Quantum Cryptography

Gilles Brassard * and Claude Crépeau †

1 Quantum Cryptography [A]

Quantum Cryptography was born in the early seventies when Stephen Wiesner wrote "Conjugate Coding", which unfortunately took more than ten years to see the light of print [50]. 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 [5]. Quantum cryptographic systems take advantage of Heisenberg's uncertainty relations, 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 key between two parties initially sharing no secret information (however they must be able to authenticate messages) 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 Vernam cipher (one-time pad) to allow the parties to communicate meaningful information in absolute secrecy.

Quantum cryptography is best known for key distribution [7]. A short summary of this so-called *BB84 protocol* is provided in Section 1.2. A remarkable surge of interest in the international scientific and industrial community has propelled quantum cryptography into mainstream computer science and physics. Furthermore, quantum cryptography is becoming increasingly practical at a fast pace. The first quantum key distribution prototype, built in 1989, worked over a distance of 32 centimetres [5], [11]. Since then, many additional experimental demonstrations have been set up, covering distances of tens of kilometres. Consult [46] or [42] for popular accounts of the state of the art in experimental quantum cryptography.

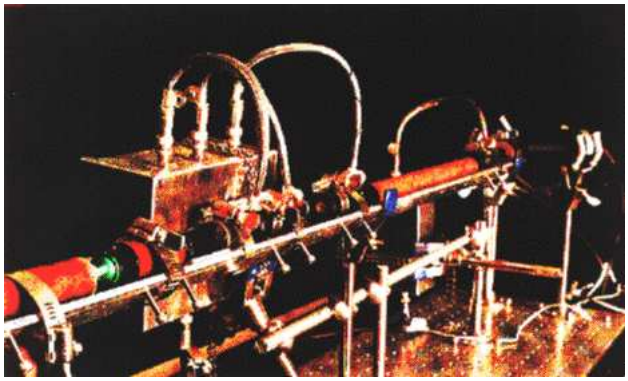

Figure 1: First experiment (IBM Yorktown Heights)

1.1 The various uses of quantum physics for cryptography

In addition to key distribution, quantum techniques may also assist in the achievement of subtler cryptographic goals, important in the post-cold war world, such as protecting private information while it is being used to reach public decisions. Such techniques, pioneered by Claude Crépeau [10], [15], allow two people to compute an agreed-upon function $f(x, y)$ on private inputs x and y when one person knows x, the other knows y, and neither is willing to disclose anything about his private input to the other, except for what follows logically from one's private input and the function's output. The classic example of such discreet decision making is the "dating problem", in which two people seek a way of making a date if and only if each likes the other, without disclosing any further information. For example, if Alice likes Bob but Bob doesn't like Alice, the date should be called off without Bob finding out that Alice likes him. On the other hand, it is logically unavoidable for Alice to learn that Bob doesn't like her, because if he did the date would be on.

Indeed, two applications of quantum physics to cryptography were discovered well before quantum key distribution: quantum bank notes that are impossible to counterfeit and quantum multiplexing that allows one party to send two messages to another party in a way that the re-

* Département IRO, Université de Montréal, Montréal (QC), Canada H3C 3J7. e-mail: brassard@iro.umontreal.ca.

† School of Computer Science, McGill University, Montréal (QC), Canada H3A 2A7. e-mail: crepeau@cs.mcgill.ca.

ceiver can obtain either message at his choice, but reading one destroys the other irreversibly [50]. (The notion of multiplexing was reinvented ten years later by Michael Rabin in the context of classical cryptography under the name of oblivious transfer [43], [28].) Unfortunately, even its author, Stephen Wiesner, knew from the start that the quantum multiplexing protocol could be defeated with arbitrary measurements performed by the receiver of the strings. Thus, a more elaborate quantum oblivious transfer protocol was designed subsequently [10] under the assumption of the existence of a bit commitment scheme [19], a result unlikely to be possible classically as argued by Russel Impagliazzo and Steven Rudich [34]. Another quantum cryptographic task that has been studied extensively is indeed bit commitment [15]. Unfortunately it turned out that early claims of security of certain quantum protocols for this task were after all insecure as showed by Dominic Mayers [39] and independently by Hoi-Kwong Lo and Hoi Fung Chau [37]. This no-go theorem was later extended to *any* Quantum Bit Commitment scheme consistent with quantum physics [40], [38].

