

Brief History of Quantum Cryptography: A Personal Perspective

Gilles Brassard *

Université de Montréal

Département d'informatique et de recherche opérationnelle

C.P. 6128, Succursale Centre-Ville

Montréal (Québec), H3C 3J7 Canada

<http://www.iro.umontreal.ca/~brassard>

17 October 2005

Based on my eponymous paper [21] in the
*Proceedings of the IEEE Information Theory Workshop
on Theory and Practice in Information-Theoretic Security,*
Awaji Island, Japan, 17 October 2005.
(With minor improvements on 10 April 2006)

Abstract

Quantum cryptography is the only approach to privacy ever proposed that allows two parties (who do not share a long secret key ahead of time) to communicate with provably perfect secrecy under the nose of an eavesdropper endowed with unlimited computational power and whose technology is limited by nothing but the fundamental laws of nature. This essay provides a personal historical perspective on the field. For the sake of liveliness, the style is purposely that of a spontaneous after-dinner speech.

*Supported in parts by the Natural Sciences and Engineering Research Council of Canada, the Canada Research Chair Programme and the Canadian Institute for Advanced Research.

1 Prehistory

The story begins in the early 1960's, when Stephen Wiesner and Charles Bennett were undergraduate students together at Brandeis University. Having many common friends, they enjoyed talking with each other. Later, after Wiesner had gone to graduate school at Columbia and Bennett at Harvard, they kept in touch. In particular, the former payed frequent visits to the latter's communal house in Boston. During one of those visits¹ in the late 60's or early 70's², Wiesner told Bennett of his ideas for using quantum mechanics to make bank-notes that would be impossible to counterfeit according to the laws of nature, as well as of a "quantum multiplexing" channel, which would allow one party to send two messages to another in a way that the receiving party could decide which message to read but only at the cost of destroying the other message irreversibly.³

Wiesner submitted his paper "Conjugate Coding" to the *IEEE Transactions on Information Theory*.⁴ Unfortunately, it was rejected, probably deemed incomprehensible by the editors and referees⁵ because it was written in the technical language of physicists (which must have seemed normal for a physicist!). It is fortunate that Wiesner had expounded his ideas to Bennett, for they might otherwise have been lost forever. Instead, Bennett mentioned them occasionally to various people in the subsequent years, invariably meeting with very little sympathy until...

¹ Probably... Bennett's memories of those long gone days have somewhat faded.

² Ditto.

³ It can be argued that this marks the invention of Oblivious Transfer—or rather one-out-of-two Oblivious Transfer [30]—ten years before Michael Rabin independently introduced his original concept in the theoretical computer science community [40]. Of course, it took the genius of Rabin to realize the central place that Oblivious Transfer was destined to occupy in the sky of cryptography.

⁴ It is written "Submitted to IEEE, Information Theory" on top of Bennett's surviving copy of the original typewritten manuscript, but it is probably safe to guess that the *Transactions* were meant.

⁵ This is an educated guess.

2 History

One fine afternoon in late October 1979, I was swimming at the beach of a posh hotel in San Juan, Puerto Rico. Imagine my surprise when this complete stranger swims up to me and starts telling me, without apparent provocation on my part, about Wiesner’s quantum banknotes! This was probably the most bizarre, and certainly the most magical, moment in my professional life.⁶ Within hours, we had found ways to mesh Wiesner’s coding scheme with some of the then-new concepts of public-key cryptography [27]. Thus was born a wonderful collaboration that was to spin out quantum teleportation [12], entanglement distillation [17], the first lower bound⁷ on the power of quantum computers [4], privacy amplification [18, 13] and, of course, quantum cryptography [21].

The ideas that Bennett and I tossed around on the beach that day resulted in the first paper ever published on quantum cryptography [11], indeed the paper in which the term “Quantum Cryptography” was coined. It was presented at CRYPTO ’82, an annual conference that had started one year earlier. By a strange twist of history, our paper triggered the belated publication of Wiesner’s original paper in a special issue of the ACM Newsletter SIGACT News [44] that was otherwise devoted to a selection of papers from the earlier CRYPTO ’81 conference.⁸ Thus, “Conjugate Coding” was finally disseminated in 1983, admittedly after Rabin’s independent invention of his original version of Oblivious Transfer [40].

