Post-Quantum-Kryptographie

Hashbasierte Signaturverfahren - Fortsetzung

Fabio Campos

7. November 2018

RheinMain University of Applied Sciences

Winternitz one-time signature scheme (W-OTS)

Sei w der Winternitzparameter und H eine Hashfunktion:

$$H : \{0,1\}^* \rightarrow \{0,1\}^n$$

dann gilt:

$$H^i(x) = \underbrace{H \circ H \circ \cdots \circ H}_{\text{i-mal}}$$

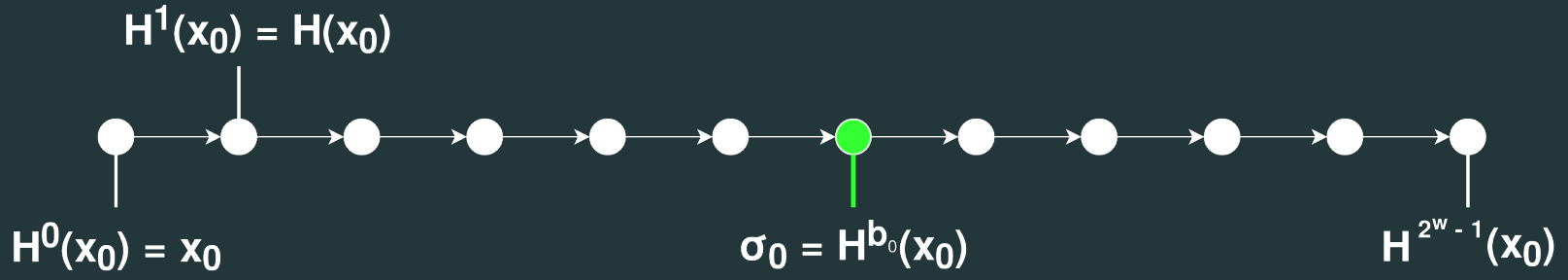

Abbildung 1: gerichteter azyklischer Graph in W-OTS

W-OTS Varianten

Sei r ein zufälliger Wert und H_k eine Hashfunktion abhängig vom Schlüssel k:

$$H_k : \{0,1\}^* \rightarrow \{0,1\}^n$$

dann definieren wir weitere W-OTS-Varianten, wie folgt:

- $W\text{-}OTS^{PRF} : H_k^i(x) = H_{H_k^{(i-1)}(x)}(r)$
- $W\text{-}OTS^{+} : H_k^i(x) = H_k(H_k^{i-1}(x) \oplus r_{i-1}) \oplus r_i$