On a closely related topic, various Quantum Coin Tossing protocols have been also introduced [7] as well as a lower bound of $1/\sqrt{2}$ on the bias of such a protocol in a very general quantum mechanical framework [1].

1.2 Quantum Key Distribution

The purpose of quantum key distribution is to enable two honest parties, Alice and Bob, to agree on a random cryptographic key in a situation where eavesdropping is possible. By transmitting one of four possible non-orthogonal quantum states, Alice may send to Bob a random bit-stream that she knows exactly and of which Bob will randomly select a constant fraction. These four possible states may be the 0°, 45°, 90° and 135° polarizations of a photon. According to quantum mechanics, orthogonally polarized photons ($(0^\circ,90^\circ)$ or $(45^\circ,135^\circ)$) are perfectly distinguishable whereas non-orthogonal photons ($(0^\circ,45^\circ)$, $(45^\circ,90^\circ)$, etc.) are not. When Alice sends Bob a random state from these four, he may choose to measure whether it is $(0^\circ,90^\circ)$ or $(45^\circ,135^\circ)$. If he makes the correct measurement then he detects perfectly the original state. If he makes the wrong measurement then he detects a random state among the two he was trying to distinguish. When Alice later tells him which was the correct measurement, he keeps the correctly measured states and discards the others. Thus, in a perfect world, Bob would receive 50% of Alice's photons in their exact original state and discard the other 50% of the photons. If we assign binary value 0 to 0° and 45° and value 1 to 90° and 135°, then their agreed bit-stream is obtained by the correctly measured 50% of the photons.

However, the world is not perfect. Therefore, a fraction of the correctly measured photons will be detected incorrectly. Also, if an eavesdropper (Eve) tries to measure Alice's photons before they reach Bob, errors will be induced by the fact that she is measuring information about the photons' polarizations. Moreover, these two situations are indistinguishable from each other: natural noise or induced noise look the same. (Indeed, part of the "natural" noise is produced by "nature" eavesdropping on Alice and Bob!) The beauty of quantum cryptography is that an estimate on the noise level leads to an estimate of the information obtained by Eve. Consequently, a three-phase classical protocol allows Alice and Bob to extract an agreed upon, smaller secret cryptographic key from their noisy, partly eavesdropped bit-stream. These three phases are called "error estimation", "information reconciliation" and "privacy amplification".

1.2.1 Error estimation

Error estimation is performed by having one of Alice or Bob pick at random a certain number t of bits previously transmitted according to the correct measurement and announce them to the other party. The latter compares these bits with his/her own copy and announces the number of errors e. For large enough samples, the ration e/t should be a reasonable estimate of the fraction of errors left in the undisclosed bits.

1.2.2 Information reconciliation

Although interactive error correction such as [16] was first encouraged in [5], Claude Crépeau pointed out that traditional error-correcting codes may be used here as well [10]. In both cases, this process will disclose some extra information about the remaining (corrected) bits to any potential eavesdropper. This extra information must be taken into account in the last privacy amplification phase.

1.2.3 Privacy amplification

Assume an eavesdropper is left with only ℓ bits of Rényi (collision) entropy about the bit-stream W of size n resulting from the information reconciliation phase. If Alice and Bob can estimate ℓ from error estimation and error correction, they may produce a new smaller bit-stream K of size nearly ℓ from W. Let H be a uniformly selected hash function from a Strongly Universal Set [49] mapping n bits to $\ell - s$ bits. Then we obtain a tight bound on the uncertainty $\mathbf{H}(H(W) \mid H, E) \leq 2^{-s}$ where

E is the eavesdropping information (including error correction). This means that if one of Alice or Bob picks a random hash function h and announces it publicly to the other, they are able to use it to replace their longer string W by $K = h(W)$ that is almost perfectly secret to the eavesdropper [9] with nearly probability one.

