Hash-Based Signatures

Johannes Buchmann, Andreas Hülsung
Supported by DFG and DAAD

Part V:
Winternitz One-Time Signature Scheme (WOTS)

Winternitz OTS (WOTS)

CASED

First idea: Winternitz (Mer89)
Full scheme: Even et al. (EGM96)
Security Proofs: Hevia & Micciancio (HM02)
Dods et al. (DSS05)
Requires collision-resistant undetectable one-way function family.

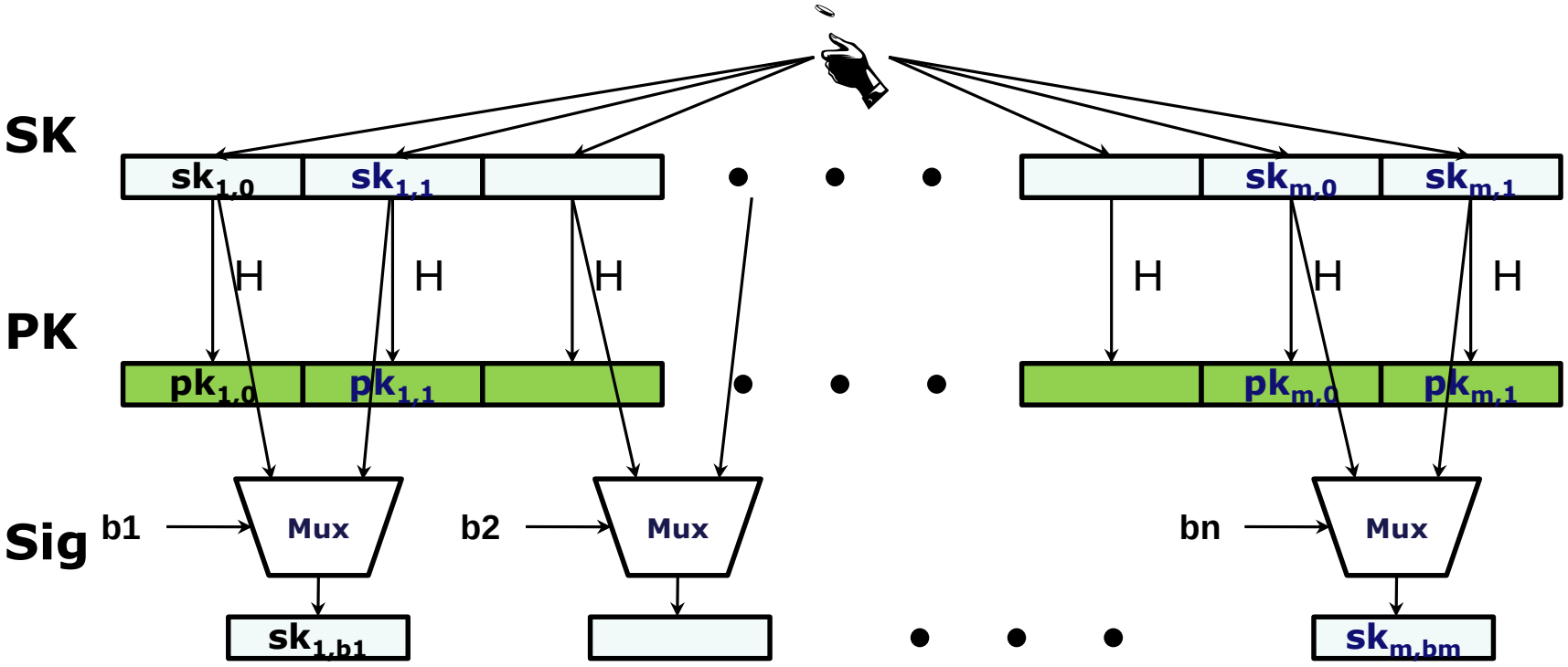
WOTS$^{\$}$: Buchmann et al. (BDEH^{+}11)
Requires pseudorandom function family.

WOTS^{+}: Hülsing (Hül13)
Requires second preimage resistant undetectable one-way function family.

