Hash-Based Signatures

Johannes Buchmann, Andreas Hülsung
Supported by DFG and DAAD

Part XI:
XMSS in Practice

Hash functions & Blockciphers

CASED

AES
Blowfish
3DES
Twofish
Threefish
Serpent
IDEA
RC5
RC6
…

SHA-2
SHA-3
BLAKE
Grøstl
JH
Keccak
Skein
VSH
MCH
MSCQ
SWIFFTX
RFSB
…

PRF and Hash Function from AES

CASED

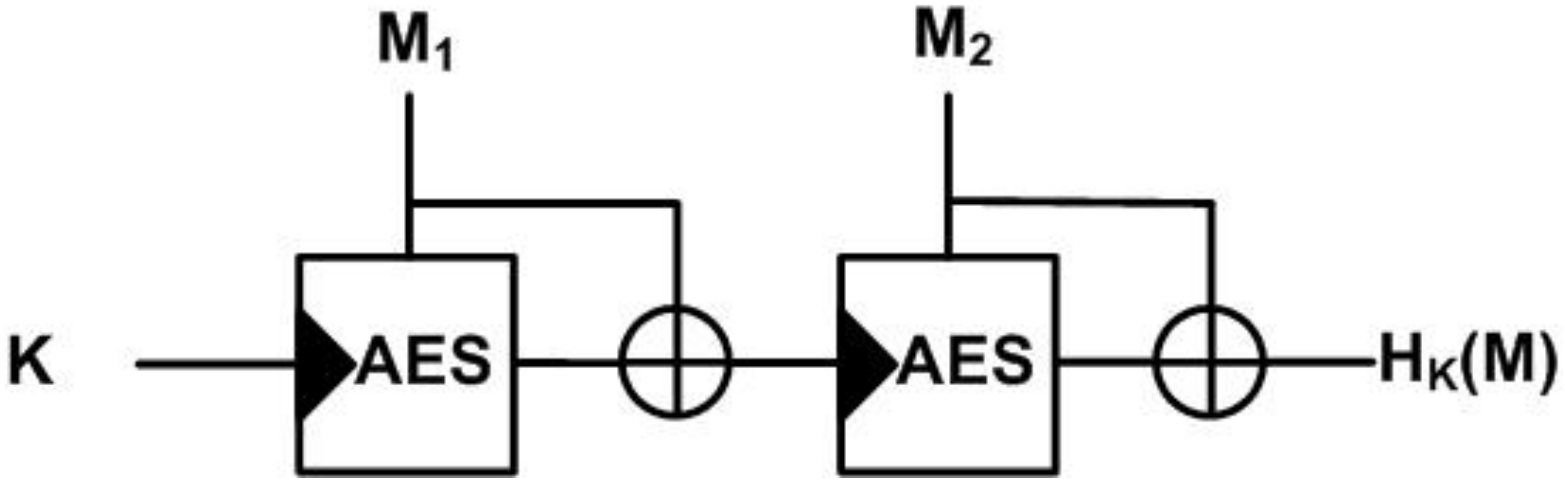
AES: $\{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$

PRF:

- Plain AES

Hash function

- AES with Matyas-Meyer-Oseas in Merkle-Damgård mode



PRF and Hash Function from SHA2

CASED

SHA2: $\{0,1\}^* \rightarrow \{0,1\}^{256}$

PRF

- Simplified **SHA2-HMAC**:

$$F_K(M) = \text{SHA2}(\ \text{Pad}(K) \ ||\ M\ )$$

- Pad(x) prepends 0's to reach blocksize (512bit)
- No MD-Strengthening needed

Hash function

- Plain SHA2

XMSS Implementations
C Implementation

CASED

C Implementation, using OpenSSL [BDH2011]