1.2.4 Eavesdropping

The key distribution protocol described above has been proven secure regardless of the eavesdropper's strategy and computing power. The first proof of this theorem is due to Mayers [41]. However, the very technical nature of that proof encouraged many alternate proofs to be developed such as those of Biham, Boyer, Boykin, Mor and Roychowdhury [14], Shor-Preskill [45], Gottesman and Lo [31], etc. A more powerful security proof in the universal composability framework was recently demonstrated by Ben-Or, M. Horodecki, Leung, Mayers, and Oppenheim [13].

1.3 Alternative quantum key distribution protocols and Implementations

The original quantum key distribution protocol uses four different polarization states of single photons as carrier of quantum information [7], but other approaches have been put forward. Early variations were to use only two non-orthogonal states rather than four [4], and to use phase modulation rather than polarization [26], [48]. A more fundamental variation, due to Artur Ekert [25], was to make use of Einstein-Podolsky-Rosen entangled pairs [24], which allows the key to remain protected by quantum mechanics even in storage, rather than merely in transit. More interestingly, Ekert's scheme can benefit from powerful quantum techniques that were discovered only years later, such as entanglement distillation [12], [23]. Prototypes of entanglement-based quantum cryptography, working over kilometres of fibre, came soon after the theoretical invention [26] as well as much more recently [27].

The past decade has seen an explosion in experimental demonstrations of quantum cryptography, with distances ever increasing, sometimes at the expense of giving up the Holy Grail of unconditional security. We can mention only a few examples here. A plug-and-play device built in Switzerland was tested successfully using 67 kilometres of optical fibre laid out between Geneva and Lausanne [47]. More recent experiments achieve even further distances such as 150 kilometres of optical fibre [35]. The notion of *quantum repeaters* has been discussed in order to achieve even greater distances [18]. Free-space prototypes have shown the possibility of line-of-sight quantum cryptography over distances of tens of kilometres [33], [36], making it legitimate to dream of a quantum-cryptographic satellite-based global network [44]. A thorough survey of quantum cryptography, with an emphasis on technological issues, can be found in [29]. A living roadmap of the work ahead can be obtained at [6].

Finally, we point out that quantum key distribution is now available as a commercial product. Information about quantum-cryptographic products can be found at the Web sites of the Swiss company *id Quantique* (`www.idquantique.com`) and the American corporation *MagiQ Technologies* (`magiqtech.com`).

1.4 Cryptography on quantum data

The last component of quantum cryptography is the *cryptography on quantum data* where cryptographic tools are developed for information imbedded in quantum systems. A first example is known as the *one-time quantum pad* where sender Alice and receiver Bob share *a priori* a pair of maximally entangled particles and use them to teleport [8] an arbitrary qubit (quantum bit) from Alice to Bob. The only public transmission of this scheme is a pair of classical random bits from sender to receiver, allowing him to reconstruct the original state she wanted to communicate.

A second example is the *Quantum Vernam Cipher* [2] where a classical key of four possible values is used by Alice who applies one of four unitary (Pauli) operators 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. An interesting difference between the quantum and classical scenario is that two key bits are required to encrypt a general qubit in the quantum setting [2], but this may be reduced to nearly one key bit to encrypt a qubit almost perfectly if we tolerate arbitrarily small errors, as long as it is not entangled with Eve [32]. It was also demonstrated recently how the secret key used for Quantum Vernam Cipher may be reused [22] when the plaintexts are classical.

Quantum error-correcting codes have lead to the notion of *Quantum Message Authentication* [3] 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. Surprisingly, quan-

tum authentication requires quantum encryption, whereas classically these two tasks are fairly independent from each other. A very interesting notion of *Uncloneable Encryption*, linking Quantum Encryption and Quantum Authentication, was later introduced by Gottesman [30].

We conclude with a short list of recent quantum cryptographic applications: *Quantum Secret Sharing* [17] where the secret to be shared is a quantum state, *Verifiable Quantum Secret Sharing* [20] offers the extra guarantee that if enough honest people are involved the secret may be uniquely reconstructed, *Multi-Party Quantum Computation* [20] allows multi-party evaluation of a quantum circuit in which each party secretly provides some of the input quantum states, and *Quantum Zero-Knowledge* [21] that generalizes the classical notion although "rewinding" a quantum computer is impossible.

