Cryptology Column —
25 Years of Quantum Cryptography [*]

Gilles BRASSARD [†] and Claude CRÉPEAU [†]

Département d'informatique et de R. O.
Université de Montréal
C.P. 6128, Succursale Centre–Ville
Montréal (Québec)
CANADA H3C 3J7

{brassard,crepeau}@iro.umontreal.CA

31 July 1996

1 Introduction

The fates of *SIGACT News* and Quantum Cryptography are inseparably entangled. The exact date of Stephen Wiesner's invention of "conjugate coding" is unknown but it cannot be far from April 1969, when the premier issue of *SIGACT News*—or rather *SICACT News* as it was known at the time—came out. Much later, it was in *SIGACT News* that Wiesner's paper finally appeared [74] in the wake of the first author's early collaboration with Charles H. Bennett [7]. It was also in *SIGACT News* that the original experimental demonstration for quantum key distribution was announced for the first time [6] and that a thorough bibliography was published [19]. Finally, it was in *SIGACT News* that Doug Wiedemann chose to publish his discovery when he reinvented quantum key distribution in 1987, unaware of all previous work but Wiesner's [73, 5].

Most of the first decade of the history of quantum cryptography consisted of this lone unpublished paper by Wiesner. Fortunately, Bennett was among the few initiates who knew of Wiesner's ideas directly from the horse's mouth. His meeting with the first author of this column in 1979 was the beginning of a most fruitful lifelong collaboration. It took us five more years to invent quantum key distribution [4], which is still today the best-known application of quantum mechanics to cryptography. The second author joined in slightly later, followed by a few others. But until the early 1990's, no more than a handful of people were involved in quantum cryptographic research. Since then, the field has taken off with a vengeance, starting with Artur K. Ekert's proposal to use quantum nonlocality for cryptographic purposes [33].

The golden age started in earnest when Ekert organized the first international workshop on quantum cryptography in Broadway, England, in 1993. Since then, many conferences have been devoted at least partly to quantum cryptography, which has become a major

[*] This column borrows heavily from the authors' papers [21, 27] at Pragocrypt '96.

[†] Research supported in part by Canada's NSERC and Québec's FCAR.

international topic. The purpose of the aforementioned 1993 bibliography in *SIGACT News* was to cite as much as possible *all* papers ever written on the subject, including unpublished manuscripts: there were 57 entries in total. Today, such an undertaking would be nearly impossible owing to the explosion of new research in the field.

The purpose of this column is to give an overview of the current research in quantum cryptography. It is not our intention to be exhaustive and we apologize in advance to any researcher whose work we may have omitted. Note that we do not necessarily agree with the claims in every paper mentioned here: this column should not be construed as a seal of approval!

2 Implementation of Quantum Key Distribution

When the first quantum cryptographic prototype was reported in *SIGACT News* [6] in 1989, it was no more than a proof of feasibility with no claim to practicality since it allowed for the perfectly secure transmission of cryptographic material over a distance of 32 centimetres! (See also [3] for a more complete coverage.) Since then, significantly more sophisticated prototypes have been built around the world.

Paul D. Townsend from British Telecom Laboratories, working at times with Christophe Marand, John Rarity, Paul Tapster, Ian Thompson and others, produced a succession of prototypes. In particular, they have implemented quantum key distribution over 30 kilometres of commercial optical fibre [55]. This is 10^5 times the distance covered in the 1989 prototype! However, their prototype operates in laboratory conditions too: all 30 km are spun in a coil, and sender and receiver are in the same room. More recently, Townsend and collaborators have developed a practical demonstration of how quantum cryptography can be used to secure a communication network with many users [71]. Consult [72] for an excellent review of experimental quantum cryptography at BT Laboratories.

Richard Hughes and coworkers at the Los Alamos National Laboratory built a prototype in which the signal goes through 14 kilometres of underground optical fibre that links different buildings [46]. Sender and receiver are still in the same laboratory but the quantum channel is out in the field. They found that the signal is quite stable over reasonable periods of time, excepts on those occasions when workmen play cards in the basement and get a little bit too excited. They are now working on a 24 km experiment as well as on implementing free-space quantum cryptography (without the help of a wave guide such as optical fibre) and they are considering quantum cryptography through satellites. Another successful prototype has been realized in the United States by J. D. Franson, H. Ilves and B. C. Jacobs [36, 38].

Nicolas Gisin from the University of Geneva, working with J. Breguet, Antoine Muller and Hugo Zbinden, built the first prototype in which sender and receiver are separated by a significant distance [63]. In this case, the sender is in Nyon and the receiver in Geneva, 23 kilometres away. Their quantum channel is an optical fibre deployed beneath Lake Geneva. They found that neither fish nor waves cause significant disturbance in the channel.

