XMSS
Practical Hash-Based Signatures

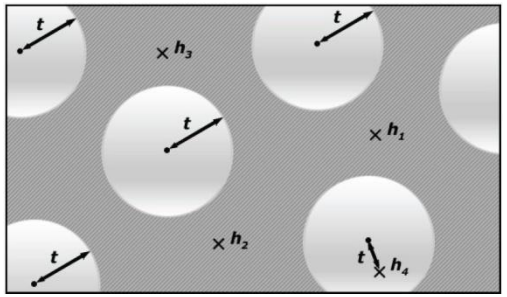
Andreas Hülsing
joint work with Johannes Buchmann and Erik Dahmen

Post-Quantum Signatures

CASED

Lattice, MQ, Coding

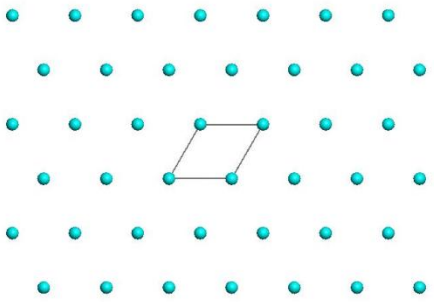
- Signature and/or key sizes
- Runtimes
- Secure parameters



$$y_1 = x_1^2 + x_1x_2 + x_1x_4 + x_3$$

$$y_2 = x_3^2 + x_2x_3 + x_2x_4 + x_1 + 1$$

$$y_3 = \ldots$$



Hash-based Signature Schemes
[Mer89]

CASED

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

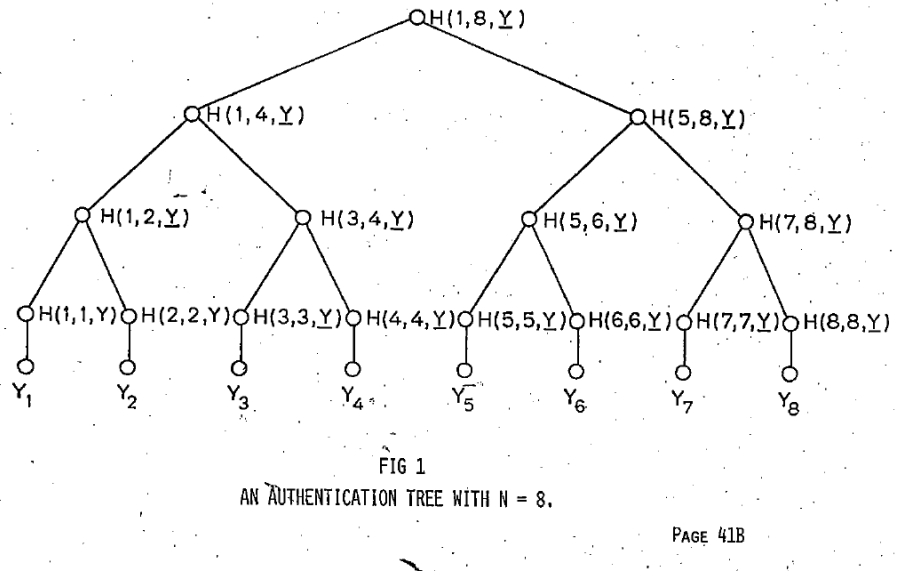
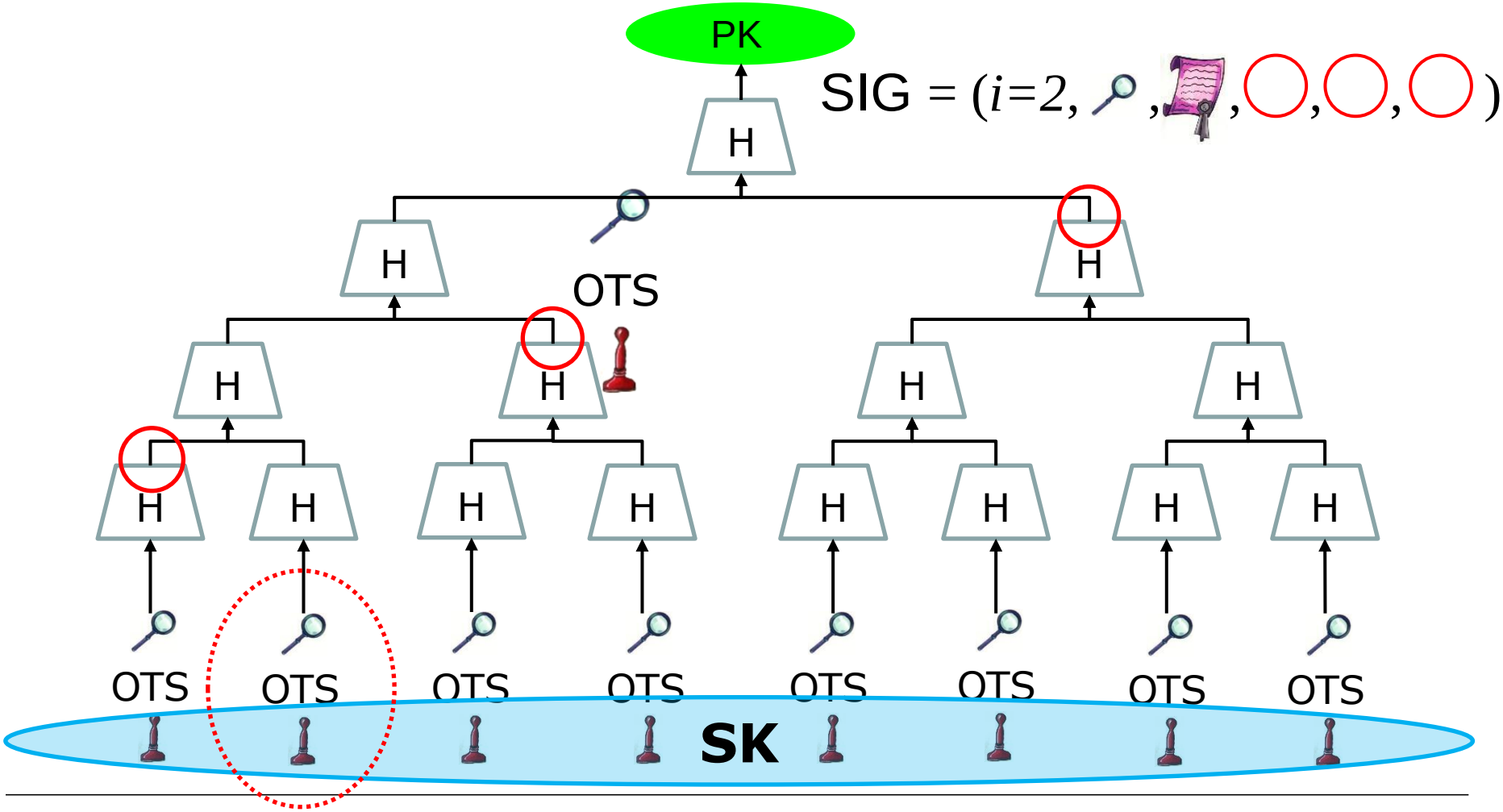