Recap LD-OTS [Lam79]

CASED

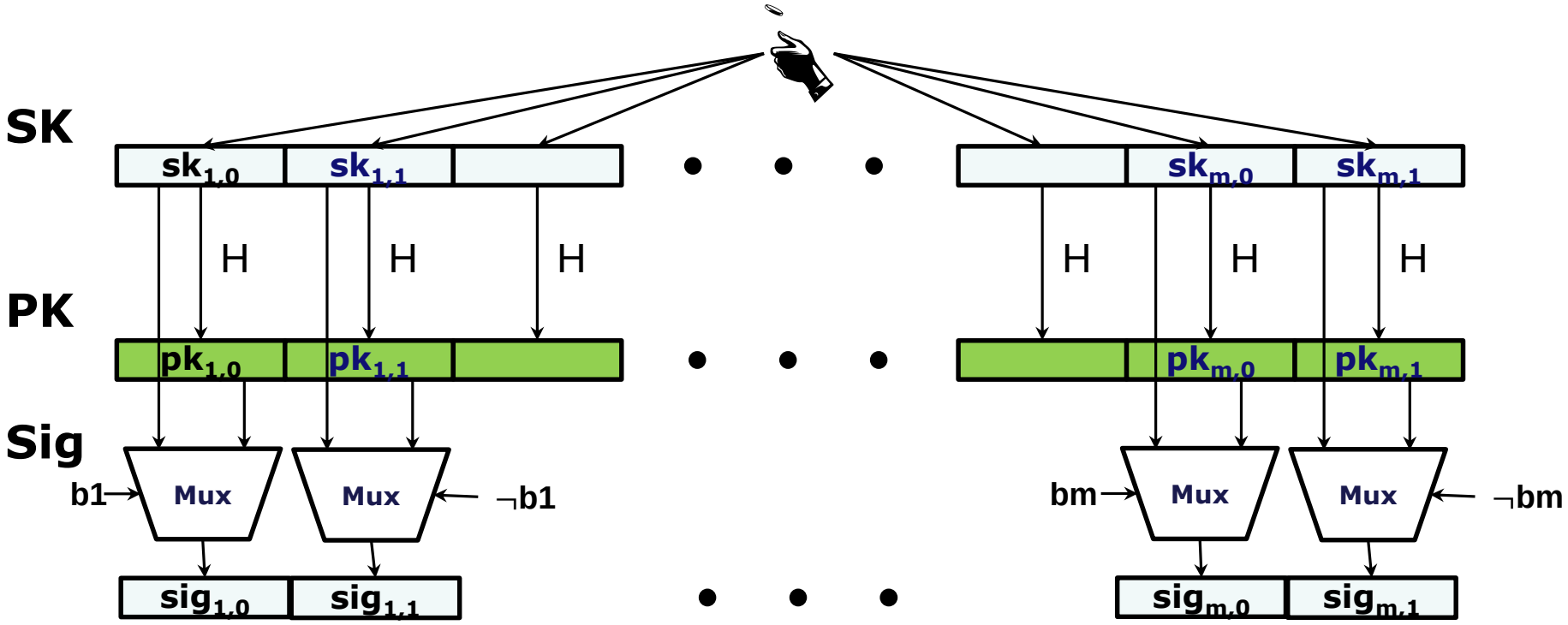
Message M = b1,…,bm, OWF H * = n bit



Trivial Optimization

CASED

Message M = b1,…,bm, OWF H * = n bit



Non-trivial Optimization

CASED

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: $M' = b_1,\ldots,b_m,\neg b_1,\ldots,\neg b_m$

Sig: $sig_i =$

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

Checksum with bad performance!

Non-trivial Optimization, cont'd

CASED

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

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

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

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

Sig: 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

WOTS
Function Chain

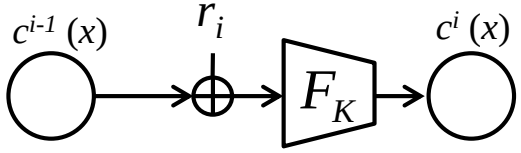
CASED

Function family: $\mathcal{F}_n = \{F_K : \{0,1\}^n \rightarrow \{0,1\}^n \mid K \in \{0,1\}^{n'}\}$