In addition to prototypes for quantum key distribution, Jaroslav Hrubý is working in Prague at implementing a quantum smart card for identification purposes [44], following the protocol of Claude Crépeau and Louis Salvail [30].

3 Alternative Proposals

Most working prototypes that we are aware of implement the original 1984 quantum key distribution protocol [4], henceforth called BB84, sometimes with the possibility of implementing also Bennett's simplified protocol based on only two nonorthogonal states [2], henceforth called B92. They use either photon polarization (as originally proposed in [4]) or phase and interferometry (as in [2]). Although not yet implemented to the best of our knowledge, other carriers of quantum information have been proposed for implementing BB84 and B92. To cite only two examples, Yi Mu proposed the use of quantized quadrature phase amplitudes of light [62] and Hrubý studied the use of q-deformed quantum mechanics [45].

In addition to alternative implementation proposals for BB84 and B92, genuinely different quantum key distribution protocols have been proposed. We already mentioned Ekert's idea to base quantum cryptography on quantum nonlocality [33]. New and exciting ideas from David Deutsch, Artur K. Ekert, Richard Jozsa, Chiara Macchiavello, Sandu Popescu and Anna Sanpera in Oxford [32] proved wrong earlier claims that the use of nonlocality held no significant benefit over the original BB84 protocol [11]. In particular, the use of entanglement purification techniques [12] yields a protocol that has no analogue along the lines of BB84. In brief, sender and receiver exchange entanglement through a noisy and possibly bugged quantum channel. Because of the potential eavesdropper and also because of natural noise, the resulting entanglement is imperfect. Using entanglement purification (also known as quantum privacy amplification), the legitimate parties distill near-perfect entanglement from their raw material, or they acknowledge failure in case eavesdropping was too severe. Finally the resulting entanglement is used as in Ekert's original protocol [33] (or Mermin's improvement [11]) to exchange a cryptographic key. Alternatively, the resulting entanglement could be used to teleport [8] the cleartext message in full confidentiality.

Another possible use of quantum nonlocality is due to Eli Biham, Bruno Huttner and Tal Mor [16]. Here, users store particles in quantum memories kept in a transmission centre. This allows for secure communication between any pair of users who have particles in the same centre. The centre must cooperate for communication to be established, but it need not be trusted for secrecy. This system can work without quantum channels (if the users bring their quantum information directly to the centre's quantum memory) and it is suitable in theory for building a quantum cryptographic network. A completely different approach to quantum cryptographic networks, not relying on quantum nonlocality, was developed by Simon J. D. Phoenix, Stephen M. Barnett, Paul D. Townsend and Keith J. Blow [65]. The practical feasibility of this approach has been demonstrated at BT laboratories [71].

Other theoretical proposals include Wiesner's idea for a quantum cryptographic system with bright light [75]. J. D. Franson and H. Ilves have a protocol that uses polarization feedback [37]. Bruno Huttner and Asher Peres implement quantum key distribution with (unentangled) pairs of photons [50]. Bruno Huttner, Nobuyuki Imoto, Nicolas Gisin and Tal Mor use weak coherent states for the purpose of significantly reducing the information available to the eavesdropper [49]. Mohammad Ardehali describes a system based on Wheeler's delayed choice experiment [1]. Hideaki Matsueda uses the modulation of spontaneous photon emissions [56]. Lior Goldenberg and Lev Vaidman proposed a quantum cryptographic system based on orthogonal states [42], but this has been criticized by Peres [64, 43].

4 The Security of Quantum Key Distribution

The most important question in quantum cryptography is to determine how secure it really is. Quantum cryptography has fostered new fundamental questions in quantum information theory, such as determining how much information can be measured from a quantum system for a given amount of expected disturbance. These questions go far beyond their quantum cryptographic significance, but it seems that no one had thought of asking them before. In the end, the research generated by these questions may be the most significant legacy of quantum cryptography for theoretical quantum mechanics and physics in general. The work of Christopher Fuchs (and collaborators) is especially remarkable in this respect: even though he does not usually address questions directly relevant to quantum cryptography, he was clearly inspired by it [39, 41, 40, etc.].

In early papers on quantum cryptography such as [3], the security of quantum key distribution was studied under the assumption that the eavesdropper is restricted to making the simplest type of von Neumann measurements on the photons as they fly from the sender to the legitimate receiver. But quantum mechanics allows for much more sophisticated eavesdropping strategies and it is difficult to take all possible attacks into account. Many researchers have studied the security of quantum key distribution under various assumptions on the type of attack allowed by the eavesdropper. The preprint literature on this subject has recently become considerable and we are sure to forget significant contributions. Again, we apologize for possible oversights.

