The Security of Quantum Bit Commitment Schemes

Gilles Brassard [*]
Université de Montréal [†]

Claude Crépeau [‡]
McGill University [§]

Dominic Mayers
Princeton University [¶]

Louis Salvail [‖]
Aarhus Universitet [**]

Abstract

Can quantum mechanics be harnessed to provide unconditionally secure bit commitment schemes and other cryptographic primitives beyond key distribution? We review the general impossibility proof of Mayers and illustrate it by showing how to break some recent attempts to bypass it. In particular, secure schemes would follow if we could force participants to perform measurements at specified points in the execution of the protocol. It has been suggested to use short-lived classical bit commitment schemes for this purpose. Alas, this strategy was doomed as measurements can always be postponed in an undetectable way until cheating becomes possible.

It is well known that quantum mechanics can be used to allow two people to establish confidential communication under the nose of an eavesdropper equipped with unlimited computing power [1, 3, 4]. Can quantum mechanics be useful for the implementation of other cryptographic tasks? One of the most important primitives in classical cryptography is the *bit commitment scheme*, which allows one party, Alice, to give something to another party, Bob, in a way that commits her to a bit b of her choice so that Bob cannot tell what b is, but Alice can later prove to him what b originally was. You may think of this as Alice sending to Bob a locked safe that contains the value of b written on a slip of paper; later, she can send him the key that opens the safe if she wants him to know to which bit she had committed.

A commitment scheme is *binding* if Alice cannot change the value of b and it is *concealing* if Bob cannot obtain any information about b without the help of Alice. It is *secure* if it is simultaneously binding and concealing, and it is *unconditionally* secure if it is secure against a cheater, either Alice or Bob, equipped with unlimited technology and computational power. It has long been known that unconditionally secure bit commitment schemes cannot exist in

[*] Supported in part by Canada's NSERC, Québec's FCAR and the Canada Council.

[†] Département IRO, Université de Montréal, C.P. 6128, succursale centre-ville, Montréal (Québec), Canada H3C 3J7. e-mail: brassard@iro.umontreal.ca.

[‡] Supported in part by Canada's NSERC and Québec's FCAR.

[§] School of Computer Science, McGill University, Pavillon McConnell, 3480 rue University, Montréal (Québec), Canada H3A 2A7. e-mail: crepeau@cs.mcgill.ca.

[¶] Department of Computer Science, Princeton University, Princeton, NJ 08544–2087, USA. e-mail: mayers@cs.princeton.edu.

[‖] Supported in part by the Danish National Research Foundation under the Basic Research in Computer Science (BRICS) programme.

[**] Department of Computer Science, University of Aarhus, Ny Munkegade, building 540, DK–8000 Århus C, Denmark. e-mail: salvail@daimi.aau.dk.

the classical world. After the success of quantum key distribution, it was natural to hope that quantum mechanics might provide such an unconditionally secure scheme. A protocol for quantum bit commitment, henceforth referred to as BCJL, was proposed in 1993 and claimed to be provably secure [5], which would also have allowed secure quantum oblivious transfer [2], another fundamental primitive in classical cryptography. Because of this, the future of quantum cryptography looked very bright indeed, with new applications such as the identification protocol of Crépeau and Salvail [8], coming up regularly.

Trouble began in October 1995 when Mayers found a subtle flaw in the BCJL protocol. The proof that Bob cannot cheat BCJL and learn information on the committed bit was correct, and so was the proof that it is not possible for Alice to simultaneously know how to open the commitment to show a 0 and how to open it to show a 1. However, it was possible for Alice, through the magic of quantum entanglement, to learn at her choice *either* how to open the commitment to show a 0 *or* how to open it to show a 1. Because of the destructive nature of quantum measurements, choosing either one of these alternatives destroyed her chances for learning how to open the commitment the other way, a situation that has no classical analogue. It is as if Alice could provide Bob with one of two possible quantum keys to open the safe, whose effect would be to make the desired bit appear surreptitiously on the slip of paper in an irreversible manner.

Though Mayers explained his discovery to several researchers interested in quantum information processing [10], his result was not made public until after Lo and Chau discovered independently a similar technique [9]. This prompted several attempts at fixing the protocol, but every time *ad hoc* successful attacks soon followed. This cat-and-mouse game went on until Mayers proved that all these attempts had been in vain: unconditionally secure quantum bit commitment schemes are impossible [11]. Despite all odds, various kinds of ideas continued to be proposed by some of us as well as others in the hope they would not fall prey to Mayers' result [4, 7]. Perhaps the most interesting approach consisted in using various types of short-lived *classical* bit commitment schemes to force the cheater to perform measurements at specified points in the execution of the protocol, which indeed would fix the problem. Alas, this strategy was doomed as measurements can always be postponed until cheating becomes possible. This is not surprising in retrospect because it has since been realized that these apparently promising ideas were also ruled out by Mayers' general impossibility theorem. Nevertheless, these attempts contributed to enhance our understanding of what is going on with quantum bit commitment schemes and other quantum cryptographic protocols.

