The dawn of a new era for quantum cryptography: The experimental prototype is working!

Charles H. BENNETT
IBM T. J. Watson Research Laboratory
Yorktown Heights
New York, NY 10598
U.S.A.

Gilles BRASSARD*
Département I. R. O.
Université de Montréal
C.P. 6128, Succ. "A"
Montréal (Québec)
CANADA H3C 3J7

Draft — 29 October 1989

Quantum cryptography has recently entered the experimental era. The first convincingly successful quantum exchange took place a few weeks ago. After a short historical review of quantum cryptography, we report on the apparatus designed by Charles H. Bennett and built by him at the IBM T. J. Watson Research Center in Yorktown Heights, NY, with the help of John Smolin. Our preliminary results follow.

Quantum cryptography was born in the late sixties when Stephen Wiesner wrote "Conjugate Coding". Unfortunately, this highly innovative paper was unpublished at the time and it went mostly unnoticed. In there, Wiesner explained how quantum physics could be used in principle to produce bank notes that would be impossible to counterfeit and how to implement what he called a "multiplexing channel", a notion strikingly similar to what Rabin was to put forward more than ten years later under the name of "oblivious transfer" (in our opinion, it would be fair to give at least equal credit to Wiesner for the concept of oblivious transfer).

Fortunately, one of us (Charles H. Bennett) knew Wiesner quite well and heard about his idea from the horse's mouth. Nevertheless, it was only when he met the other one of us (Gilles Brassard) that quantum cryptography was revived. This happened on the occasion of the 20th IEEE Symposium on the Foundations of Computer Science, held in Puerto Rico in October 1979. Following our discussion of Wiesner's idea, we discovered how to incorporate the (almost new at the time) notion of public key cryptography, resulting in our CRYPTO '82 paper coauthored by Wiesner and Seth Breidbart [BBBW]. This brought Wiesner's paper back to life, and it was subsequently published in *SIGACT News* [Wies], together with a selection of papers from the earlier CRYPTO '81 workshop (for which "real" proceedings were not published).

*Supported in part by Canada's NSERC under grant A4107

Initially, quantum cryptography was thought of by everyone (including ourselves) mostly as a work of science-fiction because the technology required to implement it was out of reach (for instance, one of the protocols in [BBBW] required the ability to keep a single photon bouncing back and forth between two mirrors for a significant amount of time without losing its polarization). Unfortunately, the impact of the CRYPTO '82 conference had left most people under the impression that everything having to do with quantum cryptography was doomed from the start to being unrealistic.

Our main breakthrough came when we realized that photons were never meant to *store* information, but rather to *transmit* it (ironically, half of Wiesner's original paper dealt precisely with the use of quantum physics for the transmission of information). This lead initially to our *self-winding reusable one-time pad* (also coauthored by Breidbart) [BBB], which was still not very practical. Later, Bennett thought of the *quantum public key distribution channel* and Brassard designed the somewhat less realistic *quantum coin-tossing protocol* [BB1, BB2]. This report deals specifically with the experimental quantum public key distribution channel. A good description of the quantum channel itself can be found in chapter 6 of [B].

Let us recall that the purpose of quantum public key distribution is for Alice and Bob to agree on a random key, which must remain secret from an eavesdropper Eve despite her potentially nasty behaviour. Although Eve can jam the channel by excessive interference, she cannot fool Alice and Bob into thinking that they have succeeded when in fact they have not (except with negligible probability).

For about five years thereafter, quantum cryptography was put on the back burner, even though it certainly never left our mind entirely. An amusing event took place in 1987 when the quantum public key distribution channel was reinvented by Wiedemann after he read Wiesner's paper in *SIGACT News* [Wied, BB3]. On a more serious note, quantum cryptography was picked up by other researchers. For instance, Crépeau and Kilian showed how the quantum channel could be used to implement oblivious transfer in a strong way (Wiesner's original multiplexing channel could leak information on both channels), zero-knowledge protocols, and secure two-party computation [CK, C]. Also, the principle of quantum cryptography was described in major popular magazines such as *Scientific American* [Wa] and *The Economist* [G].

With time, it became increasingly obvious that we had to physically implement a quantum cryptography prototype in order to dispel mounting skepticism and demonstrate that our concept is workable. This is what we have now achieved with the help of three students: John Smolin, who helped Bennett build the apparatus at IBM, and François Bessette and Louis Salvail, who wrote the control and display software under Brassard's supervision in Montréal.