An early paper on information versus disturbance and its quantum cryptographic significance was written by Huttner and Ekert [48]. A subsequent paper by the same authors was written in collaboration with Massimo Palma and Asher Peres [34]. Norbert Lütkenhaus also studied the security of quantum cryptography against eavesdropping [54]. A particularly promising approach is due to Eli Biham and Tal Mor, where they consider what they call the "collective attack" [17, 18]. See also [14] for a study of the security of the parity bit in quantum cryptography. Even though they have retracted their claim of an ultimate proof of security for quantum cryptography in noisy channels, the techniques presented by Hoi–Kwong Lo and Hoi Fung Chau may well prove useful [52]. In addition to the above, we are aware of one claim of unconditional security for BB84 against all possible attacks consistent with quantum mechanics, which is due to Dominic Mayers [58], drawing on work by Andrew C.–C. Yao [76] and earlier work of Mayers in collaboration with Salvail [61].

In practice, it is not sufficient to prove the security of quantum key distribution if the proof simply states the existence of a positive constant ε so that secure key distribution is possible provided the quantum channel has an error rate below ε in the absence of eavesdropping. An explicit bound on ε must be obtained and the question of efficiency must be addressed. Specifically, we must be able to determine a lower bound of how many secure bits can be distilled by privacy amplification [13, 9] as function of the observed error rate on the raw quantum transmission, provided this error rate is below ε. These questions are still open and likely to be difficult if a reasonable error rate is to be tolerated. Initially, it may be better to analyse the efficiency of quantum key distribution under appropriate restrictions on the type of eavesdropping allowed, such as collective attacks, much as was done in [3] for the restriction to von Neumann measurements.

5 Beyond Quantum Key Distribution?

Wiesner's original ideas were ahead of their time even in terms of classical cryptography. Not only did he pioneer the use of quantum mechanics for cryptographic purposes, but one of his original applications was "quantum multiplexing" [74]. In retrospect, this is strangely similar to the very fruitful notion of oblivious transfer that Michael O. Rabin was to put forward more than ten years afterwards [66], unaware of Wiesner's then-unpublished work. Somewhat unfortunately quantum key distribution took centre stage and became synonymous with quantum cryptography in the eyes of many, when in fact quantum cryptography is a considerably richer field.

This is ironic because the 1984 paper that presented quantum key distribution for the first time [4] also addressed the question of achieving another cryptographic task with the help of quantum mechanics: it described a quantum coin-flipping protocol. This protocol left most researchers unimpressed because the same paper also explained how to cheat it! [1] For many years afterwards it was thought that key distribution was the only cryptographic task for which quantum mechanics would allow an unconditionally secure implementation.

Before we proceed, let us review the classical notions of coin flipping, bit commitment and oblivious transfer. The purpose of *coin-flipping* is to allow two parties $\mathcal{A}$ and $\mathcal{B}$ to flip a coin at a distance in such way that neither of them can determine the outcome of the flip by himself but such that both of them will agree on the outcome despite the fact that they do not trust each other. A *bit commitment* scheme allows $\mathcal{A}$ to send something to $\mathcal{B}$ that commits her to a bit b of her choice in such a way that $\mathcal{B}$ cannot tell what b is, but such that $\mathcal{A}$ can later prove him what b originally was. You may think of this as $\mathcal{A}$ sending to $\mathcal{B}$ a note with the value b written on it in a strongbox, and later disclosing him the combination to the safe. In (one-out-of-two) *oblivious transfer* [35], $\mathcal{A}$ transmits two pieces of information w_0 and w_1 to $\mathcal{B}$ who chooses whether to receive w_0 or w_1 but cannot learn both; $\mathcal{A}$ never finds out which information $\mathcal{B}$ chose to receive. In classical settings, coin flipping can be implemented when bit commitment is available and bit commitment can be implemented on top of oblivious transfer, but it is believed that the reverse reductions are not possible.

Despite the fact that Wiesner's protocol for oblivious transfer ("multiplexing channel") had been shown insecure from the start (*circa* 1969), it was not until 1988 that Claude Crépeau and Joe Kilian [29] presented the first alternative protocol. This protocol was clearly secure provided neither parties could store photons for long periods of time and only von Neumann measurements were allowed [25, 26]. The vulnerability to photon storage was easy to circumvent if only a secure bit commitment scheme were available. A more robust version of this protocol, capable of dealing with transmission errors on the quantum channel, was subsequently developed [10]. Then Mayers and Salvail [61] analysed the security of quantum oblivious transfer against the most general attacks allowed by quantum mechanics, under the sole restriction that the legitimate photons are measured one at a time, and they found that the protocol is secure provided a secure bit commitment is available. Finally Yao showed that no restrictions on the type of measurements are necessary at all [76], and Mayers extended the proof to oblivious transfer of strings rather than bits, and considered the possibility

[1] Note that Wiesner also showed how to cheat his own quantum multiplexing technique in the paper that introduced it [74]. Is there something wrong with us quantum cryptographers?!

of errors on the quantum channel [58]. The proof that a secure quantum bit commitment protocol is sufficient to implement secure quantum oblivious transfer was complete. Recall that it is believed in the classical world that one can*not* build secure oblivious transfer from bit commitment alone.

