) = h_{c^{i-1}(x)}(r)$
- WOTS+: $c^i(x) = h_k(c^{i-1}(x) \oplus r_i)$

WOTS Security

Theorem (informally):

W-OTS *is strongly unforgeable under chosen message attacks if* H_n *is a collision resistant family of undetectable one-way functions.*

W-OTS$^{\$}$ *is existentially unforgeable under chosen message attacks if* H_n *is a pseudorandom function family.*

W-OTS^{+} *is strongly unforgeable under chosen message attacks if* H_n *is a* 2^{nd}*-preimage resistant family of undetectable one-way functions.*

eXtended Merkle Signature Scheme (XMSS)

joint work with Johannes Buchmann, Erik Dahmen

XMSS

Tree: Uses bitmasks

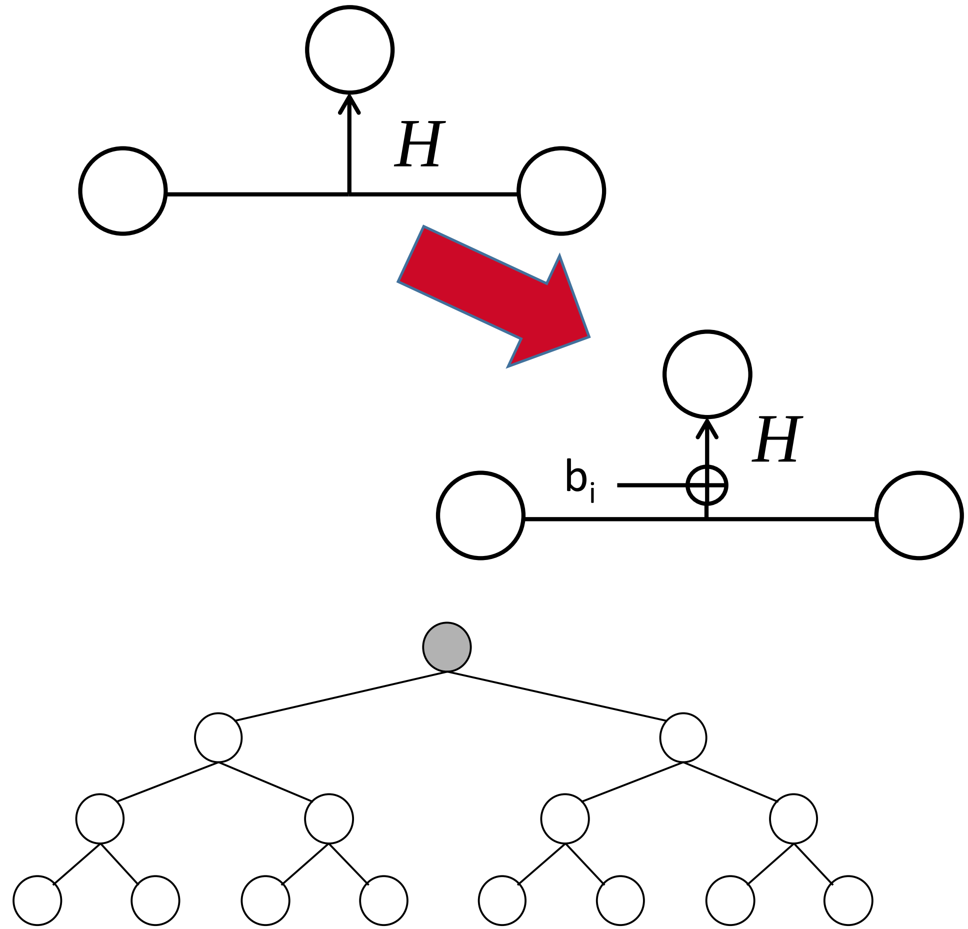
Leafs: Use binary tree with bitmasks

OTS: WOTS$^+$

Mesage digest: Randomized hashing

Collision-resilient

-> signature size halved

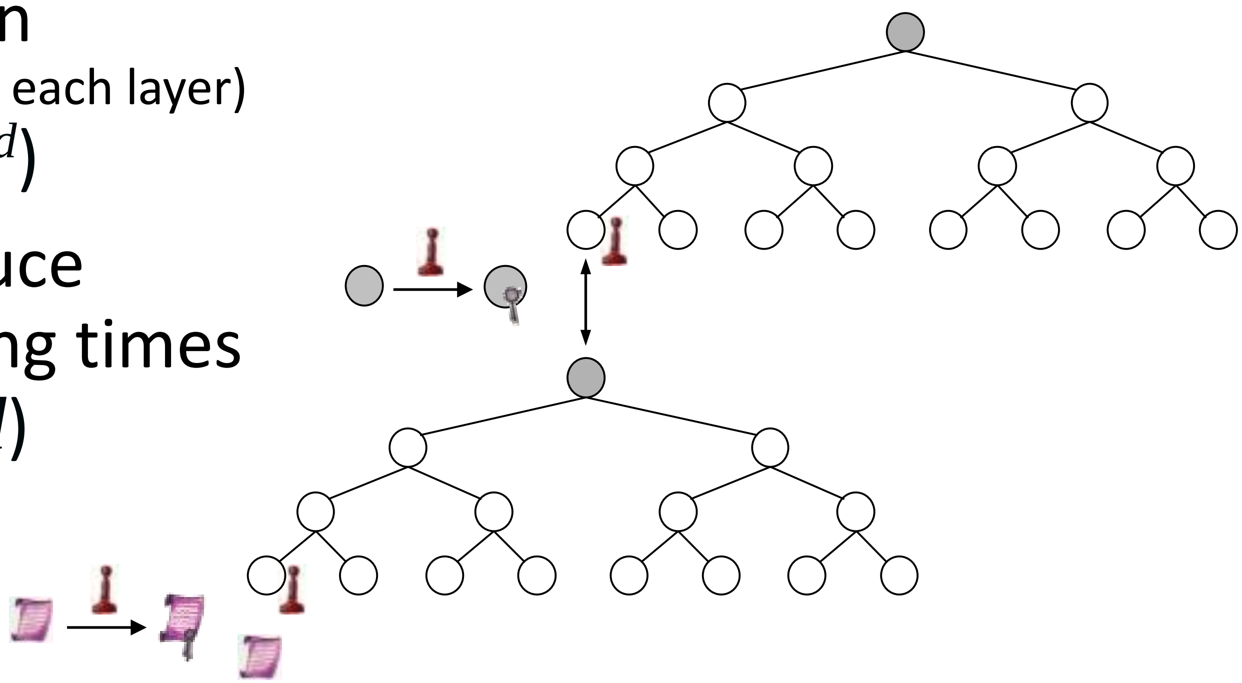


Multi-Tree XMSS

Uses multiple layers of trees

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

-> Allows to reduce worst-case signing times
$\Theta(h/2) \rightarrow \Theta(h/2d)$



XMSS-Draft since -01

Each hash function call (excl. message hash) takes now a key and a bitmask.

Issue: Order of $N \cdot w \cdot l$ keys and bitmasks that have to be published.

Put them into PK? Impractical

Solution: PRG + Seed in PK

XMSS-Draft since -01

Solution: PRG + Seed in PK

Security:

- Not really standard model.
- Natural but new assumption („Generating the public values using a PRG, the scheme does not get less secure if seed is published.“),
- Or ROM

SPHINCS: practical stateless hash-based signatures

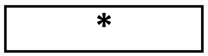
joint work with Daniel J. Bernstein, Daira Hopwood, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, Zooko Wilcox O'Hearn