References

[1] A. Ambainis. A new protocol and lower bounds for quantum coin flipping. *J. Comput. Syst. Sci.*, 68(2):398–416, 2004.

[2] A. Ambainis, M. Mosca, A. Tapp and R. de Wolf. Private quantum channels. In *FOCS '00: Proceedings of the 41st IEEE Symposium on Foundations of Computer Science*, pages 547–553, 2000.

[3] H. Barnum, C. Crépeau, D. Gottesman, A. Smith and A. Tapp. Authentication of quantum messages. In *FOCS '02: Proceedings of the 43rd IEEE Symposium on Foundations of Computer Science*, pages 449–458, 2002.

[4] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3124, 1992.

[5] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin. Experimental quantum cryptography. *J. Cryptol.*, 5(1):3–28, 1992.

[6] C. H. Bennett, D. Bethune, G. Brassard, N. Donnangelo, A. K. Ekert, C. Elliott, J. Franson, C. Fuchs, M. Goodman, R. Hughes (Chair), P. Kwiat, A. Migdall, S.-W. Nam, J. Nordholt, J. Preskill and J. Rarity. A quantum information science and technology roadmap, Part 2: Quantum cryptography, Version 1.0. *Advanced Research and Development Activity (ARDA)*, July 2004. Available at `http://qist.lanl.gov/qcrypt_map.shtml`.

[7] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE international Conference on Computers, Systems and Signal Processing, Bangalore, India*, pages 175–179, 1984.

[8] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[9] C. H. Bennett, G. Brassard, C. Crépeau and U. Maurer. Generalized privacy amplification. *IEEE Transaction on Information Theory*, 41(6):1915–1923, 1995.

[10] C. H. Bennett, G. Brassard, C. Crépeau and M.-H. Skubiszewska. Practical quantum oblivious transfer. In *Advances in Cryptology: Proceedings of Crypto'91*, pages 351–366.

[11] C. H. Bennett, G. Brassard and A. K. Ekert. Quantum cryptography. *Scientific American*, 267(4):50–57, October 1992.

[12] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin and William K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Physical Review Letters*, 76:722–725, 1996.

[13] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers and J. Oppenheim. The universal composable security of quantum key distribution. In *Proceedings of Second Theory of Cryptography Conference: TCC 2005*, Cambridge, MA, USA, February 10-12, 2005. `http://arXiv.org/abs/quant-ph/0409078`.

[14] E. Biham, M. Boyer, P. O. Boykin, T. Mor and V. Roychowdhury. A proof of the security of quantum key distribution (extended abstract). In *STOC '00: Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pages 715–724, 2000.

[15] G. Brassard, C. Crépeau, R. Jozsa and D. Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In *FOCS '93: Proceedings of the 34th IEEE Symposium on Foundations of Computer Science*, pages 362–371, 1993.

[16] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In *Advances in Cryptology: Proceedings of Eurocrypt'93*, pages 410–423, 1993.

[17] R. Cleve, D. Gottesman and H.-K. Lo. How to share a quantum secret. *Phys. Rev. Lett.*, 83(3):648–651, 1999.

[18] D. Collins, N. Gisin and H. De Riedmatten. Quantum relays for long distance quantum cryptography. *J. Mod. Optics*, 52(5):735, 2005.

[19] C. Crépeau, P. Dumais, D. Mayers and L. Salvail. Computational collapse of quantum state with application to oblivious transfer. In *Proceedings of First Theory of Cryptography Conference: TCC 2004*, Cambridge, MA, USA, February 19-21, pages 374–393, 2004.

[20] C. Crépeau, D. Gottesman and A. Smith. Secure multi-party quantum computation. In *STOC '02: Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, pages 643–652, 2002.

[21] I. Damgård, S. Fehr and L. Salvail. Zero-knowledge proofs and string commitments withstanding quantum attacks. In *Advances in Cryptology: Proceedings of Crypto'04*, pages 254–272, 2004.