In parallel with the work outlined in the above paragraph, new protocols for quantum bit commitment were developed [23] in order to close the gap and obtain provably unconditionally secure oblivious transfer. This culminated in 1993 with a protocol for quantum bit commitment, henceforth referred to as BCJL, that was robust even in the presence of transmission errors on the quantum channel, and was claimed to be *provably secure* [24]. The future of quantum cryptography was very bright indeed, with new applications such as the identification protocol of Crépeau and Salvail [30] coming up regularly.

The sky fell in October 1995 when Mayers found a subtle flaw in the BCJL "proof" of security [57]. The irony is that the successful attack was identical in spirit—although technically more difficult—to the technique published in 1984 to break the original coin-flipping protocol! The basic flaw was also discovered independently by Lo and Chau [53] even though their attack did not apply directly to BCJL. Since then, Mayers discovered that not only BCJL fails but it cannot be fixed: unconditionally secure quantum bit commitment is impossible [59].

The part of the "proof" of [24] that goes wrong is the claim that $\mathcal{A}$ is committed to a bit. The paper shows that $\mathcal{A}$ is unable to know *at the same time* classical information that would allow her to unveil the commitment as $b = 0$ and as $b = 1$, and concludes that $\mathcal{A}$ cannot change her mind. The first part of the statement is correct, but not the conclusion. As a matter of fact, the first part of the statement is also true of the BB84 coin flipping protocol and we know that *it* can be broken! The correct statement should have been that $\mathcal{A}$ is unable to obtain *at her choosing* information that allows her to unveil the commitment either as $b = 0$ **or** as $b = 1$. This is precisely what we have always known she can do to cheat the BB84 coin flipping protocol: postpone this choice until unveiling of her bit.

Mayers' attack is based on a theorem of Lane P. Hughston, Richard Jozsa and Willam K. Wootters about the classification of quantum ensembles [47]. In a nutshell, this theorem states that when two quantum systems have a similar description it is always possible to postpone the decision of whether a state comes from the first or the second system. A simple application of this theorem is the original 1984 attack against the BB84 coin flipping scheme (which was devised without knowledge of the theorem). Mayers has applied this theorem to the BCJL protocol and thus demonstrated its weakness [57]. In principle $\mathcal{A}$ can create a composite quantum system that allows her to cheat as follows. She sends part of it to $\mathcal{B}$ and keeps the rest. By measuring her part of the system appropriately, she can later force *his* part to collapse to a state allowing her to unveil $b = 0$ or to a state allowing her to unveil $b = 1$. Using a similar theorem, Mayers proved that *any* bit commitment scheme in which $\mathcal{B}$ is unable to tell whether the committed bit is $b = 0$ or $b = 1$ can be cheated by $\mathcal{A}$ [59].

Whether this means that secure quantum cryptography is from now on solely restricted to quantum key exchange is debatable. The rest of this column explains the theoretical and practical consequences of Mayers' result and exhibits current research directions to find reasonable assumptions under which quantum bit commitment and other quantum protocols that are built from it may still be shown secure.

6 Practical Impact

Question: How much impact does Mayers' attack have in practice? **Answer:** Little. The technology required to implement the general attack of Mayers seems to be more or less the power of a quantum computer [20]. (Nevertheless, it is *not proven* that breaking a specific system such as BCJL is as hard as building a quantum computer.) Standard classical cryptosystems such as RSA [67] would also collapse if such machines were built [70]. Indeed, most of public-key cryptography would be wiped out by the quantum computer. Therefore, Mayers' attack has little practical consequence unless standard public-key cryptosystems can be broken as well. Using today's technology it is fairly easy to implement BCJL's bit commitment scheme. This protocol is perfectly secure against any attack by $\mathcal{B}$ that is consistent with the laws of quantum mechanics. Moreover, it is secure against any attack that $\mathcal{A}$ can implement with current technology.

Contrary to constructions of bit commitment and other cryptographic protocols from computational assumptions that can be cracked retroactively when a quantum computer becomes available, constructions based on quantum physics will only be breakable starting at the time when the quantum computer is realized.

