Quantum Key Distribution in the Classical Authenticated Key Exchange Framework
(extended abstract)

Michele Mosca[1,2], Douglas Stebila[3], and Berkant Ustaoglu[4]

[1] Institute for Quantum Computing and Dept. of Combinatorics & Optimization
University of Waterloo, Waterloo, Ontario, Canada
[2] Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada
mmosca@uwaterloo.ca
[3] Information Security Institute, Queensland University of Technology, Brisbane, Queensland, Australia
stebila@qut.edu.au
[4] Department of Mathematics, Izmir Institute of Technology, Urla, Izmir, Turkey
bustaoglu@uwaterloo.ca

May 21, 2012

Quantum key distribution (QKD) promises new security properties compared to cryptography based on computational assumptions: QKD can provide for two parties to establish a secure key using an untrusted quantum channel and a public, authenticated classical channel, and this key is secure against any adversary who is limited solely by the laws of quantum mechanics. While some classical[1] cryptographic tasks can be achieved with information-theoretic security against unbounded adversaries, key establishment over a public authenticated channel is not one of them. Moreover, the practicality of such information-theoretically secure schemes is often limited, and as a result most classical cryptographic schemes rely for their security on various computational assumptions, the most widely used of which — factoring, discrete logarithms — could be efficiently solved by a large-scale quantum computer. As a result, QKD could be an important primitive for cryptography secure against any advances in computing technology, provided quantum mechanics remains an accurate description of the laws of nature.

Authenticated key establishment (AKE) is the cryptographic task which QKD achieves. The classical cryptographic literature has extensively studied AKE since the founding of public key cryptography in 1976. After a period of ad hoc security analysis of key establishment protocols based on resistance to various individual attacks, protocols are now generally analyzed within the context of a security model, which aims to capture a wide variety of security properties in the context of an attacker who can control all communication, as well as possibly compromise participants; proofs typically consist of probabilistic reductions to computationally hard problems. One seminal model for security of AKE protocols was proposed by Bellare and Rogaway [2]. The BR model led to the CK01 model by Canetti and Krawczyk [9], upon which was based the eCK model [17]. An alternative approach to this family of security models is given by Canetti's *universal composability framework* [8]. One of the general observations of this line of work has been that calculating a secret key is relatively easy, but properly modelling authentication — ensuring that the key is shared with precisely the intended party and no other — requires greater care.

There are many types of QKD protocols, but for our purposes we will divide them into 3 classes: prepare-send-measure protocols, measure-only protocols, and prepare-send-only protocols. The first QKD

[1] We use the adjective "classical" to mean "non-quantum", so "classical cryptography" means "non-quantum cryptography", not "historical cryptography".

protocol, now called BB84, was proposed by Bennett and Brassard [4]; it is an example of a prepare-send-measure protocol in which Alice randomly prepares one of several quantum states, sends it to Bob, and Bob randomly measures in one of several settings. Ekert [12] proposed an entanglement-based protocol, which is an example of a measure-only protocol: Alice and Bob only randomly measure in one of several settings; the state itself can be prepared by Eve entirely untrusted. Biham et al. [6] proposed a prepare-send-only protocol, in which Alice and Bob each randomly prepare one of several quantum states and send them to Eve, who measures and sends back a classical result. Different versions can be appealing due to ease of implementation, resistance to side-channel attacks on preparing or measuring, or device independence.

Research arguing for the security of QKD has largely proceeded independent of the aforementioned classical AKE security models. Various proofs of QKD have been given in a stand-alone 2-party setting; some of the most important ones include [20, 19, 5, 24, 15, 14, 23], but many others exist for different variants of QKD; some work on QKD has been done in the universal composability framework [3]. These proofs typically proceed under the assumption that classical communication happens over on authentic public channel; details on authenticating the classical communication are typically left out of the analysis. It is widely recognized that the authentication can be secure against an unbounded adversary if all classical communication is protected by information-theoretically secure message authentication codes, such as the Wegman-Carter 2-universal hash function [10, 27]. Alternatively, it is generally considered folklore [22, 1, 25, 16] that if QKD was performed using a computationally secure authentication scheme (such as public key digital signatures), then messages encrypted under the keys output by QKD would be secure provided that the adversary could not break the authentication scheme *before or during* the QKD protocol.

Contributions. Our goal is to describe the security of quantum key distribution in a security model similar to existing classical authenticated key exchange protocols and compare the relative security properties of various QKD and classical AKE protocols. Our model is explicitly a multi-party model, includes authentication, and allows for either computationally secure or information theoretically secure authentication. We aim to capture two properties: (1) QKD is *immediately secure* against an active adversary who is restricted such that he is unable to break the authentication scheme, and (2) QKD is *long-term secure*, meaning that, if it is secure against an active adversary who is restricted during the run of the protocol to be unable to break the authentication scheme, then it remains secure even when the (classical and quantum) data obtained by the active bounded adversary are subsequently given to an unbounded quantum adversary.