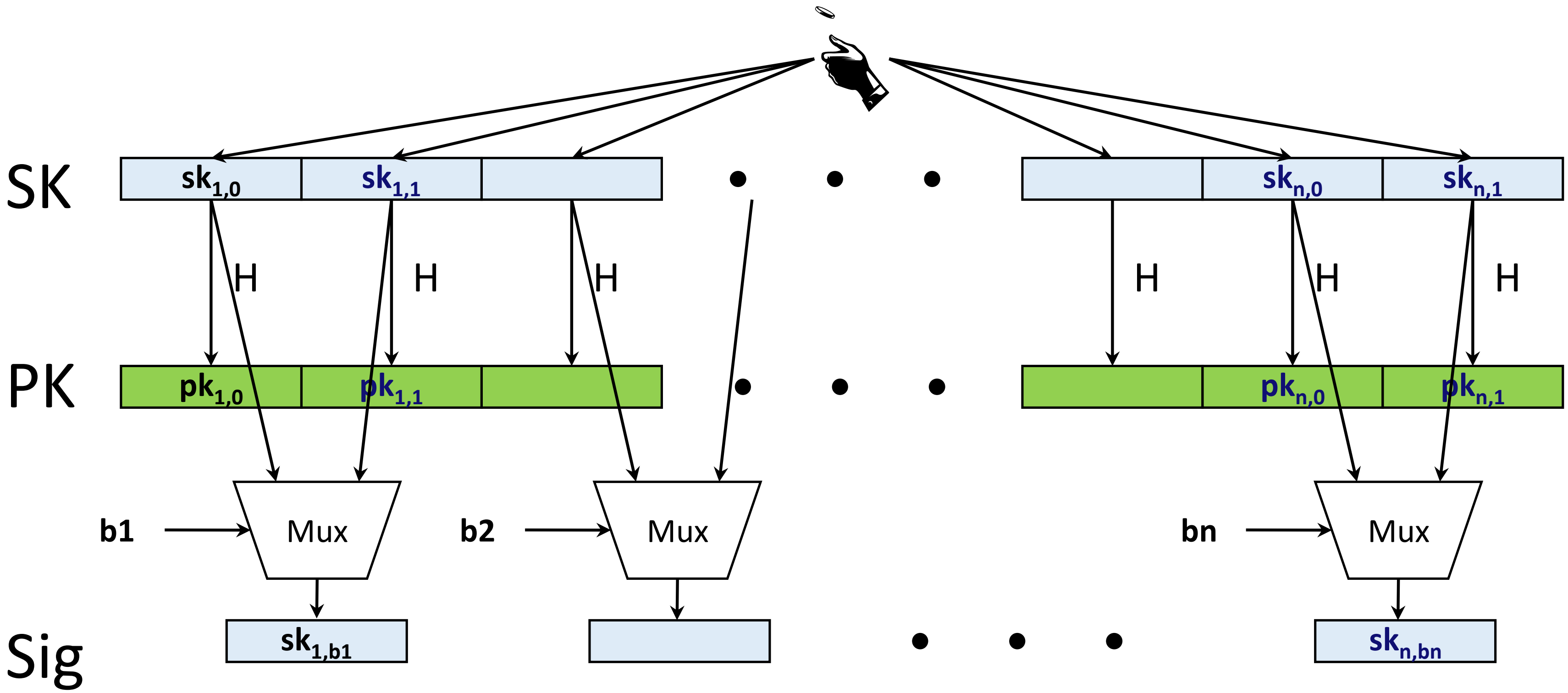
ELIMINATE
THE STATE

Protest?

