QIC 891 Topics in Quantum Safe Cryptography

Module 1: *Post-Quantum Cryptography*

Summary of Post-quantum Signature Schemes

Lecturer: Fang Song *May 12, 2016*

Approach	**Instantiation**	**Remarks**
Without trapdoors		
Hash-based $\mathsf{OWF} \to \mathsf{OTS} \xrightarrow{*} \mathsf{Sign}$ *: Merkle tree [Mer90]	SHA family [BDH11] and many variants, stateless scheme [BHH+15]	Need: more quantum cryptanalysis considering internal design of SHA
"Homomorphic" hash $\mathsf{hash} \to \mathsf{ID} \xrightarrow{*} \mathsf{Sign}$ *: Fiat-Shamir	**Lattice**: safety check with aborting. SIS [Lyu08, KTX08], Ring-SIS [Lyu09], both [Lyu12, DDLL13] **Code**: [Ste96] **MQ**: N/A	[KTX08] inspired by [Ste96]. Adapt ideas from lattice ID to code-based? Quantum security unclear: quantum rewinding+FS in QRO
With trapdoors		
"Text-book" RSA $\sigma = f^{-1}(sk, m)$ e.g. $\sigma = m^d \pmod N$	**Lattice**: [GGH97], NTUSign [HPS01, HHGP+03] (broken [NR09, DN12]) **Code**: early proposals broken **MQ**: majority (many broken)	Bad idea, **avoid**!
Hash-&-Sign in RO (Full-domain hash) $\sigma = f^{-1}(sk, \mathcal{O}(m))$ $\mathcal{O}$: random-oracle	**Lattice**: [GPV08, MP12] **Code**: [CFS01]. Formal proof of CFS01 in [Dal07], but one of the assumptions was disproved in [FGUO+13].	adapt lattice ideas to code? Fix [CFS01] proof?
Direct constructions **without RO**	**Lattice**: [Boy10, CHKP12, DM14, AS15]	provably secure code & MQ-based unclear

References

[AS15] Jacob Alperin-Sheriff. Short signatures with short public keys from homomorphic trapdoor functions. In *Public-Key Cryptography–PKC 2015*, pages 236–255. Springer, 2015.

[BDH11] Johannes Buchmann, Erik Dahmen, and Andreas Hülsing. Xmss-a practical forward secure signature scheme based on minimal security assumptions. In *Post-Quantum Cryptography*, pages 117–129. Springer, 2011.

[BHH+15] Daniel J Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn. Sphincs: practical stateless hash-based signatures. In *Advances in Cryptology–EUROCRYPT 2015*, pages 368–397. Springer, 2015.

[Boy10] Xavier Boyen. Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more. In *Public Key Cryptography–PKC 2010*, pages 499–517. Springer, 2010.

[CFS01] Nicolas T Courtois, Matthieu Finiasz, and Nicolas Sendrier. How to achieve a McEliece-based digital signature scheme. In *Advances in Cryptology—ASIACRYPT 2001*, pages 157–174. Springer, 2001.

[CHKP12] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. *Journal of cryptology*, 25(4):601–639, 2012. Preliminary version in Eurocrypt 2010.

[Dal07] Léonard Dallot. Towards a concrete security proof of courtois, finiasz and sendrier signature scheme. In *Research in Cryptology*, pages 65–77. Springer, 2007.

[DDLL13] Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky. Lattice signatures and bimodal gaussians. In *Advances in Cryptology–CRYPTO 2013*, pages 40–56. Springer, 2013.

[DM14] Léo Ducas and Daniele Micciancio. Improved short lattice signatures in the standard model. In *Advances in Cryptology–CRYPTO 2014*, pages 335–352. Springer, 2014.

[DN12] Léo Ducas and Phong Q Nguyen. Learning a zonotope and more: Cryptanalysis of ntrusign countermeasures. In *Advances in Cryptology–ASIACRYPT 2012*, pages 433–450. Springer, 2012.

[FGUO+13] Jean-Charles Faugere, Valérie Gauthier-Umana, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. A distinguisher for high-rate McEliece cryptosystems. *Information Theory, IEEE Transactions on*, 59(10):6830–6844, 2013.

[GGH97] Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Public-key cryptosystems from lattice reduction problems. In *Advances in Cryptology—CRYPTO'97*, pages 112–131. Springer, 1997.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206. ACM, 2008.

[HHGP+03] Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H Silverman, and William Whyte. Ntrusign: Digital signatures using the ntru lattice. In *Topics in cryptology—CT-RSA 2003*, pages 122–140. Springer, 2003.

[HPS01] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. Nss: An ntru lattice-based signature scheme. In *Advances in Cryptology—Eurocrypt 2001*, pages 211–228. Springer, 2001.

[KTX08] Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa. Concurrently secure identification schemes based on the worst-case hardness of lattice problems. In *Advances in Cryptology-ASIACRYPT 2008*, pages 372–389. Springer, 2008.

[Lyu08] Vadim Lyubashevsky. Lattice-based identification schemes secure under active attacks. In *Public Key Cryptography–PKC 2008*, pages 162–179. Springer, 2008.

[Lyu09] Vadim Lyubashevsky. Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. In *Advances in Cryptology–ASIACRYPT 2009*, pages 598–616. Springer, 2009.

[Lyu12] Vadim Lyubashevsky. Lattice signatures without trapdoors. In *Advances in Cryptology–EUROCRYPT 2012*, pages 738–755. Springer, 2012.

[Mer90] Ralph C Merkle. A certified digital signature. In *Advances in Cryptology–CRYPTO 1989*, pages 218–238. Springer, 1990.

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Advances in Cryptology–EUROCRYPT 2012*, pages 700–718. Springer, 2012.

[NR09] Phong Q Nguyen and Oded Regev. Learning a parallelepiped: Cryptanalysis of ggh and ntru signatures. *Journal of Cryptology*, 22(2):139–160, 2009. Preliminary version in Eurocrypt 2006.

[Ste96] Jacques Stern. A new paradigm for public key identification. *Information Theory, IEEE Transactions on*, 42(6):1757–1768, 1996.