⁶ At the risk of taking some of the magic away, I must confess that it was not by accident that Bennett and I were swimming at the same beach in Puerto Rico. We were both there for the 20th *Annual IEEE Symposium on the Foundations of Computer Science*. Bennett approached me because I was scheduled to give a talk on relativized cryptography [20] on the last day of the Symposium and he thought I might be interested in Wiesner’s ideas. By an amazing coincidence, on my way to San Juan, I had read Martin Gardner’s account [31] of Bennett’s report [3] on Chaitin’s Omega, which had just appeared in the November 1979 “Mathematical Games” column of *Scientific American*—so, I knew the name but I could not recognize Bennett in that swimmer because I did not know what he looked like.

⁷ We were trying to prove that unstructured search requires linear time even on quantum computers but eventually had to settle on our best finding, which was an $\Omega(\sqrt{n})$ lower bound. This result was rejected from all major theoretical computer science conferences until, giving up on conferences, we published it in *SIAM Journal on Computing* [4]. Then, Lov Grover discovered his celebrated algorithm [32] to solve the same unstructured search problem in a matching time in $O(\sqrt{n})$. At first blissfully unaware of our lower bound, he too was disappointed in not being able to do better! This was a rare case in which an algorithm was proven optimal before its discovery!

⁸ The proceedings of that very first CRYPTO had appeared solely as a Technical Report of the University of California at Santa Barbara.

Wiesner’s original banknotes, as well as our improvement, required quantum information to be held captive in one place. This was a major practical drawback—if any of this were ever to become practical, which certainly seemed unlikely at the time—because, in those early days, we were using photon polarization as the carrier of quantum information as if it were the only choice. Strangely, it took us a few years after meeting on the beach before we realized, shortly after the CRYPTO ’82 conference, that God had meant photons to travel rather than to stay put!⁹ This was the insight that made us think of using a quantum channel to transmit confidential information. But, however obvious it may seem now, we did not think of quantum key distribution right away.

At first, we wanted the quantum signal to encode the transmitter’s confidential message in such a way that the receiver could decode it if no eavesdropper were present, but any attempt by the eavesdropper to intercept the message would spoil it without revealing any information. Any such futile attempt at eavesdropping would be detected by the legitimate receiver, alerting him to the presence of the eavesdropper. Since this early scheme was unidirectional, it required the legitimate parties to share a secret key, much as in a one-time pad encryption. The originality of our scheme was that the same one-time pad could be reused safely over and over again if no eavesdropping were detected. Thus, the title of our paper was “Quantum Cryptography II: How to reuse a one-time pad safely even if $P = NP$ ” [10]. We submitted this paper to major theoretical computer science conferences, such as STOC (The *ACM Annual Symposium on Theoretical Computer Science*), but we failed to have it accepted. Contrary to Wiesner’s “Conjugate Coding”, however, our “Quantum Cryptography II” paper has forever remained unpublished (copies are available from the authors).¹⁰

We all but forgot about this early idea in 1983, when we realized how much easier it would be to use the quantum channel to transmit an arbitrarily long *random* secret key. If eavesdropping were detected on the quantum channel, due to unavoidable disturbance, the key would be thrown away; otherwise it could be used safely to transmit a sensitive message by use of the classical one-time pad scheme. In essence, this detour via the one-time pad allowed us to turn nature’s

⁹ This is *really* a shame because Wiesner’s original multiplexing channel already used polarized photons to *transmit* information!

