A Bibliography of Quantum Cryptography*

Gilles Brassard †

Département IRO
Université de Montréal.
C.P. 6128, Succursale "A"
Montréal (Québec) Canada H3C 3J7

3 December 1993

Abstract

This paper provides an extensive annotated bibliography of papers that have been written on quantum cryptography and related topics.

1. Introduction

For ages, mathematicians have searched for a system that would allow two people to exchange messages in perfect privacy. 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 [1]. 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 [2]. Quantum cryptographic 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,

* A preliminary version of this paper has appeared in the ACM newsletter *Sigact News* [75].
† Supported in part by Canada's NSERC E. W. R. Steacie Memorial Fellowship and Québec's FCAR.

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.

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 [3, 4], 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 their 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.

In the past few years, 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 [2] worked over a distance of 32 centimetres in 1989. Two additional experimental demonstrations have been set up since, which work over significant lengths of optical fibre [13, 14].

The purpose of this work is to provide an extensive bibliography of most papers ever written on quantum cryptography, including some unpublished papers. In addition, a limited selection of key papers that describe techniques of crucial importance to quantum cryptography, such as privacy amplification [63, 73], is included. The papers are listed in chronological order within each section.

2. The various uses of quantum physics for cryptography

Quantum cryptography is best known for key distribution. The most complete paper written on the subject, which also describes the original prototype, is [2]. However, two applications of quantum physics to cryptography were discovered well before quantum key distribution: *quantum bank notes* are impossible to counterfeit and *quantum multiplexing* allows one party to send two messages to another party in a way that the receiver can obtain either message at his choice, but reading one destroys the other irreversibly [1]. (The notion of multiplexing was reinvented ten years later in the context of classical cryptography under the name of *oblivious transfer*, which will be used henceforth in this paper.) A more elaborate quantum oblivious transfer protocol was designed subsequently [3]. Another quantum cryptographic task that has been studied extensively is bit commitment [4]. Applications of bit commitment and oblivious transfer are mentioned in Section 9.

1. Wiesner, S., “Conjugate coding”, *Sigact News*, vol. 15, no. 1, 1983, pp. 78 – 88; original manuscript written *circa* 1970.
2. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. and Smolin, J., “Experimental quantum cryptography”, *Journal of Cryptology*, vol. 5, no. 1, 1992, pp. 3 – 28. Preliminary version in *Advances in Cryptology — Eurocrypt '90 Proceedings*, May 1990, Springer – Verlag, pp. 253 – 265.
3. Bennett, C. H., Brassard, G., Crépeau, C. and Skubiszewska, M.–H., “Practical quantum oblivious transfer”, *Advances in Cryptology — Crypto '91 Proceedings*, August 1991, Springer – Verlag, pp. 351 – 366.
4. Brassard, G., Crépeau, C., Jozsa, R. and Langlois, D., “A quantum bit commitment scheme provably unbreakable by both parties”, *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science*, November 1993, pp. 362 – 371.

3. Alternative quantum key distribution protocols

The original quantum key distribution protocol uses four different polarization states of single photons as carrier of quantum information [2], but other approaches have been put forward. Early variations were to use Einstein–Podolsky–Rosen entangled pairs [5], to use only two nonorthogonal states rather than four [6], and to use phase modulation rather than polarization [6, 7]. A theoretical advantage of using entangled pairs is to allow the key to remain protected by the uncertainty principle even in storage, rather than merely in transit. More recent variations use rejected-data protocols [8, 9], photon pairs [10], and bright light [11].

5. Ekert, A. K., “Quantum cryptography based on Bell's theorem”, *Physical Review Letters*, vol. 67, no. 6, 5 August 1991, pp. 661 – 663.
6. Bennett, C. H., “Quantum cryptography using any two nonorthogonal states”, *Physical Review Letters*, vol. 68, no. 21, 25 May 1992, pp. 3121 – 2124.
7. Ekert, A. K., Rarity, J. G., Tapster, P. R. and Palma, G. M., “Practical quantum cryptography based on two-photon interferometry”, *Physical Review Letters*, vol. 69, no. 9, 31 August 1992, pp. 1293 – 1295.
8. Barnett, S. M. and Phoenix, S. J. D., “Information-theoretic limits to quantum cryptography”, *Physical Review A*, vol. 48, no. 1, July 1993, pp. R5 – R8.

