Long-term Security Through Quantum Cryptography

Related Literature

Dominique Unruh

February 27–March 4, 2011

In the following, I give a list of references related to my lecture at the 16th Estonian Winter School in Computer Science in Palmse. These references consist partly of historical papers and partly of papers covering the state of the art. This list is by no means intended to be complete.

- **Quantum computing & quantum information.** A good introduction into the topic (and the basis for further reading) is [NC00].
- **Quantum key distribution (QKD).** The idea of using quantum mechanical effects for cryptography first appeared in [Wie83]. The idea of QKD was made explicit and popularized by [BB84]. However, the first security proofs for QKD protocols were only given in [LC99, SP00]. More modern approaches for proving the security of QKD can be found in [Ren05], and, perhaps more accessible, [BF10].
- **Oblivious transfer (OT).** OT was first recognized to be complete for multi-party computation (MPC) in [Kil88]. Universally composable constructions for MPC from OT where given by [IPS08]. How to construct OT from commitments in a quantum setting was first suggested by [CK88], the idea was extended by [BBCS91]. The first proof of security for this construction was given in [Yao95], however, that proof is incomplete. A full proof was given by [DFL+09]; see also [BF10]. In a universally composable setting, the security of this construction was shown in [Unr10]. In [May97], it was shown that it is impossible to construct a commitment without using additional assumptions, even in the quantum setting.
- **Bounded quantum storage (BQS).** Commitment and OT protocols in the BQS model were first presented by [DFSS05]. Compositionality issues in this model were discovered in [DM04]. Solutions for sequential composition are given in [WW08, FS09]. Universal composition is treated in [Unr11]; they show the possibility of arbitrary MPC in the BQS model. Bounded storage in the classical case was studied in [CM97, CCM02].
- **Long-term security.** (Also known as everlasting security.) Statistically hiding commitments and zero-knowledge arguments were constructed by [NOVY98]; these can be seen as long-term secure commitments and zero-knowledge arguments. The problem of composition of long-term secure protocols was treated in [MQU10]. To the best of my knowledge, no treatment of long-term secure MPC in the quantum setting exists so far (except for the BQS model, of course).

References

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 1984*, pages 175–179. IEEE Computer Society, 1984.

[BBCS91] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska. Practical quantum oblivious transfer. In *Crypto '91*, volume 576 of *LNCS*, pages 351–366. Springer, 1991.

[BF10] Niek J. Bouman and Serge Fehr. Sampling in a quantum population, and applications. In Tal Rabin, editor, *Advances in Cryptology - CRYPTO 2010*, volume 6223 of *LNCS*, pages 724–741. Springer, 2010. Full version at arXiv:0907.4246v3 [quant-ph].

[CCM02] Christian Cachin, Claude Crépeau, and Julien Marcil. Oblivious transfer with a memory-bounded receiver. In *34th Annual ACM Symposium on Theory of Computing, Proceedings of STOC 2002*, pages 493–502. ACM Press, 2002.

[CK88] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *FOCS 1988*, pages 42–52. IEEE, 1988.

[CM97] Christian Cachin and Ueli Maurer. Unconditional security against memory-bounded adversaries. In Burton S. Kaliski Jr., editor, *Advances in Cryptology, Proceedings of CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 292–306. Springer-Verlag, 1997.

[DFL+09] Ivan Damgård, Serge Fehr, Carolin Lunemann, Louis Salvail, and Christian Schaffner. Improving the security of quantum protocols. In *Crypto 2009*, volume 5677 of *LNCS*, pages 408–427. Springer, 2009. Full version is arXiv:0902.3918v3 [quant-ph].

[DFSS05] Ivan Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded quantum-storage model. In *FOCS 2005*, pages 449–458, 2005. Full version is arXiv:quant-ph/0508222v2.

[DM04] Stefan Dziembowski and Ueli Maurer. On generating the initial key in the bounded-storage model. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology, Proceedings of EUROCRYPT '04*, volume 3027 of *Lecture Notes in Computer Science*, pages 126–137. Springer-Verlag, 2004. Online available at `ftp://ftp.inf.ethz.ch/pub/crypto/publications/DziMau04b.pdf`.

[FS09] Serge Fehr and Christian Schaffner. Composing quantum protocols in a classical environment. In *TCC 2009*, volume 5444 of *LNCS*, pages 350–367. Springer, 2009.

[IPS08] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer – efficiently. In *Crypto '08*, volume 5157 of *LNCS*, pages 572–591, 2008.

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In *Twentieth Annual ACM Symposium on Theory of Computing, Proceedings of STOC 1988*, pages 20–31. ACM Press, 1988. Online available at `http://external.nj.nec.com/homepages/joe/collected-papers/Kil88b.ps`.

[LC99] H. K. Lo and H. F. Chau. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science*, 283(5410):2050, 1999. Online available at `http://arxiv.org/abs/quant-ph/9803006`.

[May97] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, 1997. Preprint at arXiv:quant-ph/9605044v2.

[MQU10] Jörn Müller-Quade and Dominique Unruh. Long-term security and universal composability. *Journal of Cryptology*, 23(4):594–671, 2010. Preprint on IACR ePrint 2006/422.

[NC00] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[NOVY98] Moni Naor, Rafail Ostrovsky, Ramarathnam Venkatesan, and Moti Yung. Perfect zero-knowledge arguments for NP using any one-way permutation. *Journal of Cryptology*, 11(2):87–108, March 1998.

[Ren05] Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich, September 2005. Available at `http://arxiv.org/abs/quant-ph/0512258v2`.

[SP00] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85(2):441–444, Jul 2000.

[Unr10] Dominique Unruh. Universally composable quantum multi-party computation. In *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 486–505. Springer, May 2010. Preprint on arXiv:0910.2912 [quant-ph].

[Unr11] Dominique Unruh. Concurrent composition in the bounded quantum storage model, May 2011. To appear, preprint on IACR ePrint 2010/229.

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. Manuscript written ca. 1970.

[WW08] Stephanie Wehner and Jörg Wullschleger. Composable security in the bounded-quantum-storage model. In *ICALP 2008, track C*, Lecture Notes in Computer Science, pages 604–615. Springer, 2008. Full version available at `http://arxiv.org/abs/0709.0492v1`.

[Yao95] Andrew Chi-Chih Yao. Security of quantum protocols against coherent measurements. In *Twenty-Seventh Annual ACM Symposium on Theory of Computing, Proceedings of STOC 1995*, pages 67–75. ACM Press, 1995.