¹⁰ The idea of safely reusing a one-time pad was resurrected two decades later by Ivan Damgård, Thomas Pedersen and Louis Salvail [24, 25], who were totally unaware of our earlier work [10]. It must be said, however, that the scheme put forward by Bennett and me was an unproven hack at best, whereas the new work is beautifully set on firm foundations.

given eavesdropping-*detection* channel into an eavesdropping-*prevention* channel. Moreover, the new scheme was much more robust against lost photons since a random subsequence of a random bit string is still a random bit string, albeit shorter. We wrote up a proposal for the 1983 *IEEE Symposium on Information Theory* (ISIT), which was held in St-Jovite (near my hometown of Montréal) that year. Not only was it accepted (yeah!), but it was granted a long presentation. The corresponding one-page abstract [6]—such is the rule at ISIT—provides the official birth certificate for *Quantum Key Distribution*, which remains to this date the most feasible of all proposed applications for the burgeoning field of quantum information science. So feasible indeed that all you need to implement quantum key distribution is a few chocolate balls [42]! :-)

Shortly thereafter, my good friend Vijay Bhargava was in charge of a special session on coding and information theory for yet another IEEE conference, which took place in Bangalore, India¹¹, in December 1984. He invited me to give a talk on any subject of my choice, and naturally I chose Quantum Cryptography considering how difficult it was to get these ideas published at the time. The resulting paper [7] gave its name to the “BB84 protocol” even though it had been described in detail as early as 1983 at the IEEE ISIT *talk* but not in the *paper* (how much can you say in a one-page abstract?). Retrospectively, it is amusing to note that the only reason the BB84 protocol was finally published is that it had not been submitted to the conference that printed it in its proceedings! Thanks Vijay!

A curious episode took place when Doug Wiedemann, having read Wiesner’s “Conjugate Coding” in SIGACT News, reinvented the *exact* BB84 protocol in 1997, even called it “quantum cryptography”, and published it in SIGACT News [43] as well; see also [8].

Throughout the 1980’s, very few people took quantum cryptography seriously and most people simply ignored it. Eventually, Bennett and I decided we had to *show them* by building a working prototype! Bennett asked John Smolin to help with the hardware and I asked François Bessette and Louis Salvail to help with the software. Essentially without any special budget allocated to the project, we were able, in late October 1989, to establish history’s first secret quantum transmission, over a staggering distance of 32.5 centimetres, precisely on the tenth anniversary of our meeting at the San Juan beach [9, 5]!

¹¹ This conference was organized in parts to celebrate the 75th anniversary of the Indian Institute of Technology.

It remains a mystery to me that this successful prototype made a world of difference to physicists, who suddenly paid attention. In particular, it gave us the opportunity to publish in *Scientific American* [15]. The funny thing is that, while our theory had been serious, our prototype was mostly a joke. Indeed, the largest piece in the prototype was the power supply needed to feed in the order of one thousand volts to Pockels cells, used to turn photon polarization. But power supplies make noise, *and not the same noise for the different voltages needed for different polarizations*. So, we could literally hear the photons as they flew, and zeroes and ones made different noises. Thus, our prototype was unconditionally secure *against any eavesdropper who happened to be deaf!* :-)

Perhaps inspired by our “success”, gifted experimentalists¹² began building ever more sophisticated prototypes capable of realizing quantum key distribution over tens of kilometres of optical fibre, some of which are even commercially available. Line of sight experiments have also been carried out over similar distances. Serious plans already exist to link earth-based users by a quantum cryptographic process mediated by satellite.¹³ The possibilities are endless now that a worldwide quantum cryptographic network is within reach of current technology. Several decades ago, transatlantic telephone communications were carried out by submarine cables. The idea that ordinary people would soon communicate through satellites was as far fetched back then as an array of quantum communication satellites would appear today. As Theodore Roosevelt once said, “The only limit to our realization of tomorrow will be our doubts of today. Let us move forward with strong and active faith.”¹⁴

Far more important than the “success” of our prototype, another factor played a crucial role in the newly-found interest of physicists for quantum cryptography in the early 1990’s. This was the re-invention of quantum key distribution by Artur Ekert, and the fact that he published his ideas in *Physical Review Letters* [29] rather than computer science journals and conferences. Contrary to Wiedemann, however, Ekert did not reinvent the BB84 protocol. Instead, he involved quantum entanglement [28] and the violation of Bell’s theorem [2]. Even though Ekert’s

¹² The list of experimentalists involved goes beyond the scope of this historical essay and we prefer to mention no one rather than to omit many.