Salvail has recently shown [68] that a protocol similar to BCJL is secure against attacks from both parties provided the legitimate photons can only be measured one at a time, even if arbitrary measurements are performed on those photons. Thus only major improvements in quantum technology may eventually yield feasible attacks against the scheme.

7 Alternative security models

Of course, relying on technological limitations is far from being satisfactory from a theoretical point of view, especially for quantum cryptographers! One approach we have considered is to rely temporarily on a different kind of bit commitment (computational for instance) in order to restrict the behaviour of the players and later drop this short-term assumption to obtain a quantum bit commitment not relying on any long-term assumption. This idea is very natural since the bit commitment required for the oblivious transfer protocols of [29, 10] is only used on a short-term basis. Similarly, a protocol for quantum bit commitment, inspired by these oblivious transfer protocols, is described in [27]. The resulting scheme also requires to rely temporarily on a different kind of bit commitment.

The first approach that comes to mind to implement this idea is to use a computational bit commitment (consult [22] for several examples). If we do this assuming that $\mathcal{B}$ is computationally limited, $\mathcal{B}$ may eventually break this computational assumption and figure out $\mathcal{A}$'s temporary commitments. In the proposed scheme this would allow him to find out her global commitment to b as well. Thus the whole protocol is only computationally secure and there is no point using anything quantum at all!

If we follow this line of thought assuming that $\mathcal{A}$ is computationally limited (again consult [22] for several examples), it seems in the proposed scheme that she must break this assumption on-line in order to cheat using Mayers' attack. Nevertheless, Mayers has shown that his attack stretches to this situation, so that $\mathcal{A}$ may arrange to open her commitment as $b = 0$ or $b = 1$ *without breaking the computational assumption* [60]! The computational approach is apparently a dead end but several options remain to be analysed.

Salvail has recently suggested [69] to use an unconditionally secure temporary bit commitment in a multiprover model as introduced in [15]. In this setting, the committing party is split in two entities $\mathcal{A}$ and $\mathcal{A}'$ collaborating but physically separated for a short period of time. They could either be spatially separated (in which case the security will also rely on *relativity*, which guarantees that $\mathcal{A}$ and $\mathcal{A}'$ cannot communicate faster than light) or isolated in Faraday cages to avoid any kind of classical communication between them. Nevertheless, $\mathcal{A}$ and $\mathcal{A}'$ are allowed to communicated *before* and *after* the protocol. The multiparty approach is very promising and will be investigated in a future paper [31].

8 General Cryptographic Protocols

From a theoretical point of view, Mayers' result has completely obliterated the possibility of a secure quantum bit commitment scheme with no further assumption. Does that imply the same for general cryptographic protocols?

A general two-party cryptographic protocol is a scheme that allows $\mathcal{A}$ and $\mathcal{B}$ to compute a publicly known two-argument function f over two inputs x and y, respectively provided by $\mathcal{A}$ and $\mathcal{B}$. This is done in such a way that they both learn $z = f(x, y)$ without disclosing more to $\mathcal{B}$ about x than what is given by knowledge of y and z, and without disclosing more to $\mathcal{A}$ about y than what is given by knowledge of x and z. In a classical model, one-out-of-two oblivious transfer can be used to implement any two-party cryptographic protocol securely [51], and in particular it may be used to achieve bit commitment. Therefore if the latter is not possible, the former should not be either. However, in the quantum model, the standard reduction of bit commitment to one-out-of-two oblivious transfer may not work: in the light of Mayers' result this standard reduction might be cheated as well. Thus, the possibility of a quantum oblivious transfer is not discarded directly by Mayers' result. Nevertheless, if quantum oblivious transfer survives, the power of this primitive would clearly not be the same as in the classical model and therefore current reductions of general cryptographic protocols to one-out-of-two oblivious transfer may no longer work either. Note however that all currently published quantum oblivious transfer protocols are already broken because they rely on the existence of a bit commitment scheme. Some cryptographic protocols might still be achieved, some might not. A number of questions are still open in this area.

From a practical point of view, the remarks we made earlier apply as well: unless an adversary can build a quantum computer, we may continue to think as before Mayers discovered his attack and implement bit commitment, oblivious transfer and general cryptographic protocols securely. Moreover, if we are willing to make extra (temporary) assumptions it may well be that both bit commitment and oblivious transfer can be achieved and, using standard reductions [51, 28], all cryptographic protocols as well, in the multiparty model for instance.

The big lesson to learn from all this is that quantum information is always more elusive than its classical counterpart: extra care must be taken when reasoning about quantum cryptographic protocols and analysing them.

References

[1] Ardehali, M., "Quantum cryptography based on Wheeler's delayed choice experiment", manuscript, 1995. Available at `http://xxx.lanl.gov/ps/quant-ph/9508008`.

