The early days of experimental quantum cryptography

J. A. Smolin

This paper describes the first quantum cryptography experiment, performed at the IBM Thomas J. Watson Research Center in the summer of 1989 by Charles H. Bennett and the author. The apparatus and some of the lesser-known details of the experiment are illustrated and discussed, and quantum cryptography is discussed in the light of some of the more recent research. Also included as an appendix is a short essay about Bennett written by Rolf Landauer.

Introduction

I would like to share with the reader some of my experiences in the early days of quantum cryptography [1, 2], beginning with the summer of 1989 when I had just graduated from MIT. I would have been happy to do nothing all summer, but, since I already knew Charlie Bennett, mostly through his stepson George Dyer, I knew that Charlie wanted help building his quantum cryptography experiment, so I came to IBM for the summer to help him out.

I assume that readers, for the most part, know how the Bennett–Brassard scheme for quantum key distribution works [3]. For those who don't, a good review can be found in [4]. Briefly, *Alice* (the sender in the protocol) sends a single photon in one of four possible polarizations, either a vertical or horizontal photon, representing a 0 or 1 in the *rectilinear* basis, or a photon polarized along one of the diagonal directions, representing a bit in the *diagonal* basis. Actually, in the experiment we used a third choice of basis: right and left circular polarizations, instead of the diagonal basis. When *Bob* (the receiver) receives the photon, he measures in one of the bases, and only then does Alice announce which basis she used. Half the time Bob uses the wrong basis, and they have to throw away that bit and do it again. When they are right, however, they have a bit that ought to agree. Anyone eavesdropping in the middle also would not know which basis to use and thus would be likely to disturb the photon. If Alice and Bob check their agreement on some of their photons, they can detect attempted eavesdropping.

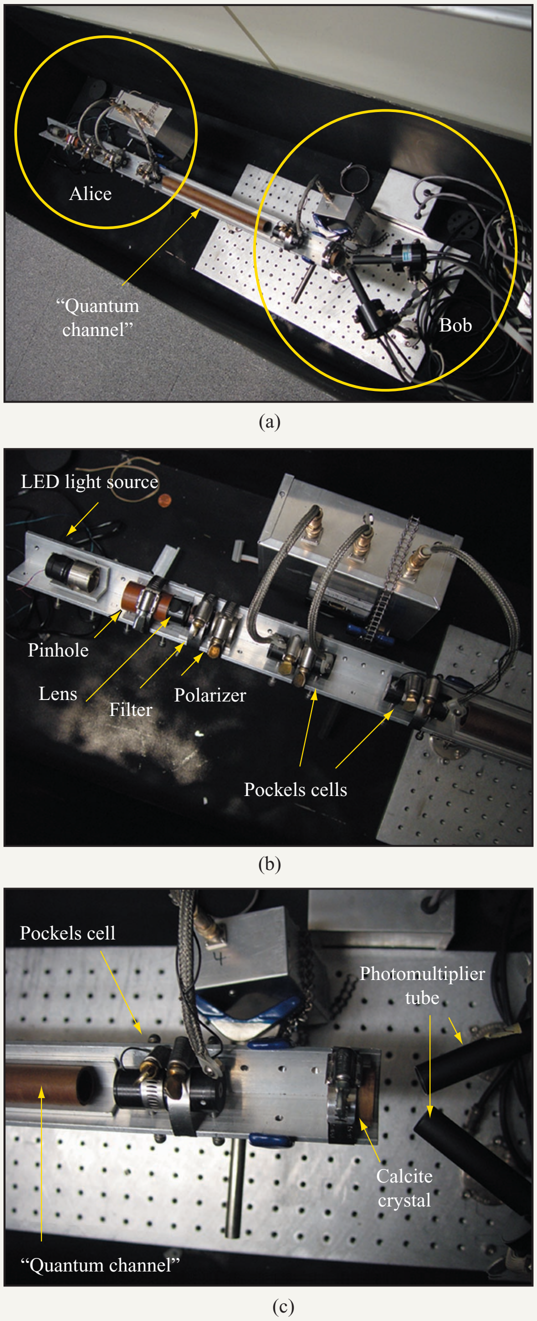
The apparatus

Our apparatus (**Figure 1**) consisted of a light-emitting diode (LED) that emits dim pulses, a lens and pinhole to collimate the beam, a 550-nm filter, a polarizing filter, and two Pockels cells (crystals that rotate the polarization of light as a function of applied voltage) for Alice, which allowed her to choose a basis and a bit. By the time the light pulses left Alice's section of the apparatus, they were attenuated to an expectation value of less than one photon per pulse. Next was the quantum channel (30 cm long) and then Bob, who got a Pockels cell and a calcite crystal. The crystal split orthogonal polarization states into two different beams, and the Pockels cell let him choose his basis. Finally, there were two photomultipliers able to detect single photons with a quantum efficiency of a few percent.