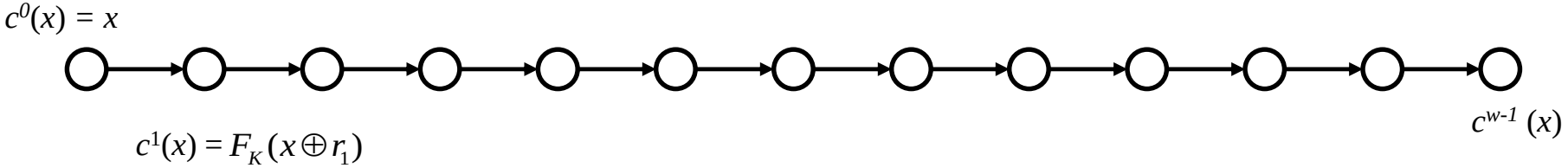
Formerly: $c^i(x) = F_K(c^{i-1}(x)) = \underbrace{F_K \circ F_K \circ \ldots \circ F_K}_{i-times}(x), K \in \{0,1\}^{n'}$

WOTS+

For $w \geq 2$ select $\mathcal{R} = (r_1, \ldots, r_{w-1}) \in \{0,1\}^{n \times w-1}, K \in \{0,1\}^{n'}$



$$c^i(x) = F_K(c^{i-1}(x) \oplus r_i)$$



WOTS Function Chains

CASED

For $x \in \{0,1\}^n$ define $c_0(x) = x$ and

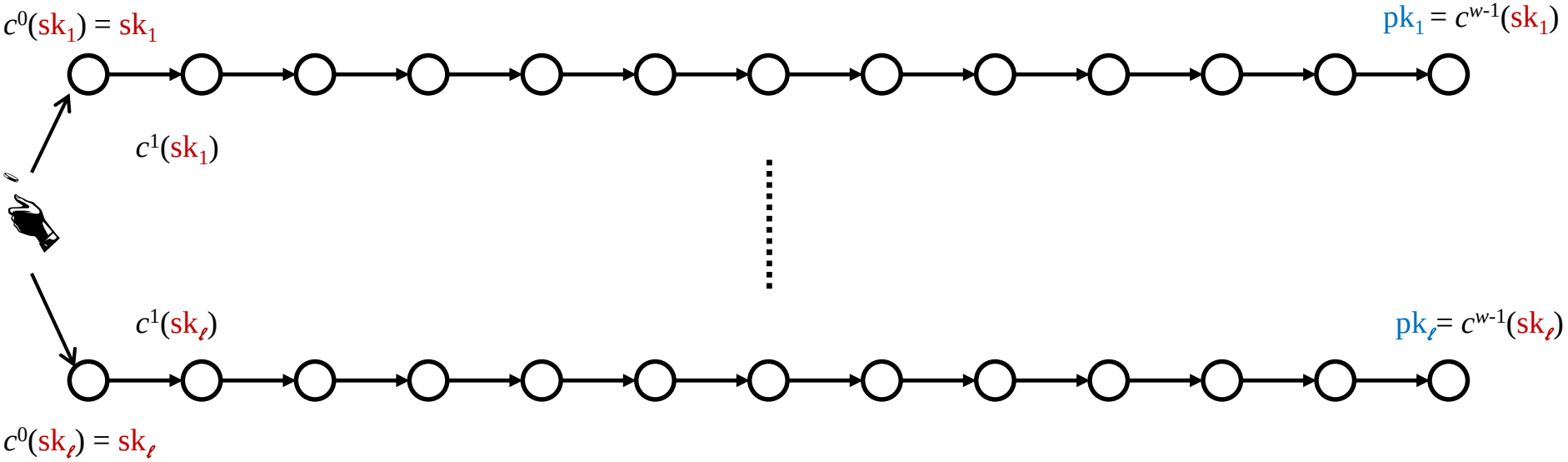
- WOTS: $c_i(x) = F_K(c_{i-1}(x))$
- WOTS$^{\$}$: $c_i(x) = F_{c_{i-1}(x)}(r)$
- WOTS^{+}: $c_i(x) = F_K(c_{i-1}(x) \oplus r_i)$