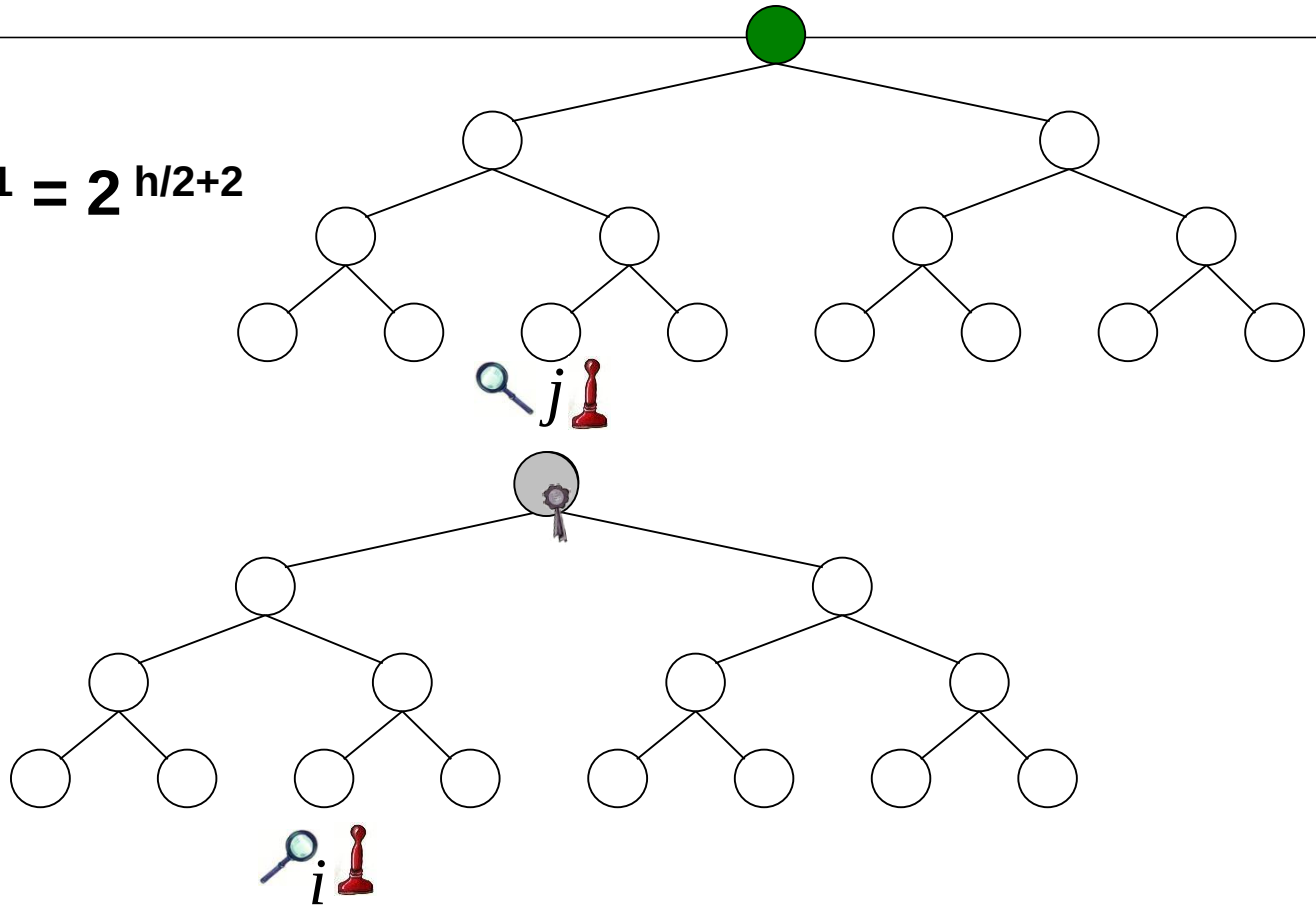
	Sign (ms)	Verify (ms)	Signature (bit)	Public Key (bit)	Secret Key (byte)	Bit Security	Comment
XMSS-SHA-2	35.60	1.98	**16,672**	13,600	3,364	157	h = 20, w = 64,
XMSS-AES-NI	**0.52**	**0.07**	19,616	7,328	1,684	84	h = 20, w = 4
XMSS-AES	1.06	0.11	19,616	7,328	1,684	84	h = 20, w = 4
RSA 2048	**3.08**	**0.09**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

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

Reminder: Tree Chaining

CASED

$2^{h+1} \longrightarrow 2*2^{h/2+1} = 2^{h/2+2}$



But: Larger signatures!

XMSS Implementations
Smartcard Implementation

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)

[HBB12]

CASED

Thank you!
Questions?