Neither Charlie nor I knew much about building anything, but we knew enough to be dangerous. As an example of Charlie's experimental agility, I remember a time I was visiting George in their apartment in Cambridge, Massachusetts. Charlie was excited about some fancy new tea he had gotten somewhere. He had set up a little double boiler using a pot and a teapot, explaining how this was the right way to cook the very delicate tea. George and I left the house for some time, returning hours later; when we came into the kitchen, we noticed the teapot. If you know about black-body radiation, you've probably seen how a black body turns

Note: This paper is based on a talk presented in May 2003 at a symposium at the IBM Thomas J. Watson Research Center in Yorktown Heights, New York, honoring Charles Bennett on the occasion of his sixtieth birthday.

0018-8646/04/$5.00 © 2004 IBM



(a)

(b)

(c)

Figure 1

The apparatus used to perform the first quantum cryptography experiment: (a) The entire apparatus; (b) detailed view of Alice; (c) detailed view of Bob.

invisible in a furnace, radiating the same spectrum as fills the cavity. The situation we found was not quite that, but there was a red teapot sitting in an empty pot on the stove. This would not have been disturbing, except for the fact that at room temperature the teapot had been green. I had forgotten this and wouldn't have known except that George pointed it out, and proved it by turning off the stove. The delicate tea had left nothing but a faint burnt aroma.

I can't resist a further aside about the time George, Charlie, and I attended an engine fair near Wendell, Massachusetts. There were many hobbyists with these antique gasoline engines with big flywheels. At a certain point in the flywheel's revolution, a bit of gas would get squirted into a piston, there would be a kind of cough, and the wheel would pick up enough speed to rotate another revolution. There were maybe a hundred such engines belching away, and all kinds of stalls selling parts and old tools. We bought a gas—or maybe kerosene—blowtorch to play with, an idea as bad as the teapot. We took it home, filled it with gas, and lit it. This resulted in a lovely flame for a time, but as the thing heated up, the solder bits mending the many holes in it started to melt, and we ended up with tongues of flames bursting out in all directions. There was no way to go near the thing and nothing much to do but let it run out of gas.

Anyway, that's the kind of experimental background Charlie and I were starting with. We also had no budget. The stockroom at the time was very good, and we could get all kinds of small parts more or less for free. Charlie had discovered the difference between capital and expense budgets. He said he could order nothing worth more than $300, but as much as he wanted under $300. I think there may have been a slight exception made for the photomultiplier tubes, but mainly we had to improvise. Charlie had come up with a poor-man's version of a laser table. He had some pieces of angle-iron (actually aluminum) with holes drilled for small set screws. This allowed for all six degrees of freedom that were possible with professional laser-table mounts, but they cost almost nothing. (They didn't work all that well, either.) **Figure 2** shows a Pockels cell in one of the mounts. To adjust it, the screws were turned, which moved the cell in a complicated function of the degrees of freedom you actually wanted to adjust. You also had the additional excitement of the apparatus moving substantially when you stopped touching the screw, because of the significant amount of lash in the threads. (For readers who know more about physics than screws, that could also be called *mechanical hysteresis*.)

The Pockels cells had to be centered on the beam path that we established using a HeNe laser. The cells worked well only when they were right on axis and had the correct orientation relative to each other and to the polarization of the beam. We were supposed to be able to see the alignment by putting crossed polarizers around the Pockels cell and looking through it. I think one was supposed to see an X, but I never could. Apparently my eyes were too good at focusing on the crystal itself, and I really should have looked somewhere else.

To keep the Pockels cells in place and avoid moving them during adjustments, we “naturally” used hose clamps. The problem with that was that when they were clamped down enough to keep them from moving on the screws, we couldn’t adjust them rotationally, which was the final step. They were smooth cylinders, and we couldn’t get a good grip on them. We solved this with hose clamps as well. We clamped them directly on the Pockels cells and they served as pretty good handles.

Pockels cells are crystals that rotate the polarization of light as a function of applied voltage. They require 1000–2000 volts. A simple circuit (**Figure 3**) controls each cell. I remember the look of terror on Charlie’s face when I built the first test circuit. Wire and solder were hanging out every which way; there was no way it was safe. I wasn’t very neat when making electronics, but I improved as we went along. A notable safety innovation that Charlie insisted on was the use of Zener diodes between the transistor–transistor logic (TTL) levels and the high voltage. These short to ground if the voltage goes above something like six volts. We even tested them with no explosions reported.