[2] Bennett, C. H., "Quantum cryptography using any two nonorthogonal states", *Physical Review Letters*, Vol. 68, no. 21, 25 May 1992, pp. 3121 – 2124.

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

[4] Bennett, C. H. and G. Brassard, "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.

[5] Bennett, C. H. and G. Brassard, "Quantum public key distribution reinvented", *Sigact News*, Vol. 18, no. 4, 1987, pp. 51 – 53.

[6] Bennett, C. H. and G. Brassard, "The dawn of a new era for quantum cryptography: The experimental prototype is working!", *Sigact News*, Vol. 20, no. 4, 1989, pp. 78 – 82.

[7] Bennett, C. H., G. Brassard, S. Breidbart and S. Wiesner, "Quantum cryptography, or Unforgeable subway tokens", *Advances in Cryptology: Proceedings of Crypto 82*, August 1982, Plenum Press, New York, 1983, pp. 267 – 275.

[8] Bennett, C. H., 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", *Physical Review Letters*, Vol. 70, no. 13, 29 March 1993, pp. 1895 – 1899.

[9] Bennett, C. H., G. Brassard, C. Crépeau and U. M. Maurer, "Generalized privacy amplification", *IEEE Transactions on Information Theory*, Vol. IT–41, no. 6, November 1995, pp. 1915 – 1923.

[10] Bennett, C. H., G. Brassard, C. Crépeau and M.–H. Skubiszewska, "Practical quantum oblivious transfer", *Advances in Cryptology — Proceedings of Crypto '91*, August 1991, Springer – Verlag, pp. 351 – 366.

[11] Bennett, C. H., G. Brassard and N. D. Mermin, "Quantum cryptography without Bell's theorem", *Physical Review Letters*, Vol. 68, no. 5, 3 February 1992, pp. 557 – 559.

[12] Bennett, C. H., G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels" *Physical Review Letters*, Vol. 76, no. 5, 29 January 1996, pp. 722 – 725.

[13] Bennett, C. H., G. Brassard and J.–M. Robert, "Privacy amplification by public discussion", *SIAM Journal on Computing*, Vol. 17, no. 2, April 1988, pp. 210 – 229.

[14] Bennett, C. H., T. Mor and J. Smolin, "The parity bit in quantum cryptography", *Physical Review A*, Vol. 54, no. 3, September 1996, in press.

[15] Ben–Or, M., S. Goldwasser, J. Kilian and A. Wigderson, "Multi-prover interactive proofs: How to remove intractability assumptions", *Proceedings of 20th Annual ACM Symposium on Theory of Computing*, 1988, pp. 113 – 132.

[16] Biham, E., B. Huttner and T. Mor, "Quantum cryptography network based on quantum memories", *Physical Review A*, Vol. 54, no. 3, September 1996, in press.

[17] Biham, E. and T. Mor, "On the security of quantum cryptography against collective attacks", manuscript, 1996. Available at `http://xxx.lanl.gov/ps/quant-ph/9605007`.

[18] Biham, E. and T. Mor, "Bounds on information and the security of quantum cryptography", manuscript, 1996. Available at `http://xxx.lanl.gov/ps/quant-ph/9605010`.

[19] Brassard, G., "Cryptology column — Quantum cryptography: A bibliography", *Sigact News*, Vol. 24, no. 3, 1993, pp. 16 – 20.

[20] Brassard, G., "A quantum jump in computer science", in *Computer Science Today*, J. van Leeuwen (editor), Lecture Notes in Computer Science, Vol. 1000, Springer-Verlag, Berlin, 1995, pp. 1 – 14.

[21] Brassard, G., "Recent developments in quantum cryptography", *Proceedings of Pragocrypt '96: 1st International Conference on the Theory and Applications of Cryptology*, Prague, October 1996.

[22] Brassard, G., D. Chaum and C. Crépeau, "Minimum disclosure proofs of knowledge", *Journal of Computer and System Sciences*, Vol. 37, no. 2, 1988, pp. 156 – 189.

[23] Brassard, G. and C. Crépeau, "Quantum bit commitment and coin tossing protocols", *Advances in Cryptology — Proceedings of Crypto '90*, August 1990, Springer – Verlag, pp. 49 – 61.

[24] Brassard, G., C. Crépeau, R. Jozsa and D. Langlois, "A quantum bit commitment scheme provably unbreakable by both parties", *Proceedings of 34th Annual IEEE Symposium on the Foundations of Computer Science*, November 1993, pp. 362 – 371.

[25] Crépeau, C., *Correct and private reductions among oblivious transfers*, PhD thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 1990. (Supervised by Silvio Micali.)

[26] Crépeau, C., "Quantum oblivious transfer", *Journal of Modern Optics*, Vol. 41, no. 12, December 1994, pp. 2445 – 2454.