Security model for classical-quantum AKE protocols. In particular, we first introduce a multi-party model for analyzing the security of QKD protocols. In our model, which adopts the formalism of Goldberg et al.'s framework for authenticated key exchange [13], parties consist of a pair of classical and quantum Turing machines, each of which is capable of sending and receiving messages. The adversary controls all communications between parties, but is restricted in its ability to affect communication between a single party's classical and quantum devices. The adversary also has the ability to compromise various values used by parties during or after the run of the protocol. As is typical, the adversary's goal is to distinguish the session key of a completed session from a random string of the same length.

Having defined the adversarial model, we then introduce our two security definitions, *immediate security* against an active, potentially bounded adversary, and *long-term security*, meaning security against an adversary who during the run of the protocol is potentially bounded, but after the protocol completes is unbounded (except by the laws of quantum mechanics). Our model is generic enough to allow the bound on the adversary to be computational — assuming that a particular computational problem is hard — or run-time or memory-bounded [7]. We adapt the long-term security notion of Müller-Quade and Unruh [21] from the classical universal composability framework to our classical-quantum model.

Security of BB84. We then proceed to show that the BB84 protocol, when used with a computationally secure classical authentication scheme such as a digital signature, is secure in this model. For the quantum aspects of the proof, we rely on existing proof techniques, but when combined the signature scheme in our model, this work provides a proof of the folklore theorem that QKD, when used with computationally secure authentication in a multi-party setting, is information theoretically secure, provided the adversary

did not break the authentication during the run of the protocol. Note, importantly, that this is the first proof of QKD in a multi-party setting; while our QKD protocol is still a 2-party protocol, it operates in an environment where many parties may be interacting simultaneously, whereas previous proofs of security of QKD — including the universal composability proof of Ben-Or et al. [3] — deal with only 2 honest parties (plus the adversary).

Comparison of quantum and classical AKE protocols. Finally, we use our generic security model to compare the security properties of classical key exchange protocols and examples from each of the three classes of QKD protocols (prepare-send-measure, measure-only, prepare-send-only). This comparison is facilitated by our phrasing of QKD in a security model more closely related to traditional AKE security models, which we can then use to compare the relative powers afforded to the adversary under those models. In particular, our model allows us to compare how different protocols react when the randomness used in the protocol is revealed — or if it is later discovered that bad randomness was used. For example, some classical AKE protocols such as UP [26] are secure even if the randomness used for either a party's long-term secret key or ephemeral secret key is revealed *before* the run of the protocol, but the same is not true for the randomness used to pick basis choices in BB84. And the EPR protocol of Ekert is secure even if all of the randomness used by the parties is leaked after the protocol completes, unlike BB84 where data bit choices must remain secret.

Protocol	Signed Diffie–Hellman [9]	UP [26]	BB84 [4]	EPR [12]	BHM96 [6, 15]
Protocol type	classical	classical	quantum prepare-send-measure	quantum measure-only	quantum prepare-send-only
Security model in which can be proven secure	CK01 [9], this paper	eCK [17], this paper	this paper	this paper	this paper
Randomness revealable **before** protocol run?	× static key × ephemeral key	at most 1 of static key, ephemeral key	× static key × basic choice × data bits × info. recon. × priv. amp.	× static key × basis choice × info. recon. × priv. amp.	× static key × basis choice × data bits × info. recon. × priv. amp.
Randomness revealable **after** protocol run?	✓ static key × ephemeral key	at most 1 of static key, ephemeral key	✓ static key ✓ basis choice × data bits ✓ info. recon. ✓ priv. amp.	✓ static key ✓ basis choice ✓ info. recon. ✓ priv. amp.	✓ static key ✓ basis choice × data bits ✓ info. recon. ✓ priv. amp.
Short-term security	computational assumption	computational assumption	computational or information-theoretic	computational or information-theoretic	computational or information-theoretic
Long-term security	×	×	assuming short-term-secure authentication	assuming short-term-secure authentication	assuming short-term-secure authentication

Discussion. The ability to compare various classical and quantum protocols in our model has allowed us to identify an important distinction between existing classical key establishment and quantum key distribution protocols. At a high level, classical protocols can provide more assurances against online adversaries who can leak or infiltrate in certain ways, but in the long run may be insecure against potential future advances. Current quantum protocols provide assurances against somewhat weaker online adversaries but retain secrecy indefinitely, even against future advances in computing technology.

Since in our model the relative strength of a fresh session is specified by the conditions given in the output of the protocol, an interesting open problem would be to use our model develop a quantum key distribution protocol which does retain its security attributes in the short- and long-terms even if some random values were known before the run of the protocol.

Acknowledgements The authors gratefully acknowledge helpful discussions with Norbert Lütkenhaus, Alfred Menezes, and Kenny Paterson. MM is supported by NSERC (Discovery, SPG FREQUENCY, CREATE), QuantumWorks, MITACS, CIFAR, ORF. IQC and Perimeter Institute are supported in part by the Government of Canada and the Province of Ontario.

References

[1] R. Alléaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, A. Leverrier, N. Lütkenhaus, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger. SECOQC white paper on quantum key distribution and cryptography, January 2007. `http://www.arxiv.org/abs/quant-ph/0701168`.

