Unconditionally Secure Bit Commitment by Transmitting Measurement Outcomes

Adrian Kent

*Centre for Quantum Information and Foundations, DAMTP, Centre for Mathematical Sciences, University of Cambridge,
Wilberforce Road, Cambridge, CB3 0WA, United Kingdom*
Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario, N2L 2Y5, Canada

We propose a new unconditionally secure bit commitment scheme based on Minkowski causality and
the properties of quantum information. The receiving party sends a number of randomly chosen Bennett-
Brassard 1984 (BB84) qubits to the committer at a given point in space-time. The committer carries out
measurements in one of the two BB84 bases, depending on the committed bit value, and transmits the
outcomes securely at (or near) light speed in opposite directions to remote agents. These agents unveil the
bit by returning the outcomes to adjacent agents of the receiver. The protocol's security relies only on
simple properties of quantum information and the impossibility of superluminal signalling.

Introduction.—Much research on physics and cryptography has been devoted to the problem of bit commitment, a basic cryptographic task which also has many applications (e.g., Ref. [1]). In a bit commitment protocol, the committer, Alice, carries out actions that commit her to a particular bit value (or, in the quantum case, a particular weighted superposition of bit values). She can later (or, in the relativistic case, at one or more points in the causal future of the commitment), if she chooses, give the receiver, Bob, classical or quantum information that unveils the committed bit. Ideally, Bob should have an absolute guarantee that Alice is committed by her initial actions, and Alice should have an absolute guarantee that Bob can learn no information about the committed bit before she unveils.

Besides its intrinsic cryptographic importance and its use in applications, bit commitment also has intriguingly deep connections to fundamental physics. Initially, work in this area focussed entirely on bit commitment protocols based on nonrelativistic quantum mechanics. Bennett and Brassard invented the first quantum bit commitment protocol [2] and showed that it is secure against both parties given current technology, but insecure if Alice has a quantum memory. Later attempts at unconditionally secure nonrelativistic protocols (e.g., Ref. [3]) were ultimately shown to be futile by the celebrated results of Mayers [4,5], and Lo and Chau [6,7], later further extended [8,9], showing that no unconditionally secure nonrelativistic quantum bit commitment protocol exists.

However, the world is relativistic, and in particular to a good approximation space-time in Earth's local neighborhood is Minkowski. Allowing relativistic protocols, which exploit the signalling constraints implied by Minkowski causality, radically changes the picture. It was shown some time ago that classical relativistic protocols can evade the Mayers and Lo-Chau no-go theorems [10,11]. These schemes are provably secure against all classical attacks and against Mayers and Lo-Chau's quantum attacks, and are conjectured to be unconditionally secure, provided that quantum theory is correct and the background space-time is approximately Minkowski. Since small corrections due to general relativity can be allowed for, and the possibility of an adversary surreptitiously making major changes to the local space-time geometry is beyond any presently foreseeable science and technology, such security appears robust for the foreseeable future.

Recently, a new quantum cryptographic idea was introduced [12] and applied to bit commitment [13]. The idea is that the committer is required to send a quantum state, supplied by and known to the receiver but unknown to the committer, at light speed over secure quantum channels in one of two or more directions. This gives a practical bit commitment scheme which is also easily shown to be unconditionally secure against general attacks [13]. It relies essentially on the control over physical information that special relativity and quantum theory together allow—specifically, on the no-summoning theorem [12], which also has other cryptographic applications [14].

Here we propose another new quantum relativistic bit commitment protocol. It uses some similar intuitions to that of Ref. [13], in that the committer is forced by Minkowski causality to choose a particular commitment at the space-time point where the protocol starts. However, it relies on a different physical principle—essentially, on the impossibility of completing a nonlocal measurement on a distributed state outside the joint future light cone of its components. Its implementation requires minimal quantum resources: the receiver needs to send quantum states (which can be unentangled qubits) to the committer, who needs to carry out individual measurements on them as soon as they are received. No further quantum communication is required by either party; nor do they require any entanglement, collective measurements, or quantum state storage.