FIG 1
AN AUTHENTICATION TREE WITH N = 8.

PAGE 41B

Hash-based Signatures



CASED

XMSS

Results

CASED

- Efficient
- Minimal security assumptions
- „Small signatures"
- Forward secure
- Full smartcard implementation

CASED

New Variants of the Winternitz One Time Signature Scheme

OTS

Winternitz OTS (WOTS)
[Mer89; EGM96]

CASED

SIG = (i,  ,  , ◯, ◯, ◯)

|  | = |  | = m * | ◯ |

1.  = f()

2. Trade-off between runtime and signature size

|  | ~ m/log w * | ◯ |

WOTS+
[Hül13]

CASED

Theorem 3.9 (informally):

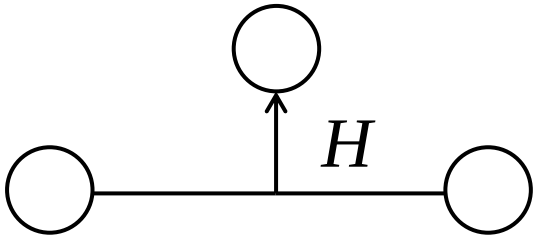
W-OTS$^+$ is strongly unforgeable under chosen message attacks if $\mathcal{F}$ is a 2nd-preimage resistant, undetectable one-way function family

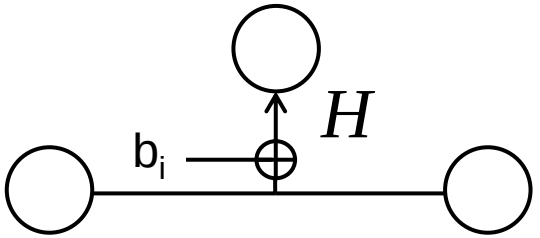
XMSS
[BDH11]

