Cryptography in a Quantum World

Claude Crépeau[1] *

[1] *Cryptography and Quantum Information Laboratory, School of Computer Science, McGill University, 3480 rue University, McConnell Engineering Building, Montréal (Québec), Canada H3A 2A7.*

Abstract. This work surveys the recent results in the theory of cryptography in a quantum computing model. Under the assumption that a quantum computer is built, we consider such notions as encryption and authentication of quantum data, and compare them with their classical counterparts. Many surprizes are unraveled. Once again, these results show how strikingly similar but different the two worlds are.

Keywords: Cryptography, Encryption, Authentication, Quantum Computer, Quantum Cryptography

1 Quantum Cryptography

Quantum Cryptography was born in the early seventies when Stephen Wiesner wrote "Conjugate Coding", which unfortunately took more than ten years to appear in print. In the mean time, Charles H. Bennett (who knew of Wiesner's idea) and Gilles Brassard picked up the subject and brought it to fruition in a series of papers that culminated with the demonstration of an experimental prototype that established the technological feasibility of the concept [3]. Quantum Key Distribution systems take advantage of Heisenberg's uncertainty principle, according to which measuring a quantum system in general disturbs it and yields incomplete information about its state before the measurement. Eavesdropping on a quantum communication channel therefore causes an unavoidable disturbance, alerting the legitimate users. This yields a cryptographic system for the distribution of a secret random cryptographic key between two parties initially sharing no secret information that is secure against an eavesdropper having at her disposal unlimited computing power. Once this secret key is established, it can be used together with classical cryptographic techniques such as the one-time-pad to allow the parties to communicate meaningful information in absolute secrecy, or in an authentic fashion with the smallest possible impersonation probability.

A similar approach was investigated in [5] and [7] in order to allow Alice and Bob to exchange high quality pairs of maximally entangled particles, even in the presence of an arbitrary powerful eavesdropper. These pairs of maximally entangled particles can later be considered as the quantum equivalent of classical secret bits: by the fact that the particles are maximally entangled, they cannot be entangled with anything else in the universe and thus are *secret*. Quantum analogs to encryption and authentication may then be considered.

*email address: crepeau@cs.mcgill.ca

2 Cryptography of quantum information

A very different component of quantum cryptography is the *cryptography of quantum information* where cryptographic tools are developed for information imbedded in quantum systems. A first example is known as *one-time-quantum-pad* where sender Alice and receiver Bob a priori share a pair of maximally entangled particles and use them to teleport [4] an arbitrary qubit from Alice to Bob. The only public transmission of this scheme is a pair of classical bits from sender to receiver, allowing him to reconstruct the original state she wanted to transfer him. A second example is the *Quantum Vernam Cipher* [1] where a classical key of four possible values is used by Alice who applies one of four Pauli operators (including identity) to an arbitrary system of a single qubit that may then be transmitted to Bob. Bob decrypts the state by applying the inverse unitary operator. The quantum description of the state transmitted is the same regardless of the original state to be transferred as long as the key is uniformly distributed and secret to an eavesdropper.

It was shown in [1] that the above scheme is more or less optimal in the sense that two classical bits are necessary and sufficient to encrypt a general qubit. However, it was also demonstrated in [6] that unless the messages sent from Alice to Bob are *entangled* with Eve, on average, slightly more than one bit is enough to encrypt a qubit. The only extra weakening necessary for this result is that the fidelity of the decrypted state is not exactly one, but exponentially close to one.

Quantum error-correcting codes have lead to the notion of *Quantum Message Authentication* [2] that allows Alice to send Bob a message in such a way that any tampering of the transmitted message will either result in detection of the tampering or actual correction of the tampering back to the original message. Again, two models may be considered, one where Alice and Bob share a pair of maximally entangled particles, and one where they share only secret bits. Surprisingly, quantum authentication *requires* quantum encryption, whereas classically these two tasks are orthogonal to each other.

References

[1] Ambainis , A., Mosca, M., Tapp, A., and de Wolf, R., "Private quantum channels", *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, pp. 547 – 553, IEEE Computer Society Press, 2000.

[2] Barnum, H., Crépeau, C., Gottesman, D., Tapp, A. and Smith, A., "Authentication of quantum messages". *Proceedings of the 43rd Annual Symposium on Foundations of Computer Science*, pp. 449 – 458, 2002. Complete version: quant-ph/0205128.

[3] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. and Smolin, J., "Experimental quantum cryptography", Journal of Cryptology, vol. 5, no. 1, pp. 3 – 28, 1992.

[4] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., and Wootters, W., "Teleporting an unknown quantum state via dual classical and EPR channels", *Phys. Rev. Lett.*, pp. 1895 – 1899, 1993.

[5] Ekert, A. K., "Quantum cryptography based on Bell's theorem", Physical Review Letters, vol. 67, no. 6, pp. 661 – 663, 1991.

[6] Hayden, P., Leung, D., Shor, P. W., and Winter, A., "Randomizing quantum states: Constructions and applications". quant-ph/0307104, 2003.

[7] Lo, H.-K. and Chau, H. F., "Unconditional Security Of Quantum Key Distribution Over Arbitrarily Long Distances", *Science*, vol. 283, pp. 2050 – 2056, 1999.