Figure 4 shows the control electronics for sending the pulses in a small time window and for receiving the signal from the photomultipliers. The ugly wiring is all on the back. In a manner of speaking, it is cheating for Alice and Bob to share this box, but not really. The only thing Alice gets from it is a light pulse that carries no information—and it’s not nearly as bad as the fact that Alice and Bob are actually in the same computer. The advantage experimentally in having Bob generate the pulse is that—since Bob is sending the pulse at a very precise time—he knows when to look for it to arrive. This time-windowing helps eliminate dark counts in the detectors. The various potentiometers set the width of the time window (when it starts relative to when the pulse is sent) and the voltage levels needed to discriminate a pulse from a non-pulse from a photomultiplier.

We had another amusing problem—getting the LED to emit enough light to get pulses with about a tenth of a photon per pulse. This was unexpected. The trouble was the pinhole, which caused us to waste most of the light. We had expected there to be plenty of light, even after the pinhole, so we weren’t too concerned with capturing all the light in the lens. This, combined with the very short pulse length we were using, made it difficult to pass enough light through the system. We had to add a transistor to push more current into the poor LED, which would definitely have fried if it had been given that much current for more than a couple of nanoseconds.

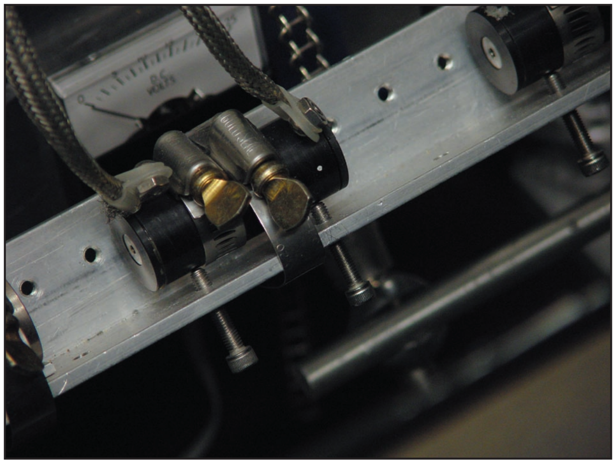


Figure 2

Pockels cell and set screws.

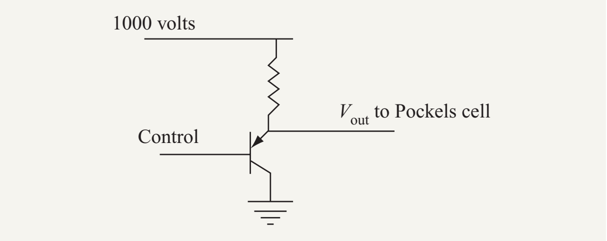


Figure 3

Circuit used to control the Pockels cells.

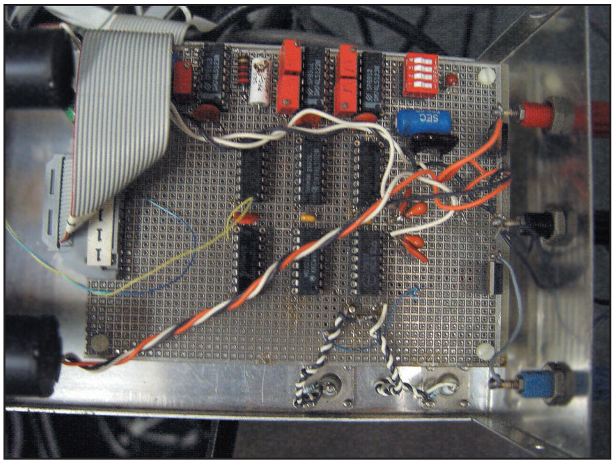


Figure 4

Electronics showing high-voltage transistors.

The apparatus had to be operated in complete darkness, so we had the machine shop build an aluminum box and we painted the inside of it flat black. The spray paint never really adhered well, and it gave off a bad odor. We worked on it in Charlie's office because we didn't have a lab, so it was always crowded and smelled like paint in there. I doubt this upset the safety people as much as the high-voltage power supply did. One day we drove to a hardware store and bought a 100 VAC switch so that we could at least turn off one of the supplies without climbing under the table to unplug it.