¹³ In the “simple” version, the satellite would be privy of the secret key it helped establish. More sophisticated proposals would use quantum entanglement to prevent this weakness. In that case, a dishonest satellite can prevent the legitimate parties from establishing a key at all, but it cannot fool them into believing their key is shared and secret when it is not.

¹⁴ As beautifully engraved in his Memorial in Washington, D.C.

proposal was equivalent to BB84 in a sense [16], the idea proved to be very fertile, particularly after the invention of entanglement distillation [17] and quantum privacy amplification [26]. Thinking about entanglement-based cryptography has made it possible to give much simpler proofs of unconditional security for the original un-entangled BB84 scheme [41]. Moreover, as mentioned already, the use of entanglement could be instrumental in a truly secure satellite-based implementation of quantum cryptography. Finally, whenever the long-term storage of quantum information will become feasible, entanglement-based cryptography will provide a form of key distribution that would remain secure not only against eavesdropping, but also against burglary.

3 Beyond Key Distribution

Many people think that quantum cryptography and quantum key distribution are one and the same. Nothing could be farther from the truth. Let us first recall the two results presented in Wiesner’s original “Conjugate Coding”, which started the entire field. Whether or not his quantum banknotes can be considered “cryptography” is a matter of taste, but there can be no doubt that his quantum multiplexing channel was mainstream cryptography ahead of its time.

One of my most vivid memories took place when our ideas for sending confidential messages by way of quantum signals were being rejected. I had been visiting Bennett at his house in Croton-on-Hudson.¹⁵ As my stay was coming to an end, he drove me back to the train station. I boarded the train; he was facing me on the platform, waving goodbye. And suddenly, we realized that Wiesner’s multiplexing channel could be used to implement Rabin’s oblivious transfer! Bennett was so excited that he started jumping up and down as the doors closed between us. As the train picked up speed, I saw his spectacles flying off into the air. In retrospect, I have seen him more excited only once in the quarter-of-century I have known him: when we invented quantum teleportation one decade later.

You may wonder what the fuss was about. Didn’t I write in the first paragraph of this essay (footnote 3) that Wiesner deserved credit for inventing oblivious transfer? Well, at the time, only Rabin’s original version of oblivious transfer had appeared in the theoretical computer science community [40]. It was already

¹⁵I cannot remember if this episode took place before or after the invention of the BB84 protocol, but I think it was before.

regarded as a powerful primitive, although its universality for secure two-party computation was yet to be established [34]. With hindsight, it is obvious that Rabin’s oblivious transfer and Wiesner’s multiplexing channels are similar, and that the latter can serve to implement the former.¹⁶ Yet, the connection had not occurred to us until that precise instant. Out of the blue, we realized for the first time that quantum mechanics could help solve mainstream (classical) cryptographic problems beyond the mere transmission of confidential information. The sky was the limit¹⁷, which did not prevent Bennett’s eyeglasses from shattering on the train platform.

The other cryptographic task that we studied in the early days was *coin-tossing*. The classical concept had been pioneered by Manuel Blum at CRYPTO ’81 [19]. It is a little-known fact that the 1983 ISIT abstract that introduced quantum key distribution [6], as well as its better known 1984 big brother [7] that gave its name to the BB84 protocol, were just as much about quantum coin-tossing as they were about quantum key distribution. Consider for instance the following excerpt from the original 1983 version:

We also present a protocol for coin-tossing by exchanges of quantum messages. [...] our protocol is secure against traditional kinds of cheating, even by an opponent with unlimited computational power. Ironically, however, it can be subverted by use of a still subtler quantum phenomenon, the so-called Einstein-Podolsky-Rosen [EPR] paradox, which in effect allows the initiating party to toss the coin after the responding party has announced his guess of the outcome.

This was a rare instance of a paper that introduces a new protocol and breaks it in the same paper¹⁸, but I guess everything is allowed in an *invited* paper. Thanks again Vijay! I remember when I was giving talks in the mid 1980’s. I used to spend most of my time on quantum key distribution, because that was the “serious” part, but I had much more fun with coin-tossing. This pleasure came in particular from the need to explain the EPR “paradox” [28] to audiences of computer scientists who had never heard about such a bizarre thing in those days. Also, we were particularly proud of having discovered a way to make “practical”

¹⁶ In fact, they are equivalent [23].