Few-Time Signature Schemes

Recap LD-OTS

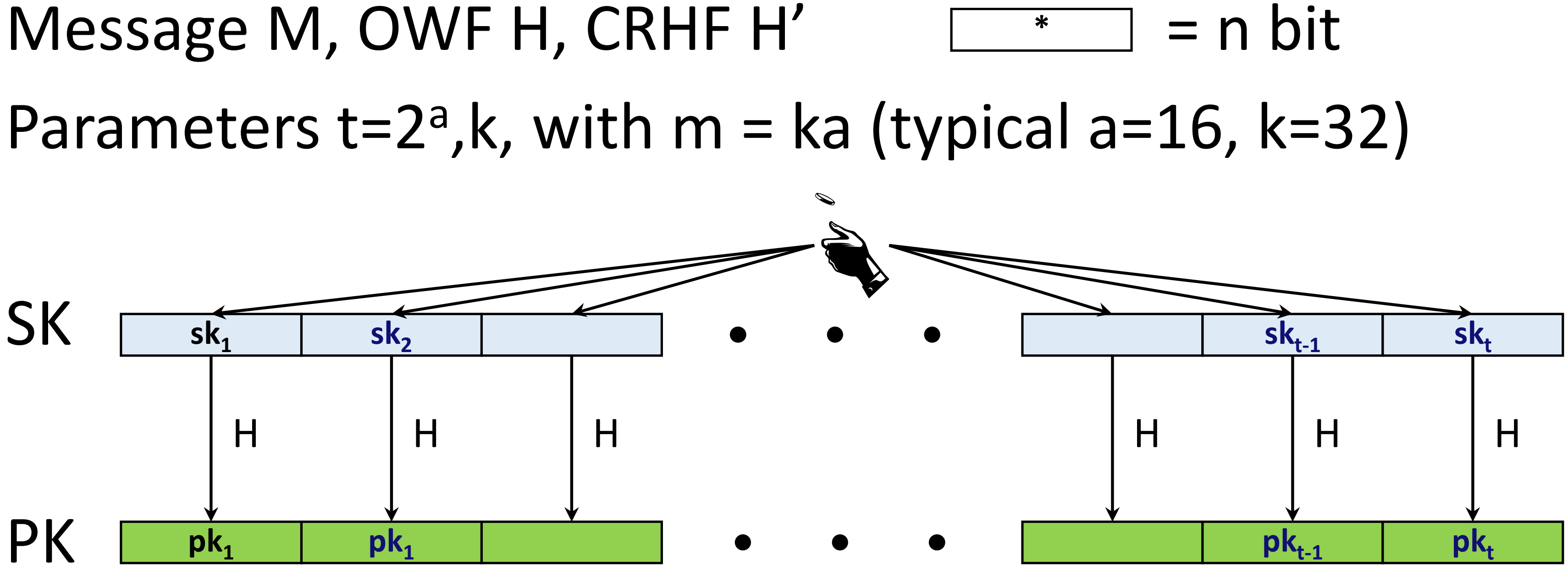
Message M = b1,...,bn, OWF H  = n bit



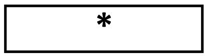
HORS [RR02]

Message M, OWF H, CRHF H’

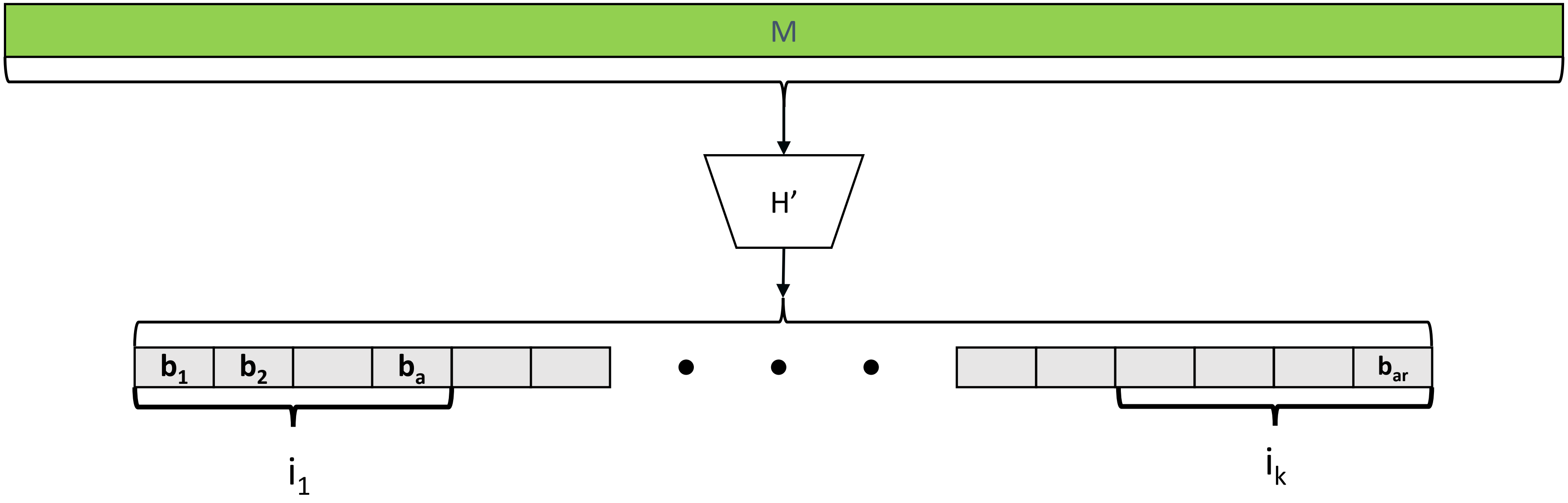
Parameters $t=2^a$,k, with m = ka (typical a=16, k=32)