After Geoff Grinstein walked by and gave us his condolences when he saw the light-tight box, it became affectionately known as *Aunt Martha's coffin*. Charlie was always bugging me to get inside it and check to see if it was really light-tight. Actually, the box wasn't entirely light-tight—a fact that our photomultipliers helpfully detected. Probably light was leaking in through the rubber stoppers with holes cut in them for the wiring. To fix this, we bought some black velvet that we draped over the apparatus and the stoppers. That's partially why we had a physical tube as the quantum channel (the other reason being that it was funny), to keep the velvet from getting in the beam line. It was great fun going to the fabric store and, when asked what we needed it for, telling the salesperson it was for a quantum cryptography experiment. One day years later, when we wanted to go outside for lunch and Charlie was worried about getting too much sun, he wore the velvet as a hat.

The experiment

The whole experiment was controlled by a computer using a program written mostly in French by François Bessette and Louis Salvail, which didn't help me much trying to make it talk to our hardware. I more or less figured it out, and eventually Gilles Brassard came down from Montréal just when we were ready to get the thing working. By then, I didn't really need his help to translate the program, but it was useful having him around to hear me complain about it.

Here is a passage from Simon Singh's *The Codebook: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* [5], which captures the feeling of that day:

> However, the mounting skepticism eventually goaded Bennett into proving that the system could really work. In 1988 he began accumulating the components he would need for a quantum cryptographic system, and took on a research student, John Smolin, to help assemble the apparatus. After a year of effort they were ready to attempt to send the first message ever to be protected by quantum cryptography. Late one evening they retreated into their light-tight laboratory, a pitch-black environment safe from stray photons that might interfere with the experiment. Having eaten a hearty dinner, they were well prepared for a long night of tinkering with the apparatus. They set about the task of trying to send polarised photons across the room, and then measuring them using a +-detector and a x-detector. A computer called Alice ultimately controlled the transmission of photons, and a computer called Bob decided which detector should be used to measure each photon.

That's almost how it was. Unfortunately, he left out Gilles' presence. I remember Gilles brought the wine for dinner, and I was impressed that he had his own corkscrew with him ready to go. And the lab wasn't light-tight, just Aunt Martha's box. So you can't believe everything you read, but the mood was spot on.

Conclusion

In a sense, the quantum cryptography experiment was not really an experiment at all. We were not attempting to test quantum mechanics, and if one believes that quantum mechanics is correct, we had no reason to believe that the apparatus wouldn't do exactly what it did. It was really more of an engineering prototype. Nevertheless, our primitive experiment served an important function in bringing attention to the field. As a result of many more sophisticated experiments since then [6], quantum key distribution has come of age. A review of recent work may be found in [7], and two companies have started to offer actual systems.[1]

On a more theoretical or philosophical note, quantum cryptography keeps showing up in unexpected places, perhaps owing to its being based on something fundamental—the impossibility of reliably distinguishing non-orthogonal states. This observation led Chris Fuchs and Gilles Brassard to suggest, not entirely seriously, that perhaps quantum mechanics itself could be derived from the existence of secure key distribution together with the impossibility of bit commitment.[2] Jeffrey Bub took this quite seriously and, together with Rob Clifton and Hans Halvorson, showed that something like this can be done [8]. Their formulation takes as a given that the structure of the theory is a C* algebra. There have been some objections to this, and the issue is still open. I've been working on something I like to call *lockboxes*, which are an alternate physics that has key distribution, lacks bit commitment, and definitely cannot give you quantum mechanics.

[1] ID Quantique, *http://www.idquantique.com/*; MagiQ Technologies, *http://www.magiqtech.com/*.

[2] Brassard comments (in notes on this paper given to the author), "Hmmm . . . maybe not entirely, but still, this was serious enough to organize three international meetings over the past few years: two in Montréal and one in Sweden."

Briefly, a lockbox is a system containing a bit that cannot be read except when the box is presented with the correct *combination* bits. Some additional features have to be added to rule out bit commitment, essentially to permit whoever put the bit in the box to change it later. Such a physics is not going to give quantum mechanics, since it is explainable with a local hidden-variable theory. On the other hand, it isn't classical either. Classical mechanics differs from quantum mechanics not so much in being explainable by a local hidden-variable theory, but by being a local *unhidden*-variable theory. This is often overlooked, but makes classical physics what it is—a physics in which, in principle, you can find out everything about a system. It does seem doubtful that the lockbox physics forms a C* algebra and therefore can peacefully coexist with Clifton et al. [8], but it is unclear what that actually is telling us about quantum mechanics.

Appendix: A holiday greeting from an old friend

A few years ago, Charles H. Bennett's stepson, George Dyer, had the idea of making a website for Charlie as a kind of holiday card. People would contribute stories or scientific articles, whatever they wanted. He asked me to get Charlie's scientific colleagues involved. Somehow the idea never came fully to fruition, but there were several submissions. Below is what Rolf Landauer[3] wrote.