¹⁷ Well, not exactly because Wiesner had explained in “Conjugate Coding” how to defeat his own quantum multiplexing channel! But the attack was very complicated and we were hoping at the time that it would be unfeasible to mount or possible to circumvent.

¹⁸ Wiesner’s multiplexing channel provides another such example.

use of entanglement, albeit for an evil purpose. To this day, I still think our 1983 ISIT paper marks the first explicit use of EPR long-distance correlations for information processing purposes.

Nearly every time I gave this talk, someone would suggest a way to fix the coin-tossing protocol, so as to get around the EPR attack. Invariably, I could find within seconds a way to adapt the attack to the modified protocol... until Claude Crépeau came along. Soon, Crépeau joined the select group of believers, at a time when Bennett and I were possibly the only two active researchers in quantum cryptography. We quickly realized that the quantum coin-tossing protocol could easily be turned into a quantum bit commitment protocol, which is possibly a stronger primitive. But of course, the quantum bit commitment protocol derived from the ISIT83 and BB84 papers were just as vulnerable to an EPR attack as the corresponding coin-tossing protocol.

Helped by Richard Jozsa and Denis Langlois, we thought at some point that we had designed an unbreakable quantum bit commitment scheme [22]. This was a time of high hopes because we had already developed a quantum protocol to achieve oblivious transfer provided bit commitment were available [14].¹⁹ Alas, we had fallen into the same trap that had doomed the earlier ISIT83/BB84 coin-tossing/bit-commitment protocol [37, 35]! After many failed attempts at fixing the problem, it was discovered that unconditionally secure quantum bit commitment is in fact impossible [38, 36].

Does it mean that the benefits of quantum information for cryptography cannot go further than allowing two people to exchange messages with absolute confidentiality? Certainly not! Consider coin-tossing again. Perfect coin-tossing is possible even classically if relativity is invoked [39]. At a very precise moment in time²⁰, each party sends a random bit to the other. The parties have agreed that the coin-toss is heads if the bits are the same and tails otherwise. Cheating is not possible since relativity forbids either party to know what the other party has sent at the time transmission is required.

The situation changes drastically if we restrict our attention to (more usual) protocols in which parties take turn in sending messages to each other. In the

¹⁹ There are strong theoretical reasons to believe that secure oblivious transfer cannot be built out of bit commitment in the classical world [33]. This provides a definite advantage to the quantum setting. In particular, it makes it possible to derive computationally secure quantum oblivious transfer from one-way functions, a feat thought to be classically impossible.

²⁰ We assume that the two parties are in the same inertial reference frame.

case of classical messages, no matter the protocol, it is always possible for one of the two parties to decide the outcome of the coin-toss given enough computational power! Moreover, the availability of quantum computers would make such cheating possible even in practice for most proposed implementations. In the spirit of quantum key distribution, can quantum mechanics help in designing protocols that remain secure against cheaters endowed with unlimited computational power and whose technology is limited by nothing but quantum mechanics? The bad news is that perfect coin-tossing protocols—in which neither party could influence the coin-toss at all—cannot exist even if the players are allowed to transmit quantum messages. However, Andris Ambainis has discovered a wonderful quantum protocol [1] in which neither party can select a desired outcome and influence the process in a way that this wish will come true with a probability better than 75%. This is not perfect, but it is certainly better than anything classically achievable.

And what about quantum bit commitment, oblivious transfer and other post-key-distribution cryptographic tasks? As I write these lines, Crépeau and others are hard at work, finding ever more imaginative ways to resurrect them in our quantum world.

But this is where I put down my pen for tonight.

Acknowledgement

I am most grateful to Charles Bennett, whose assistance with fact-checking was essential, especially in the prehistory part of this essay. In addition, he gave me his advice on several points. Tongue-in-cheek, he pointed out that I should mention that I did *not* accept all his suggestions for otherwise the resulting paper would have been more sedate but boring! This paper owes its existence to the fact that Ueli Maurer invited me to participate in the *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*, Awaji Island, Japan. Furthermore, I acknowledge the help of my students Anne Broadbent and André Allan Méthot in the final stretch of the writing and submission process to the Proceedings of that Workshop [21].