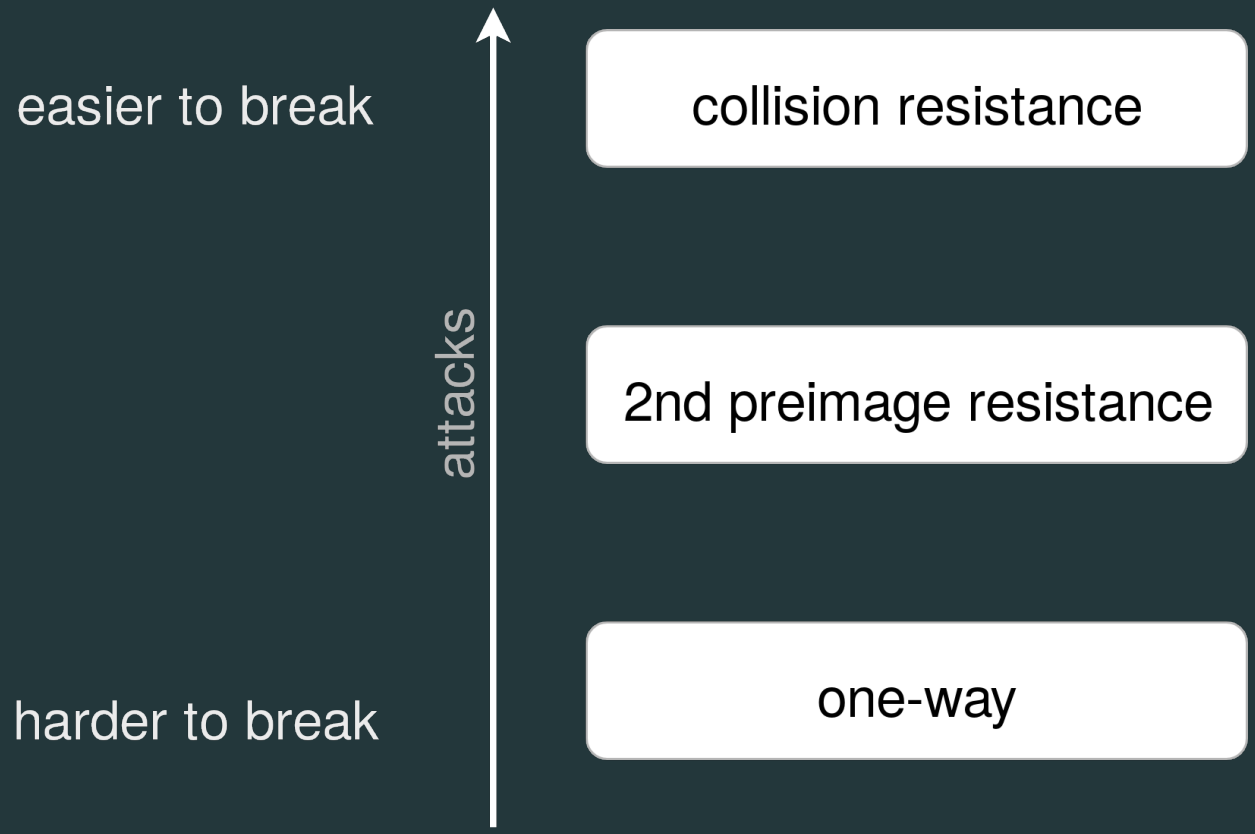

Abbildung 2: Sicherheitseingenschaften

Sicherheitseingenschaften von Hashfunktionen

Function	Output Size	Security Strengths in Bits		
		Collision	Preimage	2nd Preimage
SHA-1	160	< 80	160	$160 - L(M)$
SHA-224	224	112	224	$\min(224, 256 - L(M))$
SHA-512/224	224	112	224	224
SHA-256	256	128	256	$256 - L(M)$
SHA-512/256	256	128	256	256
SHA-384	384	192	384	384
SHA-512	512	256	512	$512 - L(M)$
SHA3-224	224	112	224	224
SHA3-256	256	128	256	256
SHA3-384	384	192	384	384
SHA3-512	512	256	512	512
SHAKE128	d	$\min(d/2, 128)$	$\geq \min(d, 128)$	$\min(d, 128)$
SHAKE256	d	$\min(d/2, 256)$	$\geq \min(d, 256)$	$\min(d, 256)$