9. Barnett, S. M. and Phoenix, S. J. D., "Bell's inequality and rejected-data protocols for quantum cryptography", *Journal of Modern Optics*, vol. 40, no. 8, August 1993, pp. 1443 – 1448.
10. Huttner, B. and Peres, A., "Quantum cryptography with photon pairs", *Journal of Modern Optics*, to appear.
11. Wiesner, S., "Quantum cryptography with bright light", manuscript, 1993.

4. Implementation

At least three experimental apparatuses have been built for implementing quantum key distribution, in addition to the original 32 centimetre implementation [2]. A prototype built in Geneva follows the original protocol of [2]: it uses four different polarization states to carry the quantum information over more than one kilometre of optical fibre [14]. Another prototype built independently by British Telecom in association with the Defence Research Agency works by phase modulation over a distance of 10 kilometres of fibre; it is described in a sequence of two papers [12, 13]. Yet another experimental demonstration is in the works, which uses Einstein–Podolsky–Rosen entangled pairs sent over kilometres of fibre [15].

12. Townsend, P. D., Rarity, J. G. and Tapster, P. R., "Single photon interference in a 10 km long optical fibre interferometer", *Electronics Letters*, vol. 29, no. 7, 1 April 1993, pp. 634 – 635.
13. Townsend, P. D., Rarity, J. G. and Tapster, P. R., "Enhanced single photon fringe visibility in a 10 km–long prototype quantum cryptography channel", *Electronics Letters*, vol. 29, no. 14, 8 July 1993, pp. 1291 – 1293.
14. Muller, A., Breguet, J. and Gisin, N., "Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km" *Europhysics Letters*, vol. 23, no. 6, 20 August 1993, pp. 383 – 388.
15. Rarity, J. G., Owens, P. C. M. and Tapster, P. R., "Quantum random number generation and key sharing", *Journal of Modern Optics*, to appear.

5. Eavesdropping

The key distribution protocol described in [2] has been proven secure regardless of the eavesdropper's computing power, but assuming some restrictions on the type of attack, such as requiring eavesdropping to be independent from one light pulse to another. More sophisticated attacks have been analysed in the papers quoted below, but none of them has yet presented a direct threat to quantum key distribution. Note that, contrary to all known quantum key distribution schemes, the quantum bit commitment protocol of [4] has been formally proven invulnerable to all attacks consistent with the laws of quantum mechanics.

16. Werner, M. J. and Milburn, G. J., "Eavesdropping using quantum-nondemolition measurements", *Physical Review A*, vol. 47, no. 1, January 1993, pp. 639 – 641.
17. Barnett, S. M., Huttner, B. and Phoenix, S. J. D., "Eavesdropping strategies and rejected-data protocols in quantum cryptography", *Journal of Modern Optics*, vol. 40, no. 12, December 1993, pp. 2501 – 2513.
18. Huttner, B. and Ekert, A. K., "Tolerable noise in quantum cryptosystems", *Journal of Modern Optics*, to appear.
19. Ekert, A. K., Huttner, B., Palma, G. M. and Peres, A., "Eavesdropping on quantum cryptosystems", *Physical Review A*, submitted.

6. Popular accounts

These papers appeared in popular science magazines. Many of them offer easy reading for the non specialist. The best introduction to quantum cryptography is perhaps [33].