WOTS+

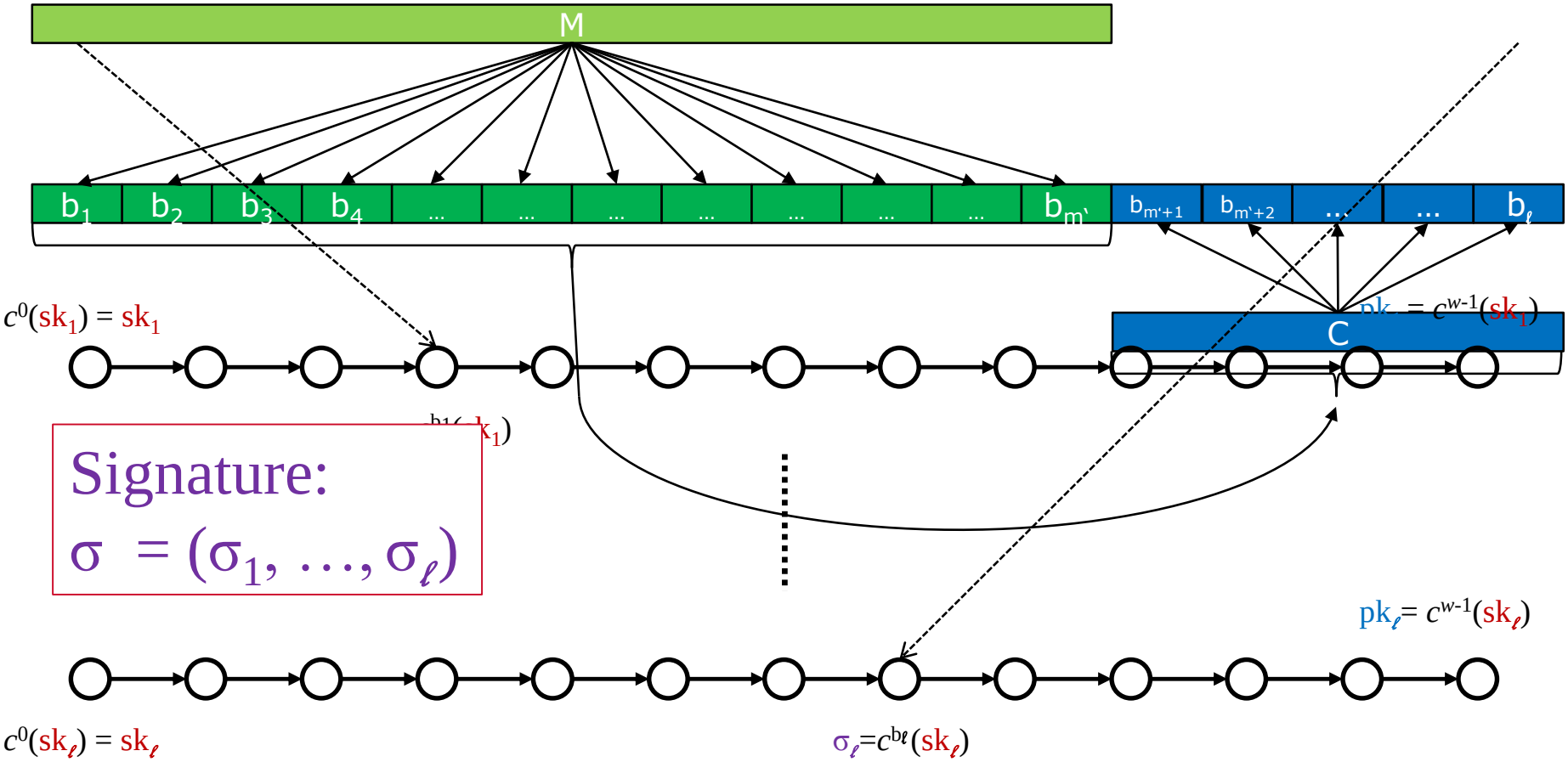
CASED

Winternitz parameter w, security parameter n, message length m, function family $\mathcal{F}_n = \{F_K : \{0,1\}^n \to \{0,1\}^n \mid K \in \{0,1\}^{n'}\}$