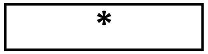
HORS mapping function

Message M, OWF H, CRHF H’  = n bit

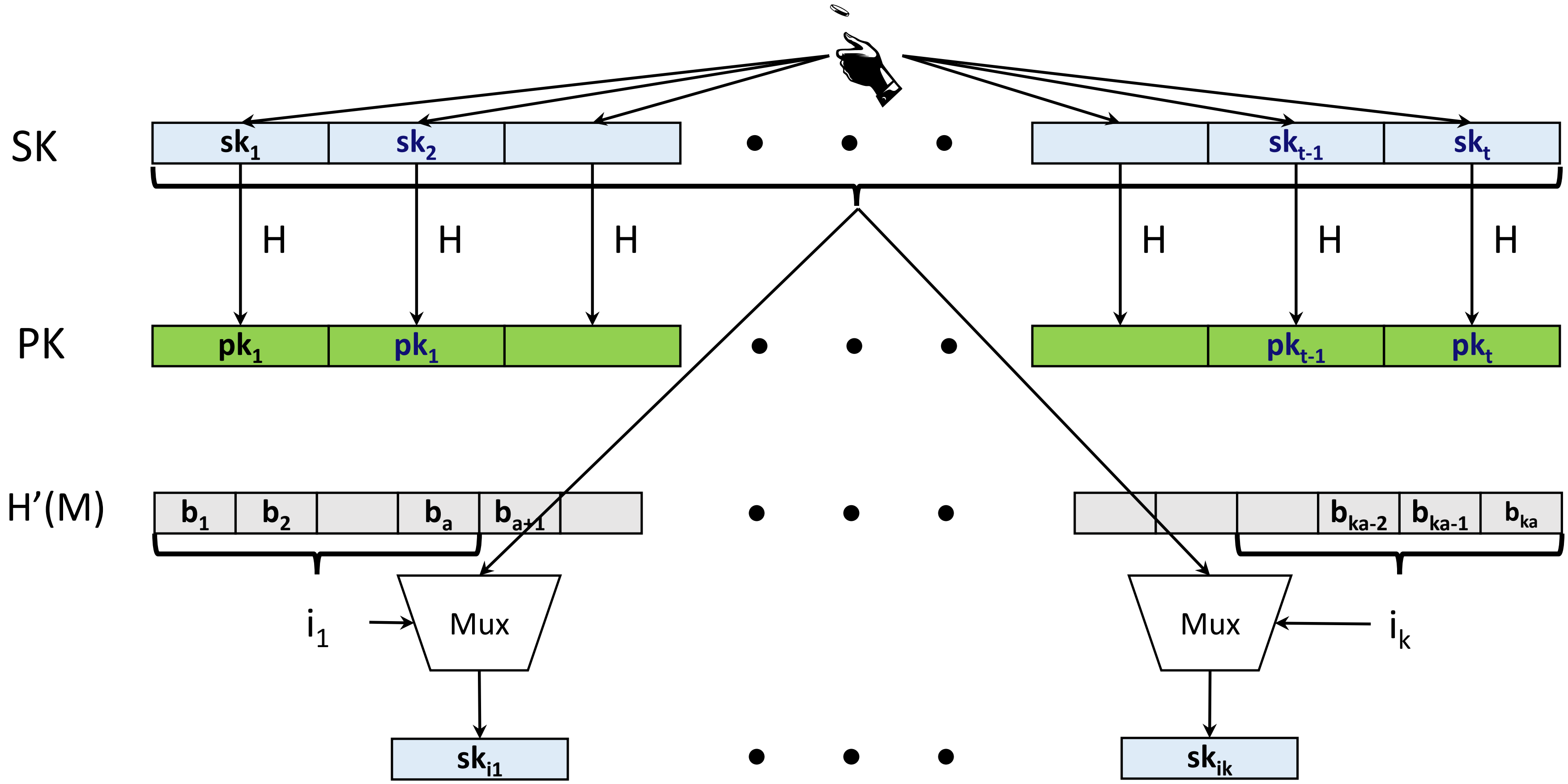
Parameters $t=2^a$,k, with m = ka (typical a=16, k=32)