The actual set-up will be described elsewhere. Let us only say here that it is relatively inexpensive. It consists mainly of an IBM personal computer with graphic display, various power supplies, one laser used for optical alignment only, one ordinary LED as actual source of photons (really!), one polarizer, one green filter, three Pockels cells, one calcite crystal and two photomultipliers. For the sake of the prototype, the quantum channel itself spans a mere 30 centimetres.

On September 15, 1989, between 1 and 3 in the morning, a limited success was obtained at last: we were able to exchange a key (which was heavily biased toward zero) with a crossover frequency of about 20% (this means that about 20% of Bob's bits were different from the corresponding bits of Alice). This was encouraging but certainly not good enough.

A much more convincing success was recorded in early October after the apparatus was lined-up with more precision. (What a wonderful way for us to celebrate the 10th anniversary of our partnership in quantum cryptography!) In this experiment, Alice sent 64516 light pulses to Bob. The pulses were so faint (0.34 expected photons per pulse) that even an ideal detector would have only about one chance in three of detecting them. The photomultipliers actually used had a quantum efficiency of about 9%, so fewer than one in thirty pulses was detected. The result, after discarding undetected pulses and those received in the wrong basis, was a string of one thousand bits exchanged between Alice and Bob, which contained a mere 66 errors. Furthermore, Alice's string was almost perfectly balanced between zeros and ones. Here are the first 50 bits of Alice and Bob's strings, respectively.

11111000100111110100101010110100010111000000011100

11111000100111110100101010110000010111000000011101

You may think that a 6.6% crossover frequency is intolerable, but this is not so thanks to a *reconciliation protocol* presented by ourselves and Jean-Marc Robert at CRYPTO '85 [BBR1]. Using the blockwise exclusive-or strategy described there, with block sizes 5, 9 and 23 (chosen to optimize the efficiency under an expected 6% crossover frequency), Alice and Bob were able to distill 443 perfectly shared bits (i.e. with crossover frequency equal to zero) from the original one thousand bits. In the process of reconciliation, Alice and Bob figured out a fairly accurate estimate on the number of transmission errors that had occurred on the quantum channel. They decided that their estimated crossover frequency could reasonably be blamed on the imperfections of their channel, and thus they went ahead with the remaining protocols described below. If they had discovered a crossover frequency too high to be attributed to natural causes, they would have concluded that eavesdropping had probably been attempted on the quantum channel and they would have discarded the results of the transmission.

With a 6.6% crossover frequency on the quantum channel, there was a probability of about 5% that some errors would have remained after the reconciliation protocol. In order to confirm that their strings were identical (which *we* meta-knew but Alice and Bob merely suspected), Alice and Bob ran an *equality confirmation protocol* based on universal hashing on their respective strings [BBR2]. The resulting string shrank from 443 bits to 403 bits in the process, but Alice and Bob gained very high confidence that the reconciliation had succeeded: their chance of not detecting an error if there had been one would have been less than 10^{-12}. In the unlikely event that they had found out during the confirmation protocol that the strings had not been properly reconciled, another protocol (not yet described anywhere) would have allowed them to eradicate the remaining errors at the cost of sacrificing roughly 10 additional bits for each error. In that case, they would have subsequently restarted the confirmation protocol in order to make sure that the probability of undetected failure remains below 10^{-12}.

Not only is this 403–bit string shared between Alice and Bob, but it is completely secret from Eve (except for its length) provided that she did not interfere at all with the original quantum transmission. Indeed, both the reconciliation and the confirmation protocols consist of public discussions between Alice and Bob that do not leak any information about the resulting string to someone who is initially ignorant of the original strings. This is true in the strongest information-theoretic sense, even if Eve had unlimited computing power.

In a more adversarial scenario, however, Eve might attempt some discreet eavesdropping on the quantum channel, enough to gain partial information on the quantum transmission, but not so much as to cause it to be rejected by Alice and Bob. Because of the uncertainty principle, any such eavesdropping must attenuate the signal, induce crossovers, or both. The amount of information leaked to Eve can be bounded as a function of the pulse intensity and crossover frequency. In the present case, she cannot hope to obtain significantly more than 30% of Alice's original 1000 bits without disturbing the transmission so severely that it would almost certainly be detected by Alice and Bob during the reconciliation protocol.