References

- [1] A. Ambainis, “A new protocol and lower bounds for quantum coin flipping”, *Journal of Computer and System Sciences* **68**(2), pp. 398–416, 2004.
- [2] J.S. Bell, “On the Einstein-Podolsky-Rosen paradox”, *Physics* **1**(3), pp. 195–200, 1964.
- [3] C.H. Bennett, “On random and hard-to-describe numbers”, IBM Report RC 7483, 1979.
- [4] C.H. Bennett, E. Bernstein, G. Brassard and U.V. Vazirani, “Strengths and weaknesses of quantum computing”, *SIAM Journal on Computing* **26**(5), pp. 1510–1523, 1997.
- [5] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, “Experimental quantum cryptography”, *Journal of Cryptology* **5**(1), pp. 3–28, 1992.
- [6] C.H. Bennett and G. Brassard, “Quantum cryptography and its application to provably secure key expansion, public-key distribution, and coin-tossing”, *Proceedings of IEEE International Symposium on Information Theory*, St-Jovite, Canada, page 91, September 1983.
- [7] C.H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing”, *Proceedings of IEEE International Conference on Computers, Systems & Signal Processing*, Bangalore, India, pp. 175–179, December 1984.
- [8] C.H. Bennett and G. Brassard, “Quantum public key distribution reinvented”, *Sigact News* **18**(4), pp. 51–53, 1987.
- [9] C.H. Bennett and G. Brassard, “The dawn of a new era for quantum cryptography: The experimental prototype is working”, *Sigact News* **20**(4), pp. 78–82, 1989.
- [10] C.H. Bennett, G. Brassard and S. Breidbart, “Quantum Cryptography II: How to reuse a one-time pad safely even if $P=NP$ ”, Rejected from *15th Annual ACM Symposium on Theory of Computing*, Boston, May 1983. Historical document dated “November 1982” available from the first two authors.
- [11] C.H. Bennett, G. Brassard, S. Breidbart and S. Wiesner, “Quantum cryptography, or Unforgeable subway tokens”, *Advances in Cryptology: Proceedings of Crypto '82*, Santa Barbara, Plenum Press, pp. 267–275, August 1982.

- [12] 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”, *Physical Review Letters* **70**(13), pp. 1895–1899, 1993.
- [13] C. H. Bennett, G. Brassard, C. Crépeau and U. M. Maurer, “Generalized privacy amplification”, *IEEE Transactions on Information Theory* **41**(6), pp. 1915–1923, 1995.
- [14] C. H. Bennett, G. Brassard, C. Crépeau and M.-H. Skubiszewska, “Practical quantum oblivious transfer protocols”, *Advances in Cryptology: Proceedings of Crypto '91*, Santa Barbara, Springer-Verlag, pp. 351–366, August 1991.
- [15] C. H. Bennett, G. Brassard and A. K. Ekert, “Quantum cryptography”, *Scientific American*, pp. 50–57, October 1992.
- [16] C. H. Bennett, G. Brassard and N. D. Mermin, “Quantum cryptography without Bell’s theorem”, *Physical Review Letters* **68**(5), pp. 557–559, 1992.
- [17] C. H. Bennett, 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* **76**(5), pp. 722–725, 1996. Erratum in *ibid* **78**(10), page 2031, 1997.
- [18] C. H. Bennett, G. Brassard and J.-M. Robert, “Privacy amplification by public discussion”, *SIAM Journal on Computing* **17**(2), pp. 210–229, 1988.
- [19] M. Blum, “Coin flipping by telephone: A protocol for solving impossible problems”, *Advances in Cryptology: A Report on Crypto '81*, Santa Barbara, pp. 11–15, August 1982. Reprinted in *Sigact News* **15**(1), pp. 23–27, 1983.
- [20] G. Brassard, “Relativized cryptography”, *Proceedings of 20th Annual IEEE Symposium on the Foundations of Computer Science*, San Juan, pp. 383–391, October 1979.
- [21] G. Brassard, “Brief history of quantum cryptography: A personal perspective”, *Proceedings of IEEE Information Theory Workshop on Theory and Practice in Information Theoretic Security*, Awaji Island, Japan, pp. 19–23, October 2005.
- [22] G. Brassard, 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*, Palo Alto, pp. 362–371, November 1993.