> December 18, 1997
>
> Charles Bennett and I first crossed paths at a statistical physics meeting in Chicago in 1971 when I realized that the number of people in the world interested in a disciplined way in the physics of computation had doubled. That was the start of a long, multi-dimensional and multi-valued relationship with Charles. I will not, here, retell my anecdotes about our early encounters and will save those stories for more formal ceremonial occasions. I will also, not here, repeat the appraisal of what Charles has done, contained in a good many of my archival papers. It suffices to say that I started more or less as his mentor. Eventually the relationship inverted, and he became the intellectual leader. Charles, once he moves on to the next subject, leaves the old topic behind totally. One of many examples relates to his contribution to a paper, "Kinematics of the Forced and Overdamped Sine–Gordon Soliton Gas," C. H. Bennett, M. Buettiker, R. Landauer, and H. Thomas, *J. Stat. Phys.* **24,** p. 419 (1981). Actually, this is one of only two papers where we ended up as formal coauthors. This was not Charles's topic; the rest of us had started this work. Charles supplied the central analytical insight which made the paper possible. He provided what I call *the ensemble member jumping trick*. I have always thought this was a tool of wide applicability, transcending this particular problem. But I could never get Charles to return to it and teach the world to appreciate that tool.
>
> Once Charles discovered quantum mechanical entanglement, in a similar way, his earlier concern with classical information handling simply disappeared. I was left to fight the rearguard skirmishes. A typical example: Thomas D. Schneider published a "Review Article" in *Nanotechnology* **5,** p. 1 (1994). Its title was "Sequence Logos, Machine/Channel Capacity, Maxwell's Demon, and Molecular Computers: A Review of the Theory of Molecular Machines." (That is the title, not the abstract.) I had earlier encounters with Schneider and was prepared for disagreement. But the violence done to my work was small compared to that done to Charles's work. Despite the emphasized relationship to Maxwell's demon, and despite Schneider's participation in PhysComp'92, where Bennett's resolution of Maxwell's demon came up repeatedly, Bennett is not even cited in the Schneider paper. Nevertheless, the paper had been given a distinguished status by the journal. I complained to the editor. Charles could not have cared less! And perhaps he was right: My complaints, despite a somewhat sympathetic reception, had no effect whatsoever! And it is, of course, this ability to discard old baggage completely, which gives Charles his effectiveness.
>
> —Rolf Landauer

References

1. C. H. Bennett, F. Bessett, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography," *J. Cryptol.* **5,** No. 1, 3–28 (1992).
2. C. H. Bennett and G. Brassard, "The Dawn of a New Era for Quantum Cryptography: The Experimental Prototype Is Working!," *Sigact News* **20,** No. 4, 78–82 (Fall 1989).
3. C. H. Bennett and G. Brassard, "Quantum Cryptography: Public-Key Distribution and Coin Tossing," *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, 1984, pp. 175–179.
4. C. H. Bennett, G. Brassard, and A. Ekert, "Quantum Cryptography," *Sci. Amer*., pp. 50–57 (October 1992).
5. S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor Books, New York, 2000; ISBN: 0385495323.
6. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," *Rev. Mod. Phys.* **74,** 145–195 (March 2002).
7. A. Galindo and M. A. Martin-Delgado, "Information and Computation: Classical and Quantum Aspects," *Rev. Mod. Phys.* **74,** 347–423 (March 2002).

[3] Rolf Landauer (1927–1999) was an IBM Fellow and a member of the IBM Research Division, Thomas J. Watson Research Center, Yorktown Heights, New York. In 1995, he received the Oliver E. Buckley Condensed Matter Physics Prize from the American Physical Society. As noted in the preface of the issue in which this paper appears, we are very grateful to his family for permission to include this previously unpublished tribute to Charles H. Bennett.

8. R. Clifton, J. Bub, and H. Halvorson, "Characterizing Quantum Theory in Terms of Information-Theoretic Constraints"; see *http://arxiv.org/abs/quant-ph/0211089/*.

Received June 17, 2003; accepted for publication August 28, 2003

John A. Smolin *IBM Research Division, Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598 (smolin@us.ibm.com).* Dr. Smolin received his B.S. degree in physics from the Massachusetts Institute of Technology in 1989, and his Ph.D., also in physics, from the University of California at Los Angeles in 1996. He has been at the IBM Research Division since receiving his doctorate. He worked with Charles H. Bennett building the first quantum cryptography apparatus at IBM in 1989. Dr. Smolin's current research interests are in quantum information theory and quantum computation, with occasional forays into the foundations of quantum mechanics.