Assume for example that you are given an unknown quantum bit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and you are expected to measure it either in the computational basis, $|0\rangle$ versus $|1\rangle$, or the diagonal basis, $(|0\rangle + |1\rangle)/\sqrt{2}$ versus $(|0\rangle - |1\rangle)/\sqrt{2}$. You could cheat the protocol if only you could postpone the choice of basis (and therefore the measurement) until after subsequent classical information becomes available. To prevent this, you are asked to use a classical (perhaps multiparty) commitment scheme to commit to your choice of basis (computational or diagonal) as well as to the result of your measurement. Then, either you are immediately challenged to open those commitments to "prove" that you had measured, in which case this quantum bit is not used any further, or you are allowed to keep secret your choice of basis and measurement result for later use. The hope was that this approach could turn a classical bit commitment scheme that is reasonably secure for a very short time into a quantum bit commitment scheme that is permanently secure. Unfortunately, it turns out that you can always postpone measuring the quantum bit and offer fake commitments even if you are unable to break the underlying commitment scheme in the time that elapses between the commitment and the challenge: if a challenge comes, you can open your "commitments" in a way consistent with what you would have committed to had you measured the quantum bit, and if the challenge does not come, you can keep the quantum bit intact for later measurement in the basis of your choice.

For a detailed description of these flawed quantum bit commitment schemes and how to break them, the reader is encouraged to consult a preliminary version of the full paper, currently available on the Los Alamos National Laboratory e-Print quantum physics archive [6].

References

[1] Bennett, Charles H., François Bessette, Gilles Brassard, Louis Salvail and John Smolin, "Experimental quantum cryptography", *Journal of Cryptology*, Vol. 5, no. 1, 1992, pp. 3 – 28.

[2] Bennett, Charles H., Gilles Brassard, Claude Crépeau and Marie–Hélène Skubiszewska, "Practical quantum oblivious transfer", *Advances in Cryptology: Proceedings of Crypto '91*, August 1991, pp. 351 – 366.

[3] Bennett, Charles H., Gilles Brassard and Artur K. Ekert, "Quantum cryptography", *Scientific American*, October 1992, pp. 50 – 57.

[4] Brassard, Gilles and Claude Crépeau, "Cryptology column — 25 years of quantum cryptography", *Sigact News*, Vol. 27, no. 3, 1996, pp. 13 – 24.

[5] Brassard, Gilles, Claude Crépeau, Richard Jozsa and Daniel Langlois, "A quantum bit commitment scheme provably unbreakable by both parties", *Proceedings of 34th Annual IEEE Symposium on Foundations of Computer Science*, November 1993, pp. 362 – 371.

[6] Brassard, Gilles, Claude Crépeau, Dominic Mayers and Louis Salvail, "Defeating classical bit commitments with a quantum computer", available as `quant-ph/9806031` in the LANL e-Print archive at URL `http://xxx.lanl.gov/archive/quant-ph`, June 1998.

[7] Crépeau, Claude, "What is going on with quantum bit commitment?", *Proceedings of Pragocrypt '96*, Prague, October 1996, Czech Technical University Publishing House, pp. 193 – 203.

[8] Crépeau, Claude and Louis Salvail, "Quantum oblivious mutual identification", *Advances in Cryptology: Proceedings of Eurocrypt '95*, May 1995, pp. 133 – 146.

[9] Lo, Hoi–Kwong and H. F. Chau, "Is quantum bit commitment really possible?", *Physical Review Letters*, Vol. 78, no. 17, 28 April 1997, pp. 3410 – 3413; first appeared as `quant-ph/9603004` in the LANL e-Print archive (see [6]), March 1996.

[10] Mayers, Dominic, "The trouble with quantum bit commitment", available as `quant-ph/9603015` in the LANL e-Print archive (see [6]); first discussed at a Workshop on Quantum Information Theory held in Montréal, October 1995.

[11] Mayers, Dominic, "Unconditionally secure quantum bit commitment is impossible", *Physical Review Letters*, Vol. 78, no. 17, 28 April 1997, pp. 3414 – 3417.