Post-Quantum-Kryptographie

Hashbasierte Signaturverfahren - Drawbacks of MSS

Fabio Campos

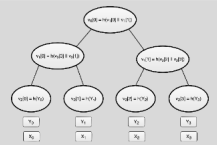
7. November 2018

RheinMain University of Applied Sciences

drawbacks

Given security level n, tree height h and message length m

public key generation time



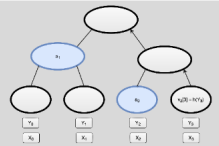
signature size

$$\sigma_i = (i, \sigma_{OTS}, Y_i, (a_0,...,a_{H-1}))$$

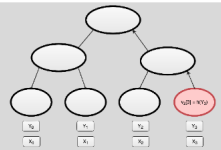
private key size

$$2bm * 2^H$$

authentication path generation time & space

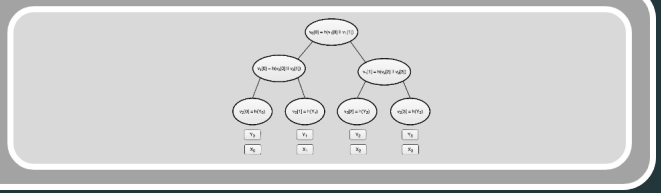


stateful

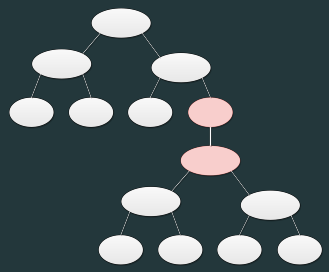


Given security level b, tree height H

public key generation time



- MSS
  - generate single trees of size of 2^H
  - cost $\sim 2^H$
- CMSS[a],XMSS[b]
  - generate t layers of trees of height H/t
  - generate t trees of size $2^{H/t}$
  - cost $\sim t * 2^{H/t}$
    (i.e. $H = 40$, $t = 2$, $2 * 2^{20} = 2^{21}$)

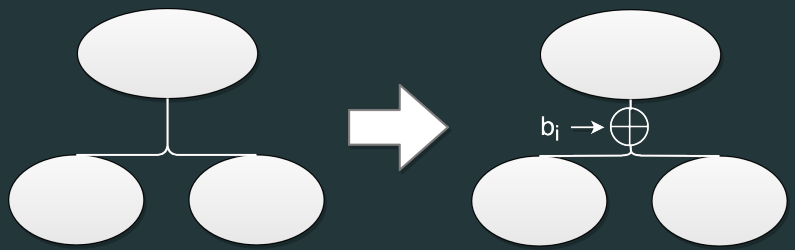


[a](BGD+06)
[b](BDH11)

Given security level b, tree height H and message length m

signature size	$\sigma_i = (i, \sigma_{OTS}, Y_i, (a_0,...,a_{H-1}))$

- using Winternitz[1] OTS $\rightarrow Y_i = f(\sigma_{OTS})$
- modifying tree construction[2] $\rightarrow$ allowing use of 2nd preimage resistant hash function



[1](Mer89)
[2](BDH11)

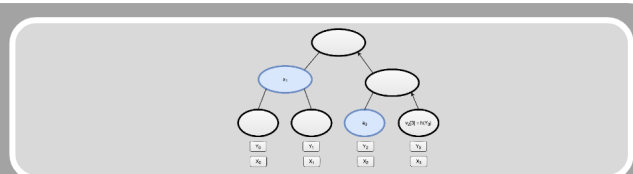
Given security level b, tree height H and message length m

- using seed-based secret key[3]: $2bm * 2^H \rightarrow b * 2^H$
- secret key size independent of message length

[3](BDH11)

Given security level b, tree height H and message length m

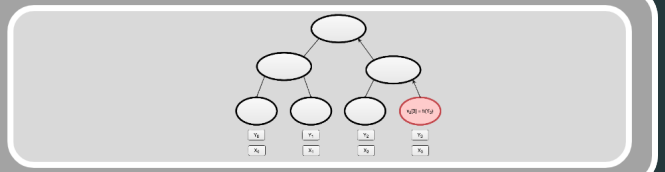
authentication path generation time & space



- MSS requires time and space of 2^H (naive)
- Treehash[4] algorithm requires only $b(H-1)$ space
- BDS[5] algorithm (time - memory trade off by parameter k):
  - time : $(H-k)/2$ (per signature)
  - memory: $(5,5H-5k-2^k)$

[4](BDS08)
[5](BDS08)

stateful

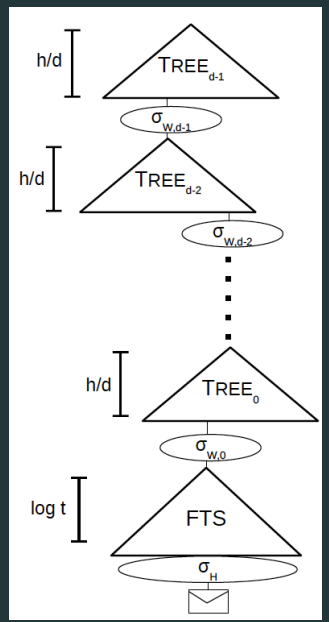


storing index $i \rightarrow$ problems:

- Load-balancing
- Multi-threading ...

Goldreich's[a] and SPHINCS[b] approach:

- use a huge/"hyper-tree"
- pick index i randomly
- messages signed with few-time signature scheme



[a] (Gol04)
[b] (BHH+15)

Bibliography

(BDS09) Johannes Buchmann, Erik Dahmen, Michael Szydlo. Introduction to post-quantum cryptography 2009.

(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.

Bibliography

2/2

(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.

(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.

9