20. Gottlieb, A., "Conjugal secrets — The untappable quantum telephone", *The Economist*, vol. 311, 22 April 1989, page 81.
21. Wallich, P., "Quantum cryptography", *Scientific American*, May 1989, pp. 28 – 30.
22. Deutsch, D., "Quantum communication thwarts eavesdroppers", *New Scientist*, 9 December 1989, pp. 25 – 26.
23. Peterson, I., "Bits of uncertainty: Quantum security", *Science News*, vol. 137, 2 June 1990, pp. 342 – 343.
24. Ekert, A. K., "La mécanique quantique au secours des agents secrets", *La Recherche*, June 1991, pp. 790 – 791.
25. Ekert, A. K., "Przygoda w kwantowej krainie szyfrów", *Wiedza i Zycie*, July 1991, pp. 45 – 49.
26. Stewart, I., "Schrödinger's catflap", *Nature*, vol. 353, 3 October 1991, pp. 384 – 385.
27. Flam, F., "Quantum cryptography's only certainty: Secrecy", *Science*, vol. 253, 1991, page 858.
28. Ekert, A. K., "Adventures in quantum cryptoland" (in Japanese), *Parity*, vol. 7, February 1992, pp. 26 – 29.
29. Ekert, A. K., "Cryptography — Beating the code breakers", *Nature*, vol. 358, 2 July 1992, pp. 14 – 15.

30. Bennett, C. H., "Quantum cryptography: Uncertainty in the service of privacy", *Science*, vol. 257, 7 August 1992, pp. 752 – 753.
31. Delahaye, J.–P., "Cryptographie quantique", *Pour la Science*, August 1992, pp. 101 – 106.
32. Zimmer, C., "Perfect Gibberish", *Discover*, September 1992, pp. 92 – 99.
33. Bennett, C. H., Brassard, G. and Ekert, A. K., "Quantum cryptography", *Scientific American*, October 1992, pp. 50 – 57. Appeared in December 1992 as translation into German (*Spektrum der Wissenschaft*, pp. 96 – 104), Italian (*Le Scienze*, pp. 84 – 93), Japanese (*Saiensu*, pp. 50 – 60), and Polish (*Świat Nauki*, pp. 28 – 37), among others.
34. Collins, G. P., "Quantum cryptography defies eavesdropping", *Physics Today*, November 1992, pp. 21 – 23.
35. Ekert, A. K., "Quantum keys for keeping secrets", *New Scientist*, 16 January 1993, pp. 24 – 28.
36. Townsend, P. D. and Phoenix, S. J. D., "Quantum mechanics will protect area networks", *Opto and Laser Europe*, July 1993, pp. 17 – 20.

7. Historical papers

These papers are superseded by other papers listed above; nevertheless they are of historical interest. Of particular importance are the first paper ever *published* on quantum cryptography [37] (recall that [1] was *written* earlier) and the first paper that gives a complete description of the quantum key distribution protocol [42].

37. Bennett, C. H., Brassard, G., Breidbart, S. and Wiesner, S., "Quantum cryptography, or unforgeable subway tokens", *Advances in Cryptology: Proceedings of Crypto 82*, August 1982, Plenum Press, pp. 267 – 275.
38. Bennett, C. H., Brassard, G. and Breidbart, S., "Quantum cryptography II: How to re-use a one-time pad safely even if $\mathcal{P} = \mathcal{NP}$", unpublished manuscript, November 1982.
39. Bennett, C.H. and Brassard, G., "Quantum cryptography and its application to provably secure key expansion, public-key distribution, and coin-tossing", *IEEE International Symposium on Information Theory*, September 1983, page 91.
40. Bennett, C. H., Brassard, G., Breidbart, S. and Wiesner, S., "Eavesdrop-detecting quantum communications channel", *IBM Technical Disclosure Bulletin*, vol. 26, no. 8, January 1984, pp. 4363 – 4366.
41. Bennett, C.H. and Brassard, G., "An update on quantum cryptography", *Advances in Cryptology: Proceedings of Crypto 84*, August 1984, Springer – Verlag, pp. 475 – 480.