HORS

Message M, OWF H, CRHF H'  = n bit

Parameters $t=2^a$,k, with m = ka (typical a=16, k=32)



HORS Security

- M mapped to k element index set $M^i \in \{1, \ldots, t\}^k$
- Each signature publishes k out of t secrets
- Either break one-wayness or…

- r-Subset-Resilience: After seeing index sets M_j^i for r messages $msg_j, 1 \leq j \leq r$, hard to find $msg_{r+1} \neq msg_j$ such that $M_{r+1}^i \in \bigcup_{1 \leq j \leq r} M_j^i$.

- Best generic attack: $\text{Succ}_{\text{r-SSR}}(A, q) = q\left(\frac{rk}{t}\right)^k$

$\longrightarrow$ Security shrinks with each signature!

HORST

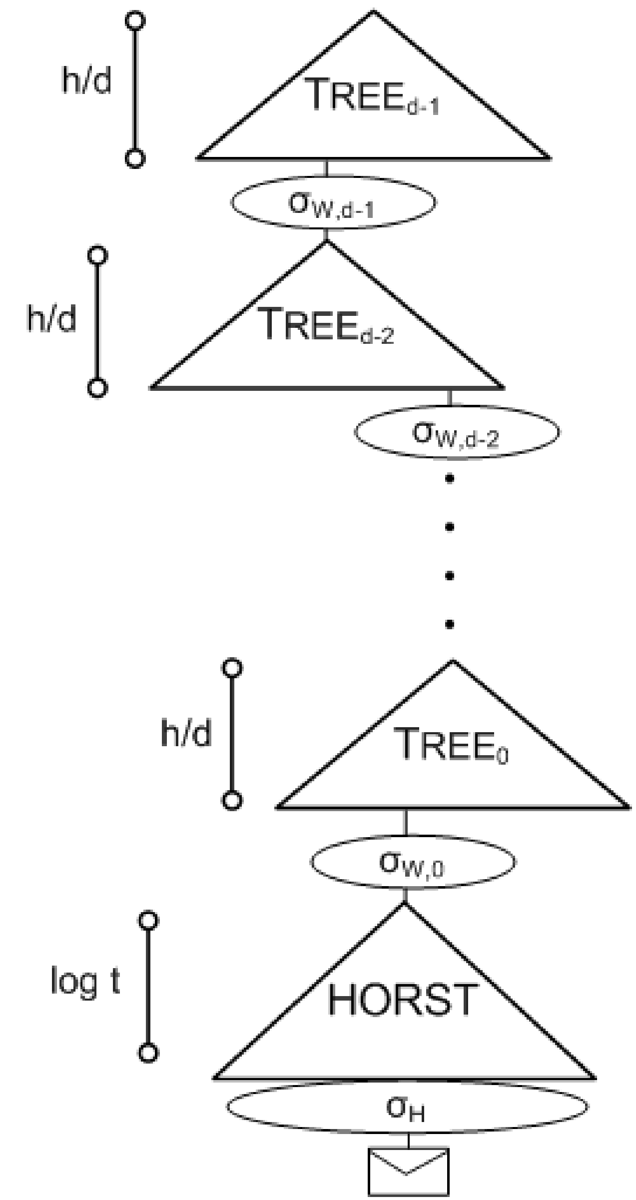
Using HORS with MSS requires adding PK (tn) to MSS signature.