- [23] C. Crépeau, “Equivalence between two flavours of oblivious transfers”, *Advances in Cryptology: Proceedings of Crypto '87*, Santa Barbara, Springer-Verlag, pp. 350–354, August 1988.
- [24] I. Damgård, T. Pedersen and L. Salvail, “On the key-uncertainty of quantum ciphers and the computational security of one-way quantum transmission”, *Advances in Cryptology: Proceedings of Eurocrypt 2004*, Interlaken, Switzerland, Springer-Verlag, pp. 91–108, May 2004.
- [25] I. Damgård, T. Pedersen and L. Salvail, “A quantum cipher with near optimal key-recycling”, *Advances in Cryptology: Proceedings of Crypto 2005*, Santa Barbara, Springer-Verlag, pp. 494–510, August 2005.
- [26] 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**(13), pp. 2818–2821, 1996. Erratum in *ibid* **80**(9), page 2022, 1998.
- [27] W. Diffie and M. E. Hellman, “New directions in cryptography”, *IEEE Transactions on Information Theory* **22**(6), pp. 644–654, 1976.
- [28] A. Einstein, B. Podolsky and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?”, *Physical Review* **47**(10), pp. 777–780, 1935.
- [29] A. K. Ekert, “Quantum cryptography based on Bell’s theorem”, *Physical Review Letters* **67**(6), pp. 661–663, 1991.
- [30] S. Even, O. Goldreich and A. Lempel, “A randomized protocol for signing contracts”, *Communications of the ACM* **28**(6), pp. 637–647, 1985.
- [31] M. Gardner, “The random number omega bids fair to hold the mysteries of the universe”, *Scientific American*, pp. 20–34, November 1979.
- [32] L. K. Grover, “Quantum mechanics helps in searching for a needle in a haystack”, *Physical Review Letters* **79**(2), pp. 325–328, 1997.
- [33] R. Impagliazzo and S. Rudich, “Limits on the provable consequences of one-way permutations”, *21st Annual ACM Symposium on Theory of Computing*, Seattle, pp. 44–61, May 1989.
- [34] J. Kilian, “Founding cryptography on oblivious transfer”, *20th Annual ACM Symposium on Theory of Computing*, Chicago, pp. 20–31, May 1988.

- [35] H.-K. Lo and H.F. Chau, “Is quantum bit commitment really possible?”, document unavailable, 1996. The relevant paper *would be* the original version of <http://arxiv.org/quant-ph/9603004>, March 1996, but only the April 1997 revision is currently available, which is essentially the same as [36].
- [36] H.-K. Lo and H.F. Chau, “Is quantum bit commitment really possible?”, *Physical Review Letters* **78**(17), pp. 3410–3413, 1997.
- [37] D. Mayers, “The trouble with quantum bit commitment”, available at <http://arxiv.org/quant-ph/9603015>, 1996.
- [38] D. Mayers, “Unconditionally secure quantum bit commitment is impossible”, *Physical Review Letters* **78**(17), pp. 3414–3417, 1997.
- [39] S. Micali, personal communication, *circa* 1985.
- [40] M.O. Rabin, “How to exchange secrets by oblivious transfer”, Technical Memo TR-81, Aiken Computation Laboratory, Harvard University, 1981.
- [41] P. W. Shor and J. Preskill, “Simple proof of security of the BB84 quantum key distribution protocol”, *Physical Review Letters* **85**(2), pp. 441–444, 2000.
- [42] K. Svozil, “Staging quantum cryptography with chocolate balls”, available at <http://arxiv.org/physics/0510050>, October 2005.
- [43] D. Wiedemann, “Quantum cryptography”, *Sigact News* **18**(2), pp. 48–51, 1987.
- [44] S. Wiesner, “Conjugate coding”, written *circa* 1970 and belatedly published in *Sigact News* **15**(1), pp. 78–88, 1983.