[2] M. Bellare and P. Rogaway. Entity authentication and key distribution. In D. R. Stinson, editor, *Advances in Cryptology – Proc. CRYPTO '93*, volume 773 of *LNCS*, pages 232–249. Springer, 1993. Full version available at `http://www-cse.ucsd.edu/~mihir/papers/key-distribution.html`.

[3] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In J. Kilian, editor, *Theory of Cryptography Conference (TCC) 2005*, volume 3378 of *LNCS*, pages 386–406. Springer, 2005.

[4] C. H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing. In *Proc. IEEE International Conf. on Computers, Systems and Signal Processing*, pages 175–179. IEEE, December 1984.

[5] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury. A proof of the security of quantum key distribution (extended abstract). In *Proc. 32nd Annual ACM Symposium on the Theory of Computing (STOC)*, pages 715–724. ACM Press, 2000.

[6] E. Biham, B. Huttner, and T. Mor. Quantum cryptographic network based on quantum memories. *Physical Review A*, 54(4):2651–2658, 1996.

[7] C. Cachin and U. Maurer. Unconditional security against memory-bounded adversaries. In B. S. Kaliski Jr., editor, *Advances in Cryptology – Proc. CRYPTO '97*, volume 1297 of *LNCS*, pages 292–306. Springer, 1997.

[8] R. Canetti. Universally composable security: a new paradigm for cryptographic protocols (extended abstract). In *Proc. 42nd Annual IEEE Symposium on Foundations of Computer Science (FOCS) 2001*, pages 136–145. IEEE Press, 2001.

[9] R. Canetti and H. Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In B. Pfitzmann, editor, *Advances in Cryptology – Proc. EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 453–474. Springer, 2001. Full version available at `http://eprint.iacr.org/2001/040`.

[10] J. L. Carter and M. N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979.

[11] C. Cremers. Examining indistinguishability-based security models for key exchange protocols: the case of CK, CK-HMQV, and eCK. In *Proc. 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS) 2011*, pages 80–91. ACM, 2011.

[12] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, August 1991.

[13] I. Goldberg, D. Stebila, and B. Ustaoglu. Anonymity and one-way authentication in key exchange protocols. *Designs, Codes and Cryptography*, 2012. Online first; print version to appear.

[14] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quantum Information and Computation*, 4(5):325–360, September 2004.

[15] H. Inamori. Security of practical time-reversed EPR quantum key distribution. *Algorithmica*, 34(4):340–365, 2002.

[16] L. M. Ioannou and M. Mosca. A new spin on quantum cryptography: Avoiding trapdoors and embracing public keys. In B.-Y. Yang, editor, *Proc. 4th International Workshop on Post-Quantum Cryptography (PQCrypto) 2011*, volume 7071 of *LNCS*, pages 255–274. Springer, 2011.

[17] B. LaMacchia, K. Lauter, and A. Mityagin. Stronger security of authenticated key exchange. In W. Susilo, J. K. Liu, and Y. Mu, editors, *First International Conference on Provable Security (ProvSec) 2007*, volume 4784 of *LNCS*, pages 1–16. Springer, 2007.

[18] L. Law, A. Menezes, M. Qu, J. Solinas, and S. A. Vanstone. An efficient protocol for authenticated key agreement. *Designs, Codes and Cryptography*, 28(2):119–134, 2003.

[19] H.-K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056, 1999.

[20] D. Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In N. Koblitz, editor, *Advances in Cryptology – Proc. CRYPTO '96*, volume 1109 of *LNCS*, pages 343–357. Springer, 1996.

[21] J. Müller-Quade and D. Unruh. Long-term security and universal composability. *Journal of Cryptology*, 23(4):594–671, 2010.

[22] K. G. Paterson, F. Piper, and R. Schack. Quantum cryptography: A practical information security perspective. In M. Zukowski, S. Kilin, and J. Kowalik, editors, *Proc. NATO Advanced Research Workshop on Quantum Communication and Security*, volume 11 of *NATO Science for Peace and Security Series, Sub-Series D: Information and Communication Security*. IOS Press, 2007. See also `http://arxiv.org/abs/quant-ph/0406147`.

[23] R. Renner. *Security of Quantum Key Distribution*. PhD thesis, Swiss Federal Institute of Technology Zürich, 2005.

[24] P. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441–444, 2000.

[25] D. Stebila, M. Mosca, and N. Lütkenhaus. The case for quantum key distribution. In A. Sergienki, S. Pascazio, and P. Villoresi, editors, *Quantum Communication and Quantum Networking: First International Conference, QuantumComm 2009*, volume 36 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 283–296. Springer, 2010.

[26] B. Ustaoğlu. Comparing sessionstatereveal and ephemeralkeyreveal for diffie-hellman protocols. In J. Pieprzyk and F. Zhang, editors, *Provable Security: Third International Conference, ProvSec 2009*, volume 5848 of *LNCS*, pages 183–197. Springer, 2009.

[27] M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, 1981.