42. Bennett, C. H. and Brassard, G., "Quantum cryptography: Public-key distribution and coin tossing", *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December 1984, pp. 175 – 179.
43. Bennett, C. H. and Brassard, G., "Quantum public key distribution system", *IBM Technical Disclosure Bulletin*, vol. 28, no. 7, December 1985, pp. 3153 – 3163.
44. Crépeau, C. and Kilian, J., "Achieving oblivious transfer using weakened security assumptions", *Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science*, October 1988, pp. 42 – 52.
45. Bennett, C. H. and Brassard, G., "The dawn of a new era for quantum cryptography: The experimental prototype is working!", *Sigact News*, vol. 20, no. 4, 1989, pp. 78 – 82.
46. Brassard, G. and Crépeau, C., "Quantum bit commitment and coin tossing protocols", *Advances in Cryptology — Crypto '90 Proceedings*, August 1990, Springer – Verlag, pp. 49 – 61.

8. Other papers

Here are various other papers, theses and book chapters that have been written on quantum cryptography.

47. Wiedemann, D., "Quantum cryptography", *Sigact News*, vol. 18, no. 2, 1987, pp. 48 – 51; but please read also [48].
48. Bennett, C. H. and Brassard, G., "Quantum public key distribution reinvented", *Sigact News*, vol. 18, no. 4, 1987, pp. 51 – 53.
49. Brassard, G., *Modern Cryptology*, Chapter 6, Springer – Verlag, Lecture Notes in Computer Science, vol. 325, 1988.
50. Crépeau, C., *Correct and Private Reductions among Oblivious Transfers*, PhD thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 1990.
51. Ekert, A. K., *Correlations in Quantum Optics*, Thesis submitted for the Degree of Doctor of Philosophy at the University of Oxford, Wolfson College, Oxford University, September 1991.
52. Bennett, C. H., Brassard, G. and Mermin, N. D., "Quantum cryptography without Bell's theorem", *Physical Review Letters*, vol. 68, no. 5, 3 February 1992, pp. 557 – 559.
53. Brassard, G., *Cryptologie contemporaine*, Chapter 7, Masson, 1992.

54. Ekert, A. K., “Quantum cryptography and Bell’s theorem”, in *Quantum Measurement in Optics* (P. Tombesi and D. Walls, eds), Plenum Press, New York, 1992, pp. 413 – 418.
55. Ardehali, M., “Efficient quantum cryptography”, manuscript, 1992.
56. Blow, K. J. and Phoenix, S. J. D., “On a fundamental theorem of quantum cryptography”, *Journal of Modern Optics*, vol. 40, no. 1, January 1993, pp. 33 – 36.
57. Phoenix, S. J. D. and Townsend, P. D., “Quantum cryptography and secure optical communication”, *British Telecom Technology Journal*, vol. 11, no. 2, April 1993, pp. 65 – 75.
58. Barnett, S. M., Ekert, A. K. and Phoenix, S. J. D., “Optical key to quantum cryptography”, *SERC Nonlinear Optics Update*, United Kingdom Science and Engineering Research Council, vol. 5, Summer 1993, pp. 3 – 7.
59. Phoenix, S. J. D., “Quantum cryptography without conjugate coding”, *Physical Review A*, vol. 48, no. 1, July 1993, pp. 96 – 102.
60. Crépeau, C., “Quantum oblivious transfer”, *Journal of Modern Optics*, to appear.

9. Useful tools and related papers

Raw quantum cryptography is useless in practice because limited eavesdropping may be undetectable, yet it may leak some information, and errors are to be expected even in the absence of eavesdropping. Also, we must protect against an eavesdropper who would impersonate Alice for Bob and Bob for Alice. For these reasons, quantum cryptography must be supplemented by classical tools such as privacy amplification [63, 73], error correction [71] and authentication [62]. Additional useful information-theoretic tools are provided in [70]. Quantum bit commitment [4] can be used to obtain zero-knowledge proofs [67] for arbitrary **NP** statements [68, 65]. Quantum oblivious transfer [3] can be used for discreet decision making [64, 66]. High-efficiency single-photon detectors [72] are crucial for photon-based quantum cryptography. Quantum teleportation [69] may be useful to increase the distance for quantum key distribution. The Einstein–Podolsky–Rosen effect is ubiquitous in quantum cryptography [61].