Abbildung 3: Security strengths of SHA-1, SHA-2, and SHA-3 functions

Attacken auf Hashfunktionen

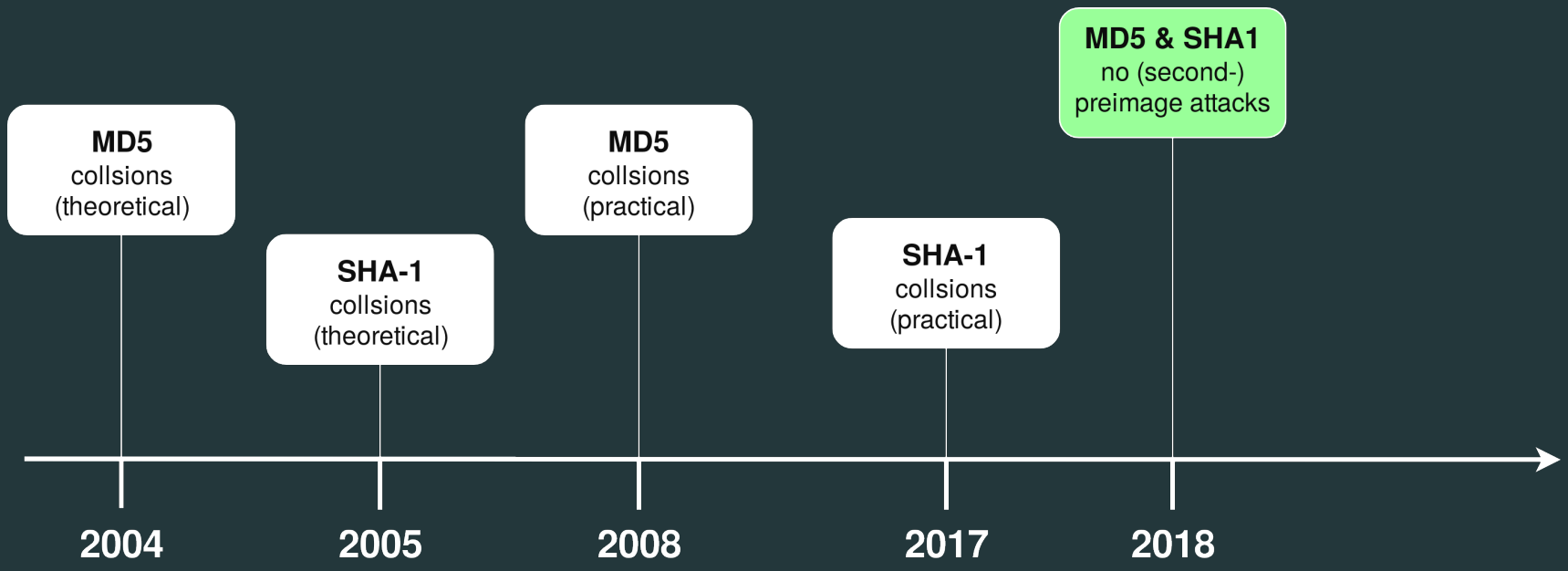

Abbildung 4: Attacken

Bibliography

(B96) Schneier, Bruce. Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C. 1996.

(KMV96) Katz, J., Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A.. Handbook of applied cryptography. CRC press. 1996

(MVZ18) Mavroeidis, Vasileios, et al. The Impact of Quantum Computing on Present Cryptography. arXiv preprint arXiv:1804.00200 (2018).

(DH76) Whitfield Diffie and Martin E. Hellman. New directions in cryptography. IEEE Trans. Information Theory 22(6):644-654. 1976.

(Mer89) Ralph C. Merkle. A certifed digital signature. In Advances in Cryptology - CRYPTO 89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings, pages 218-238, 1989.

(BDH11) Johannes A. Buchmann, Erik Dahmen and Andreas Hülsing. XMSS - A practical forward secure signature scheme based on minimal security assumptions. In Post-Quantum Cryptography 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29 - December 2, 2011. Proceedings, pages 117 -129, 2011.

(BGD+06) Johannes A. Buchmann, Luis Carlos Coronado Garcia, Erik Dahmen, Martin Döring, and Elena Klintsevich CMSS an improved merkle signature scheme. In Progress in Cryptology INDOCRYPT 2006, 7th International Conference on Cryptology in India, Kolkata, India, December 11 - 13, 2006, Proceedings, pages 349 - 363, 2006.

(JLMS03) Markus Jakobsson, Frank Thomson Leighton, Silvio Micali, and Michael Szydlo. Fractal merkle tree representation and traversal. In Topics in Cryptology CT RSA 2003, The Cryptographers Track at the RSA Conference 2003, San Francisco, CA, USA, April 13-17, 2003, Proceedings, pages 314 - 326, 2003.

(BDS08) Johannes A. Buchmann, Erik Dahmen, and Michael Schneider. Merkle tree traversal revisited. In Post-Quantum Cryptography, Second International Workshop, PQCrypto 2008, Cincinnati, OH, USA, October 17-19, 2008, Proceedings, 2008.

Bibliography

2/2

(BHLV17) Daniel J. Bernstein, Nadia Heninger, Paul Lou and Luke Valenta.
Post-quantum RSA, Cryptology ePrint Archive, Report 2017/351 ,2017, https://eprint.iacr.org/2017/351.

(Gol04) Oded Goldreich. Foundations of Cryptography: Volume 2, Basic Applications.
Cambridge University Press, Cambridge, UK, 2004.

(BHH+15) Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen,
Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, Zooko Wilcox-O'Hearn.
SSPHINCS: practical stateless hash-based signatures. EUROCRYPT 2015, Sofia, Bulgaria, 2015.

8