[27] Crépeau, C., "What is going on with quantum bit commitment?", *Proceedings of Pragocrypt '96: 1st International Conference on the Theory and Applications of Cryptology*, Prague, October 1996.

[28] Crépeau, C., J. van de Graaf and A. Tapp, "Committed oblivious transfer and private multi-party computations", *Advances in Cryptology — Proceedings of Crypto '95*, August 1995, Springer – Verlag, pp. 110 – 123.

[29] Crépeau, C. and J. Kilian, "Achieving oblivious transfer using weakened security assumptions", *Proceedings of 29th Annual IEEE Symposium on Foundations of Computer Science*, 1988, pp. 42 – 52.

[30] Crépeau, C. and L. Salvail, "Quantum oblivious mutual identification", *Advances in Cryptology — Proceedings of Eurocrypt '95*, May 1995, Springer – Verlag, pp. 133 – 146.

[31] Crépeau, C. and L. Salvail, "Quantum bit commitment in multiparty model", in preparation, 1996.

[32] Deutsch, D., A. K. Ekert, R. Jozsa, C. Macchiavello, S. Popescu and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels", submitted to *Physical Review Letters*, 1996. Available at `http://eve.physics.ox.ac.uk/Articles/QC.Articles.html`.

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

[34] Ekert, A. K., B. Huttner, G. M. Palma and A. Peres, "Eavesdropping on quantum cryptosystems", *Physical Review A*, Vol. 50, 1994, pp. 1047 – 1056.

[35] Even, S., O. Goldreich and A. Lempel, "A randomized protocol for signing contracts", *Advances in Cryptology: Proceedings of Crypto 82*, August 1982, Plenum Press, New York, 1983, pp. 205 – 210.

[36] Franson, J. D. and H. Ilves, "Quantum cryptography using optical fibres", *Applied Optics*, Vol. 33, 1994, pp. 2949 – 2954.

[37] Franson, J. D. and H. Ilves, "Quantum cryptography using polarization feedback", *Journal of Modern Optics*, Vol. 41, no. 12, December 1994, pp. 2391 – 2396.

[38] Franson, J. D. and B. C. Jacobs, "Operational system for quantum cryptography", *Electronics Letters*, Vol. 31, 1995, pp. 232 – 234.

[39] Fuchs, C. A., *Distinguishability and Accessible Information in Quantum Theory*, Ph.D. Dissertation, University of New Mexico, 1996.
Available at `http://xxx.lanl.gov/ps/quant-ph/9601020`.

[40] Fuchs, C. A., "Information gain vs. state disturbance in quantum theory", submitted to *Fourth Workshop on Physics and Computation — PhysComp '96*, Boston, November 1996.
Available at `http://xxx.lanl.gov/ps/quant-ph/9605014`.

[41] Fuchs, C. A. and A. Peres, "Quantum state disturbance vs. information gain: Uncertainty relations for quantum information", *Physical Review A*, Vol. 53, no. 4, April 1996, pp. 2038 – 2045.

[42] Goldenberg, L. and L. Vaidman, "Quantum cryptography based on orthogonal states", *Physical Review Letters*, Vol. 75, no. 7, 14 August 1995, pp. 1239 – 1243.

[43] Goldenberg, L. and L. Vaidman, "Reply to comment: Quantum cryptography based on orthogonal states?", *Physical Review Letters*, 1996, in press.
Available at `http://xxx.lanl.gov/ps/quant-ph/9604029`.

[44] Hrubý, J., "Smart-card with interferometric quantum cryptography device", *Proceedings of International Conference on Cryptography: Policy and Algorithms*, Brisbane, July 1995, Lecture Notes in Computer Science, Vol. 1029, Springer – Verlag, 1995, pp. 282 – 289.

[45] Hrubý, J., "Q–deformed quantum cryptography and verification of minimal uncertainty", *Proceedings of Pragocrypt '96: 1st International Conference on the Theory and Applications of Cryptology*, Prague, October 1996.

[46] Hughes, R. J., G. G. Luther, G. L. Morgan, C. G. Peterson and C. Simmons, "Quantum cryptography over underground optical fibers", *Advances in Cryptology — Proceedings of Crypto '96*, August 1996, Springer – Verlag.

[47] Hughston, L. P., R. Jozsa and W. K. Wootters, "A complete classification of quantum ensembles having a given density matrix", *Physics Letters A*, Vol. 183, 1993, pp. 14 – 18.

[48] Huttner, B. and A. K. Ekert, "Information gain in quantum eavesdropping", *Journal of Modern Optics*, Vol. 41, no. 12, December 1994, pp. 2455 – 2466.