CASED

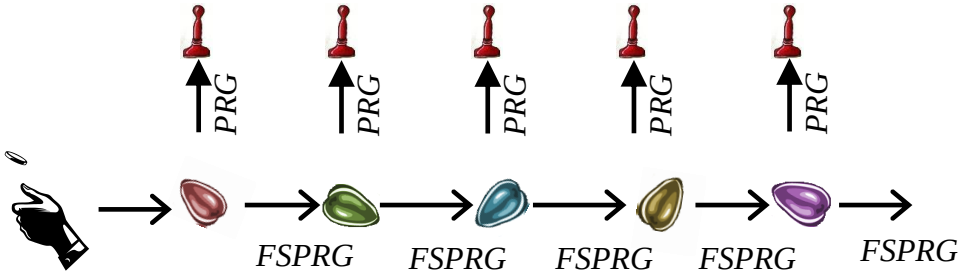
Lamport-Diffie / WOTS → WOTS$^+$

Tree construction
[DOTV08]



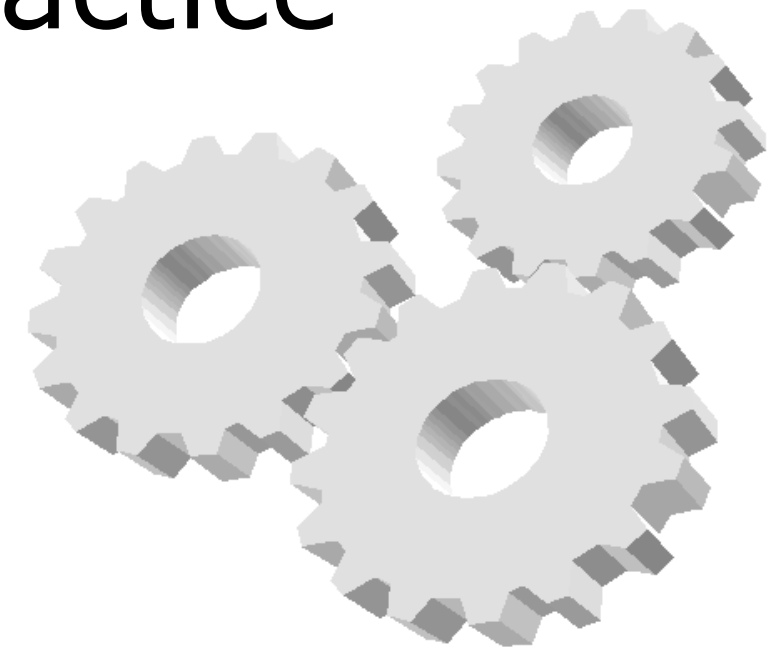


Pseudorandom key generation



CASED

XMSS* in Practice



XMSS Implementations
C Implementation [BDH11]

CASED

C Implementation, using OpenSSL

	Sign (ms)	Verify (ms)	Signature (bit)	Public Key (bit)	Secret Key (byte)	Bit Security	Comment
XMSS-SHA-2	35.60	1.98	**16,672**	13,600	3,364	157	h = 20, w = 64,
XMSS-AES-NI	**0.52**	**0.07**	19,616	7,328	1,684	84	h = 20, w = 4
XMSS-AES	1.06	0.11	19,616	7,328	1,684	84	h = 20, w = 4
RSA 2048	**3.08**	**0.09**	≤ 2,048	≤ 4,096	≤ 512	87	

Intel(R) Core(TM) i5-2520M CPU @ 2.50GHz with Intel AES-NI

XMSS Implementations
Smartcard Implementation [HBB12]

CASED

	Sign (ms)	Verify (ms)	Keygen (ms)	Signature (byte)	Public Key (byte)	Secret Key (byte)	Bit Sec.	Comment
XMSS	**134**	23	**925,400**	2,388	800	2,448	92	H = 16, w = 4
XMSS$^+$	**106**	25	**5,600**	3,476	544	3,760	94	H = 16, w = 4
RSA 2048	190	7	11,000	≤ 256	≤ 512	≤ 512	87	

Infineon SLE78 16Bit-CPU@33MHz, 8KB RAM, TRNG, sym. & asym. co-processor

NVM: Card 16.5 million write cycles/ sector,
XMSS$^+$ < 5 million write cycles (h=20)

Conclusion

Conclusion

CASED

- Fast
- Conservative Security
- Compact
- Forward secure

CASED

Main Drawback: State

Easy Migration?

- **Interfaces**
- **Key Management**

CASED

Thank you!
Questions?