Key Generation: Compute ℓ, sample K, sample $\mathcal{R}$



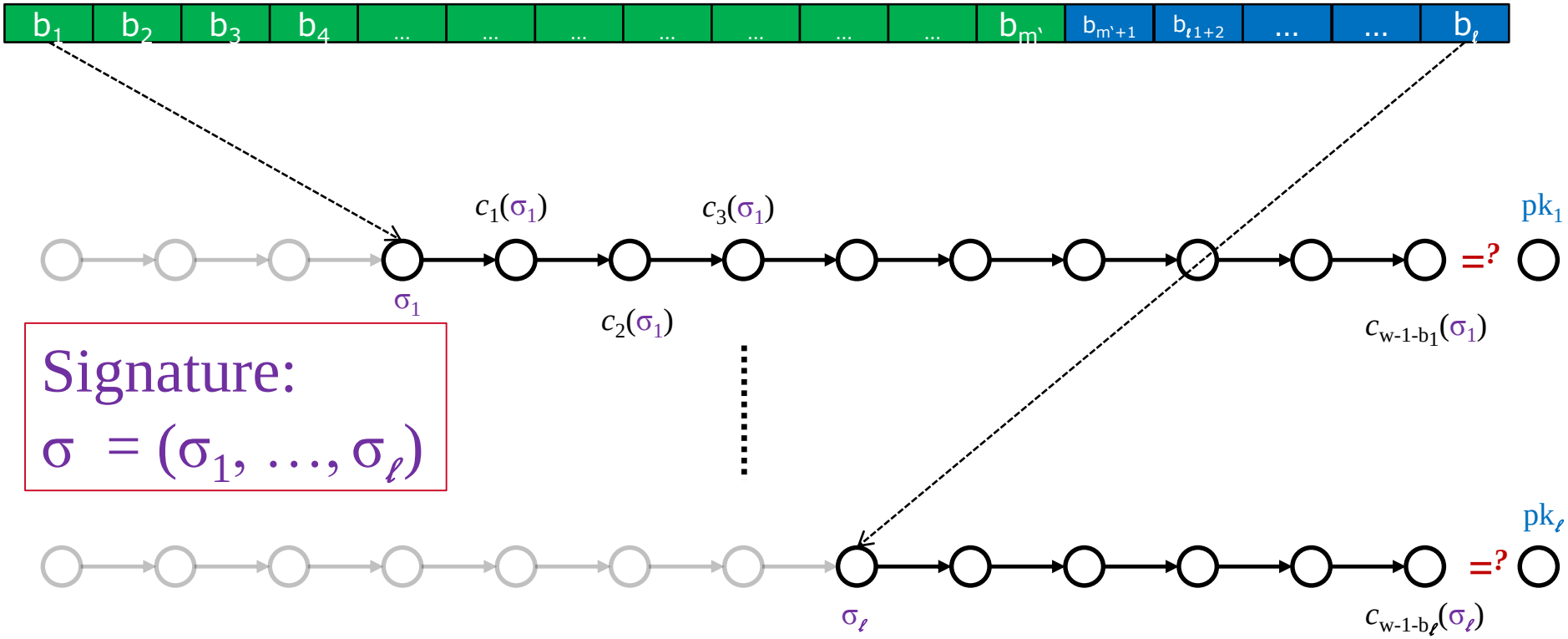
WOTS+ Signature generation



WOTS+ Signature Verification

CASED

Verifier knows: M, n, w, c



WOTS Security

CASED

Theorem (informally):

W-OTS *is strongly unforgeable under chosen message attacks if* $\mathcal{F}$ *is a collision resistant, undetectable one-way function family.*

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

W-OTS+ *is strongly unforgeable under chosen message attacks if* $\mathcal{F}$ *is a* 2^{nd}*-preimage resistant, undetectable one-way function family.*

WOTS Sizes and Runtimes

CASED

	Lamport -Diffie	WOTS	WOTS$	WOTS+
Public Key Size	2bm	ℓ 2b ~ 2bm/log w	ℓ b (+b) ~ bm/log w	ℓ b (+(w-1)b) ~ bm/log w
Secret Key Size	2bm	ℓ 2b ~ 2bm/log w	ℓ b ~ bm/log w	ℓ b ~ bm/log w
Signature Size	bm	ℓ 2b ~ 2bm/log w	ℓ b ~ bm/log w	ℓ b ~ bm/log w
Key Generation Time	~ 2m	ℓ w ~ wm/log w	ℓ w ~wm/log w	ℓ w ~ wm/log w

Security level b, Winternitz parameter w, Message Length m,

$\ell = \ell(w,m) \sim m / \log w$