61. Einstein, A., Podolsky, B. and Rosen, N., “Can quantum-mechanical description of physical reality be considered complete?”, *Physical Review*, vol. 47, 1935, pp. 777 – 780. Reprinted in *Quantum theory and measurement* (J. A. Wheeler and W. Z. Zurek, eds), Princeton University Press, 1983.
62. Wegman, M. N. and Carter, J. L., “New hash functions and their use in authentication and set equality”, *Journal of Computer and System Sciences*, vol. 22, 1981, pp. 265 – 279.

63. Bennett, C. H., Brassard, G. and Robert, J.–M., "Privacy amplification by public discussion", *SIAM Journal on Computing*, vol. 17, no. 2, April 1988, pp. 210 – 229.
64. Kilian, J., "Founding cryptography on oblivious transfer", *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, May 1988, pp. 20 – 31.
65. Brassard, G., Chaum, D. and Crépeau, C., "Minimum disclosure proofs of knowledge", *Journal of Computer and System Sciences*, vol. 37, 1988, pp. 156 – 189.
66. Crépeau, C., "Verifiable disclosure of secrets and application", *Advances in Cryptology: Proceedings of Eurocrypt '89*, April 1989, Springer – Verlag, pp. 181 – 191.
67. Goldwasser, S., Micali, S. and Rackoff, C., "The knowledge complexity of interactive proof-systems", *SIAM Journal on Computing*, vol. 18, 1989, pp. 186 – 208.
68. Goldreich, O., Micali, S. and Wigderson, A., "Proofs that yield nothing but their validity, or All languages in **NP** have zero-knowledge proof systems", *Journal of the ACM*, vol. 38, 1991, pp. 691 – 729.
69. Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A. and Wootters, W. K., "Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels", *Physical Review Letters*, vol. 70, 29 March 1993, pp. 1895 – 1899.
70. Maurer, U. M., "Secret key agreement by public discussion from common information", *IEEE Transactions on Information Theory*, vol. 39, no. 3, May 1993, pp. 733 – 742.
71. Brassard, G. and Salvail, L., "Secret-key reconciliation by public discussion", *Advances in Cryptology — Eurocrypt '93 Proceedings*, May 1993, to appear.
72. Kwiat, P. G., Steinberg, A. M., Chiao, R. Y., Eberhard, P. H. and Petroff, M. D., "High-efficiency single-photon detectors", *Physical Review A*, vol. 48, no. 2, August 1993, pp. R867 – R870.
73. Bennett, C. H., Brassard, G., Crépeau, C. and Maurer, U. M., "Generalized privacy amplification", manuscript, 1993.

10. Bibliographies

This bibliography of quantum cryptography [76] has evolved from an earlier version [75]. An earlier bibliography is available [74].

74. Crépeau, C., "Cryptographic primitives and quantum theory", *Proceedings of Workshop on Physics and Computation, PhysComp 92*, Dallas, October 1992, pp. 200 – 204.
75. Brassard, G., "Cryptology column — Quantum cryptography: A bibliography", *Sigact News*, vol. 24, no. 3, 1993, pp. 16 – 20.
76. Brassard, G., "A bibliography of quantum cryptography", this manuscript.

Acknowledgements

I wish to thank Charles H. Bennett, Claude Crépeau, Artur K. Ekert, Neil Gershenfeld, Simon J. D. Phoenix and Paul D. Townsend, who helped me put this bibliography together by supplying corrections, updates and additions to previous versions. I am also grateful to Ron Rivest, whose request for a quantum cryptography bibliography set me in motion for this work. Finally I am most grateful to the Rank Foundation and Artur K. Ekert for making possible the first international workshop on quantum cryptography, which was held in Broadway, England, in March 1993. That was a historical event for the field.