HORST: Merkle Tree on top of HORS-PK

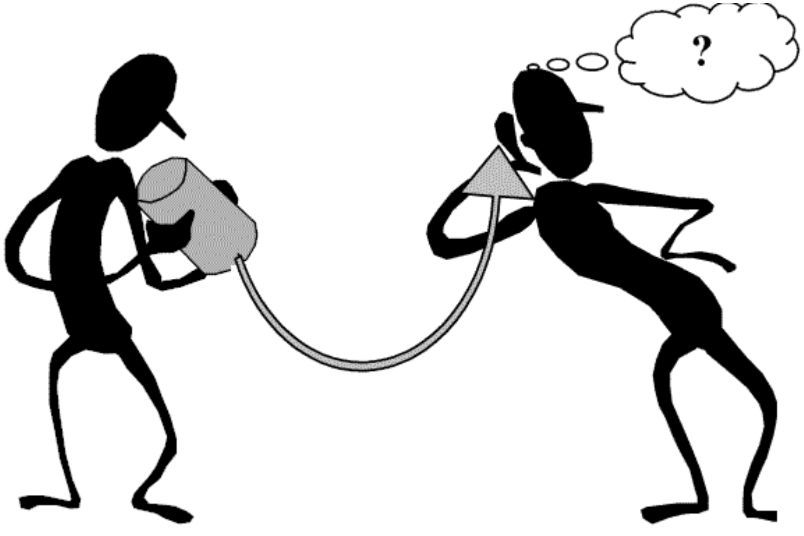
- New PK = Root
- Publish Authentication Paths for HORS signature values
- PK can be computed from Sig
- With optimizations: $tn \rightarrow (k(\log t - x + 1) + 2^x)n$
  - E.g. SPHINCS-256: 2 MB → 16 KB
- Use randomized message hash

SPHINCS

- Stateless Scheme
- $XMSS^{MT}$ + HORST
  + (pseudo-)random index
- Collision-resilient
- Deterministic signing
- SPHINCS-256:
  - 128-bit post-quantum secure
  - Hundrest of signatures / sec
  - 41 kb signature
  - 1 kb keys



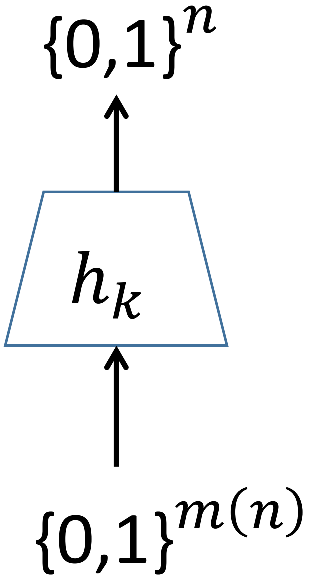
Thank you!
Questions?



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

(Hash) function families

- $H_n := \{h_k : \{0,1\}^{m(n)} \to \{0,1\}^n\}$
- $m(n) \geq n$
- „efficient“



One-wayness

$$H_n \coloneqq \{h_k : \{0,1\}^{m(n)} \to \{0,1\}^n\}$$

$$h_k \overset{\$}{\leftarrow} H_n$$
$$x \overset{\$}{\leftarrow} \{0,1\}^{m(n)}$$
$$y_c \leftarrow h_k(x)$$

Success if $h_k(x^*) = y_c$

y_c, k

$\mathcal{A}$

x^*

Collision resistance

$H_n \coloneqq \{h_k : \{0,1\}^{m(n)} \rightarrow \{0,1\}^n\}$

$h_k \overset{\$}{\leftarrow} H_n$

Success if
$h_k(x_1^*) = h_k(x_2^*)$

k

$\mathcal{A}$

(x_1^*, x_2^*)

Second-preimage resistance

$H_n \coloneqq \{h_k\colon \{0,1\}^{m(n)} \to \{0,1\}^n\}$

$h_k \xleftarrow{\$} H_n$

$x_c \xleftarrow{\$} \{0,1\}^{m(n)}$

Success if
$h_k(x_c) = h_k(x^*)$

Undetectability

$H_n := \{h_k : \{0,1\}^{m(n)} \to \{0,1\}^n\}$

$h_k \xleftarrow{\$} H_n$

$b \xleftarrow{\$} \{0,1\}$

If $b = 1$

$x \xleftarrow{\$} \{0,1\}^{m(n)}$

$y_c \leftarrow h_k(x)$

else

$y_c \xleftarrow{\$} \{0,1\}^n$

y_c, k

$\mathcal{A}$

b^*

Pseudorandomness

$$H_n \coloneqq \{h_k : \{0,1\}^{m(n)} \to \{0,1\}^n\}$$