[49] Huttner, B., N. Imoto, N. Gisin and T. Mor, "Quantum cryptography with coherent states", *Physical Review A*, Vol. 51, March 1995, pp. 1863 – 1869.

[50] Huttner, B. and A. Peres, "Quantum cryptography with photon pairs", *Journal of Modern Optics*, Vol. 41, no. 12, December 1994, pp. 2397 – 2403.

[51] Kilian, J., "Founding cryptography on oblivious transfer", *Proceedings of 20th Annual ACM Symposium on Theory of Computing*, 1988, pp. 20 – 31.

[52] Lo, H.–K. and H. F. Chau, "Quantum cryptography in noisy channels", manuscript, 1995.
Available at `http://xxx.lanl.gov/ps/quant-ph/9511025`.

[53] Lo, H.–K. and H. F. Chau, "Is quantum bit commitment really possible?", manuscript, 1996. Available at `http://xxx.lanl.gov/ps/quant-ph/9603004`.

[54] Lütkenhaus, N., "Security against eavesdropping in quantum cryptography", *Physical Review A*, Vol. 54, no. 1, July 1996, pp. 97 – 111.

[55] Marand, C. and P. D. Townsend, "Quantum key distribution over distances as long as 30 km", *Optics Letters*, Vol. 20, 15 August 1995, pp. 1695 – 1697.

[56] Matsueda, H., "Quantum cryptography by modulating spontaneous photon emissions", *CLEO Pacific Rim Conference*, July 1995, page 46.

[57] Mayers, D., "The trouble with quantum bit commitment", Presented at a workshop on quantum information theory, Montréal, October 1995.
Available at `http://xxx.lanl.gov/ps/quant-ph/9603015`.

[58] Mayers, D., "Quantum key distribution and string oblivious transfer in noisy channels", *Advances in Cryptology — Proceedings of Crypto '96*, August 1996, Springer – Verlag.

[59] Mayers, D., "Unconditionally secure quantum bit commitment is impossible", submitted to *Fourth Workshop on Physics and Computation — PhysComp '96*, Boston, November 1996. Available at `http://xxx.lanl.gov/ps/quant-ph/9605044`.

[60] Mayers, D., personal communication, 1996.

[61] Mayers, D. and L. Salvail, "Quantum oblivious transfer is secure against all individual measurements", *Proceedings of the Third Workshop on Physics and Computation — PhysComp '94*, Dallas, November 1994, IEEE Computer Society Press, pp. 69 – 77.

[62] Mu, Y., *Quantum Communication and Security*, Masters Thesis, University of Wollongong, Australia, 1994.

[63] Muller, A., H. Zbinden and N. Gisin, "Underwater quantum coding", *Nature*, Vol. 378, 30 November 1995, page 449.

[64] Peres, A., "Quantum cryptography based on orthogonal states?", *Physical Review Letters*, 1996, in press. Available at `http://xxx.lanl.gov/ps/quant-ph/9509003`.

[65] Phoenix, S. J. D., S. M. Barnett, P. D. Townsend and K. J. Blow, "Multi-user quantum cryptography on optical networks" *Journal of Modern Optics*, Vol. 42, 1995, pp. 1155 – 1163.

[66] Rabin, M. O., "How to exchange secrets by oblivious transfer", Technical Memo TR–81, Aiken Computation Laboratory, Harvard University, 1981.

[67] Rivest, R. L., A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, Vol. 21, 1978, pp. 120 – 126.

[68] Salvail, L., *Variations sur le transfert inconscient en cryptographie quantique*, Ph.D. Thesis, Département d'informatique et de recherche opérationnelle, Université de Montréal, 1996.

[69] Salvail, L., personal communication, 1996.

[70] Shor, P., "Algorithms for quantum computation: Discrete logarithm and factoring", *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, 1994, pp. 124 – 134.

[71] Townsend, P. D., personal communication, July 1996.

[72] Townsend, P. D., C. Marand, S. J. D. Phoenix, K. J. Blow and S. M. Barnett, "Secure optical communications systems using quantum cryptography", *Philosophical Transactions of the Royal Society of London A*, Vol. 354, 1996, pp. 805 – 817.

[73] Wiedemann, D., "Quantum cryptography", *Sigact News*, Vol. 18, no. 2, 1987, pp. 48 – 51.

[74] Wiesner, S., "Conjugate coding", *Sigact News*, Vol. 15, no. 1, 1983, pp. 78 – 88; original manuscript written *circa* 1969.

[75] Wiesner, S., "Quantum cryptography with bright light", manuscript, 1993.

[76] Yao, A. C.–C., "Security of quantum protocols against coherent measurements", *Proceedings of 26th Annual ACM Symposium on the Theory of Computing*, 1995, pp. 67 – 75.