[22] I. Damgård, T. Pedersen and L. Salvail. On the key-uncertainty of quantum ciphers and the computational security of one-way quantum transmission. In *Advances in Cryptology: Proceedings of Eurocrypt'04*, pages 91–108, 2004.

[23] D. Deutsch, A. K. Ekert, R. Jozsa, C. Macchiavello, S. Popescu and A. Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Physical Review Letters*, 77:2818–2821, 1996. Erratum, *Physical Review Letters*, 80:2022, 1998.

[24] A. Einstein, B. Podolsky and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935.

[25] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[26] A. K. Ekert, J. Rarity, P. Tapster and G. Palma. Practical quantum cryptography based on two-photon interferometry. *Physical Review Letters*, 69:1293–1295, 1992.

[27] D. G. Enzer, P. G. Hadley, R. J. Hughes, C. G. Peterson and P. G. Kwiat. Entangled-photon six-state quantum cryptography. *New Journal of Physics*, 4:45.1–45.8, 2002.

[28] S. Even, O. Goldreich and A. Lempel. A randomized protocol for signing contracts. *Commun. ACM*, 28(6):637–647, 1985.

[29] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74:145–195, 2002.

[30] D. Gottesman. Uncloneable encryption. *Quantum Information and Computation*, 3:581–602, 2003. `http://arXiv.org/abs/quant-ph/0210062`.

[31] D. Gottesman and H.-K. Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Trans. Inf. Theory*, 49:457–475, 2003.

[32] P. Hayden, D. Leung, P. W. Shor and A. Winter. Randomizing quantum states: Constructions and applications. *Commun. Math. Phys.*, 250(2):371–391, 2004.

[33] R. J. Hughes, J. E. Nordholt, D. Derkacs and C. G. Peterson. Practical free-space quantum key distribution over 10 km in daylight and at night. *New Journal of Physics*, 4:43.1–43.14, 2002.

[34] R. Impagliazzo and S. Rudich. Limits on the provable consequences of one-way permutations. In *STOC '89: Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, pages 44–61, 1989.

[35] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka and K. Nakamura. Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptography. *Electronics Letters*, 43(9):L1217–L1219, 2004.

[36] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster and J. G. Rarity. Quantum cryptography: A step towards global key distribution. *Nature* 419:450, 3 October 2002.

[37] H.-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, 1997. Originally `http://arXiv.org/abs/quant-ph/9603004`.

[38] H.-K. Lo and H. F. Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D*, 120:177–187, 1998.

[39] D. Mayers. The trouble with quantum bit commitment. http://arXiv.org/abs/quant-ph/9603015. The author first discussed the result in Montréal at a workshop on quantum information theory held in October 1995.

[40] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, April 1997.

[41] D. Mayers. Unconditional security in quantum cryptography. *J. ACM*, 48(3):351–406, 2001.

[42] J. Ouellette. Quantum key distribution. *The Industrial Physicist*, pages 22–25, January 2005.

[43] M. Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Harvard Aiken Computation Laboratory, 1981.

[44] J. G. Rarity, P. R. Tapster, P. M. Gorman and P. Knight. Ground to satellite secure key exchange using quantum cryptography. *New Journal of Physics*, 4:82.1–82.21, 2002.

[45] P. W. Shor and J. Preskill. Simple proof of security of BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, 2000.

[46] G. Stix. Best-kept secrets – quantum cryptography has marched from theory to laboratory to real products. *Scientific American*, 280(1):78–83, January 2005.

[47] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden. Quantum key distribution over 67 km with a plug&play system. *New Journal of Physics*, 4:41.1–41.8, 2002.

[48] P. Townsend, J. Rarity and P. Tapster. Single photon interference in 10km long optical fibre interferometer. *Electronics Letters*, 29:1291–1293, 1993.

[49] M. Wegman and J. Carter. New hash functions and their use in authentication and set equality. *J. Comp. Sys. Sc.*, 22:265–279, 1981.

[50] S. Wiesner. Conjugate coding. *Sigact News*, 15(1):78–88, 1983. original manuscript written circa 1970.