QIC 891 Topics in Quantum Safe Cryptography

Module 1: *Post-Quantum Cryptography*

Summary of Post-quantum Public-key Encryption Schemes

Lecturer: Fang Song *May 17, 2016*

Approach	**Security**	**Instantiation**		
		Lattice	**Code**	**MQ**
"Text-book" RSA. w. trapdoor functions	one-way?	• [GGH97] • NTRU [HPS98]?	McEliece [McE78], Niederreiter [Nie86]	[MI88, Pat96] ...
Constructions in random-oracle model (RO)				
[BR93] hybrid	IND-CPA in **RO**	applicable		
[BR93] with CCA Symmetric Enc	IND-CCA in **RO**	applicable		
OAEP [BR94]	≥ IND-CPA in **RO**	applicable? can we get IND-CCA?		
OAEP+ [Sho01]	IND-CCA in **RO**	applicable?		
Other transformations [Poi00, FO99, OP01]...	IND-CCA in **RO**	KEM [Pei14]	[KI01]	applicable?
Direct constructions in plain model				
Ex. leftover hash lemma [HILL99]	IND-CPA	[Reg09, GPV08] ...	[Ale03, NIKM08]	?
"lossy" trapdoor functions & correlated products	IND-CCA	[PW11, Pei09, MP12] ...	[DDMQN12]	?

References

[Ale03] Michael Alekhnovich. More on average case vs approximation complexity. In *Foundations of Computer Science, 2003. Proceedings. 44th Annual IEEE Symposium on*, pages 298–307. IEEE, 2003.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM conference on Computer and communications security*, pages 62–73. ACM, 1993.

[BR94] Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption. In *Advances in Cryptology—EUROCRYPT'94*, pages 92–111. Springer, 1994.

[DDMQN12] Nico Döttling, Rafael Dowsley, Jörn Müller-Quade, and Anderson CA Nascimento. A cca2 secure variant of the McEliece cryptosystem. *Information Theory, IEEE Transactions on*, 58(10):6672–6680, 2012. Preliminary version in CT-RSA 2009.

[FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Advances in Cryptology - CRYPTO '99*, pages 537–554, 1999. Full version in Journal of cryptology 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.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. Ntru: A ring-based public key cryptosystem. In *Algorithmic number theory*, pages 267–288. Springer, 1998.

[KI01] Kazukuni Kobara and Hideki Imai. Semantically secure McEliece public-key cryptosystems-conversions for mceliece pkc. In *Public Key Cryptography*, pages 19–35. Springer, 2001.

[McE78] RJ McEliece. A public-key cryptosystem based on algebraic coding theory. *The Deep Space Network Progress Report*, 42(44):114–116, 1978.

[MI88] Tsutomu Matsumoto and Hideki Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Advances in Cryptology—EUROCRYPT'88*, pages 419–453. Springer, 1988.

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

[Nie86] Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15:19–34, 1986. Problemy Upravlenija i Teorii Informacii 15, 159–166.

[NIKM08] Ryo Nojima, Hideki Imai, Kazukuni Kobara, and Kirill Morozov. Semantic security for the mceliece cryptosystem without random oracles. *Designs, Codes and Cryptography*, 49(1-3):289–305, 2008.

[OP01] Tatsuaki Okamoto and David Pointcheval. REACT: Rapid enhanced-security asymmetric cryptosystem transform. In *Topics in Cryptology—CT-RSA 2001*, pages 159–174. Springer, 2001.

[Pat96] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms. In *Advances in Cryptology—EUROCRYPT'96*, pages 33–48. Springer, 1996.

[Pei09] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 333–342. ACM, 2009.

[Pei14] Chris Peikert. Lattice cryptography for the internet. In *Post-Quantum Cryptography*, pages 197–219. Springer, 2014.

[Poi00] David Pointcheval. Chosen-ciphertext security for any one-way cryptosystem. In *Public Key Cryptography*, pages 129–146. Springer, 2000.

[PW11] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. *SIAM Journal on Computing*, 40(6):1803–1844, 2011. Preliminary version in STOC 2008.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):34, 2009.

[Sho01] Victor Shoup. Oaep reconsidered. In *Advances in Cryptology—CRYPTO 2001*, pages 239–259. Springer, 2001.