Unfortunately, it is not true in general that if Eve knew a proportion p of the original string, then she still knows the same proportion of the string resulting from the reconciliation and confirmation protocols. Nevertheless, a simple calculation shows that she should expect to know roughly a proportion $3p/2$ of the string resulting from the reconciliation protocol (when block sizes 5, 9 and 23 are used), and that the confirmation protocol usually does not cause her to lose bits of information at all. In our setting, this means that Eve should not expect to know more than roughly 200 bits of information about the 403 bits that were left so far. At this point, a *privacy amplification protocol* [BBR2], also based on universal hashing, can be used by Alice and Bob in order to end up with a final shared string of length 175 about which Eve is expected to know less than $\log_2(1+2^{-28}) \approx 5 \times 10^{-9}$ bits of information.

To conclude, here is the historic string that was exchanged between Alice and Bob by the very first successful use of the quantum channel.

$$
\begin{aligned}
&0001100001101000100100010000011001111011110111010100010101 \\
&0110101010001000110100001100101110110010010110000101101101 \\
&0001101111101011110001110010000110000101011101111010110
\end{aligned}
$$

In fact, the above string might not have been hidden from a clever eavesdropper as well as we have claimed (even if she was not clever enough to read this report!) because all the randomized subprotocols involved in the process used pseudo-random bits (which were not even produced with a cryptographically strong pseudo-random generator). Our next experiment will use truly random bits produced by the quantum cryptography apparatus itself. It should be noted that the pseudo-random generator used for the reconciliation protocol was given Alice's birthday as seed (February 23rd, 1989), so that no one would be tempted to think that we used different pseudo-random sequences until the reconciliation was successful. (Honestly, it worked the very first time that we ran the original data obtained by the quantum channel through the reconciliation protocol. However, we must admit that we were lucky to get as many as 443 bits from the reconciliation protocol because the expected number of bits resulting from a 6.6% crossover frequency is roughly 406, which would have produced just over 150 bits for the final string.)

Of course, the next big challenge is to make the quantum channel work over a more significant distance.

Bibliography

[BB1] Bennett, C. H. and G. Brassard, "An update on quantum cryptography", *Advances in Cryptology: Proceedings of Crypto 84*, Santa Barbara, California, August 1984, pp. 475–480.

[BB2] 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.

[BB3] Bennett, C. H. and G. Brassard, "Quantum public key distribution reinvented", *SIGACT News*, Vol. 18, no. 4, Summer 1987, pp. 51–53.

[BBB] Bennett, C. H., G. Brassard and S. Breidbart, "Quantum cryptography II: How to reuse a one-time pad safely even if P=NP", unpublished manuscript available from the authors, November 1982.

[BBBW] Bennett, C. H., G. Brassard, S. Breidbart and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens", *Advances in Cryptology: Proceedings of Crypto 82*, Santa Barbara, California, August 1982, pp. 267–275.

[BBR1] Bennett, C. H., G. Brassard and J.–M. Robert, "How to reduce your enemy's information", *Advances in Cryptology — Crypto '85 Proceedings*, Santa Barbara, California, August 1985, pp. 468–476.

[BBR2] 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.

[B] Brassard, G., *Modern Cryptology: A Tutorial*, Lecture Notes in Computer Science, Vol. 325, Springer–Verlag, Heidelberg, 1988.

[C] Crépeau, C., "Alternatives to Computational Complexity for Secure Oblivious Transfers", PhD Thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, February 1990.

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

[G] Gottlieb, A., "Conjugal secrets — The untappable quantum telephone", *The Economist*, Vol. 311, no. 7599, 22 April 1989, p. 81.

[Wa] Wallich, P., "Quantum cryptography", *Scientific American*, Vol. 260, no. 5, May 1989, pp. 28–30.

[Wied] Wiedemann, D., "Quantum cryptography", *SIGACT News*, Vol. 18, no. 2, Fall 1986 – Winter 1987, pp. 48–51.

[Wies] Wiesner, S., "Conjugate Coding", manuscript written *circa* 1970, unpublished until it appeared in *SIGACT News*, Vol. 15, no. 1, 1983, pp. 78–88.