As usual in quantum cryptography, we present the protocol in an idealized form assuming perfect state preparations, transmissions, and measurements. This poses no significant issue of principle here. For the Bennett-Brassard 1984 (BB84) scheme described below, if Alice is sent 2N qubits, the expected numbers $E(N_0)$ and $E(N_1)$ of states on which she correctly reports outcomes consistent with 0 and 1 commitments respectively obey $E(N_0) + E(N_1) \leq (1 + \frac{1}{\sqrt{2}})N$ for any strategy, in the error-free case [15–17]. It can be shown that, for sufficiently large N, the protocol can tolerate a total error rate up to $\frac{1}{2} - \frac{1}{2\sqrt{2}} \approx 14\%$. The protocol can also tolerate losses, so long as Alice can identify and communicate to Bob at (or in the nonideal case near) P which qubits she successfully measured.

We also make idealizations about the relativistic geometry and signalling speed, supposing that Alice and Bob each have agents in secure laboratories infinitesimally separated from the points P, Q_0, and Q_1, Alice can signal at precisely light speed, and all information processing is instantaneous. These, too, pose no problem of principle. Like other protocols of this type [12,13], the protocol remains secure in realistic implementations with finite separations and near light speed communication. If these corrections are small, the only significant effect is that Bob is guaranteed that Alice's commitment is binding from some point P' in the near causal future of P, rather than from P itself [13].

Bit commitment based on transmitting quantum measurement outcomes.—We give a simple version of the scheme using qubit states and measurements in the standard BB84 basis [2]. The scheme obviously generalizes to other sets of qubit states and measurements, to qudits, and to variants with more or differently located unveiling points.

Alice and Bob agree on a space-time point P, a set of coordinates (x, y, z, t) for Minkowski space, with P as the origin, and (in the simplest case) two points $Q_0 = (x, 0, 0, x)$ and $Q_1 = (-x, 0, 0, x)$ lightlike separated from P. They each have agents, separated in secure laboratories, adjacent to each of the points P, Q_0, Q_1. To simplify for the moment, we take the distances from the labs to the relevant points as negligible.

Bob securely preprepares a set of qubits $|\psi_i\rangle_{i=1}^N$ independently randomly chosen from the BB84 states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ [where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$] and sends them to Alice to arrive (essentially) at P. To commit to the bit value 0, Alice measures each state in the $\{|0\rangle, |1\rangle\}$ basis, and sends the outcomes over secure classical channels to her agents at Q_0 and Q_1. To commit to 1, Alice measures each state in the $\{|+\rangle, |-\rangle\}$ basis, and sends the outcomes as above. Alice's secure classical channels could, for example, be created by presharing one-time pads between her agent at P and those at Q_0 and Q_1 and sending pad-encrypted classical signals. If necessary or desired, these pads could be periodically replenished by quantum key distribution links between the relevant agents.

To unveil her committed bit, Alice's agents at Q_0 and Q_1 reveal the measurement outcomes to Bob's agents there. After comparing the revealed data to check that the declared outcomes on both wings are the same (somewhere in the intersection of the future light cones of Q_0 and Q_1), and that both are consistent with the list of states sent at P, Bob accepts the commitment and unveiling as genuine. If the declared outcomes are different, Bob has detected Alice cheating (see Fig. 1).

Security.—The protocol is evidently secure against Bob, who learns nothing about Alice's actions until (if) she chooses to unveil the bit.

Alice is constrained in that she has to be able to reveal her commitment data at both Q_0 and Q_1, since Bob's agents at these points verify the timing and location of the unveilings, and then later compare the data to check they are consistent. By Minkowski causality, Alice's ability to unveil data consistent with a 0 or 1 commitment at Q_0 depends only on operations she carries out on the line PQ_0. Suppose that she has a strategy in which she carries out some operations at P, but these leave her significantly uncommitted, in the sense that her optimal strategies S_i for successfully unveiling the bit values i, by carrying out suitable operations in the causal future of P, have success probabilities p_i, with $p_0 + p_1 > 1 + \delta$, for some $\delta > 0$. By Minkowksi causality, any operations she carries out on the half-open line segment $(P, Q_0]$ cannot affect the
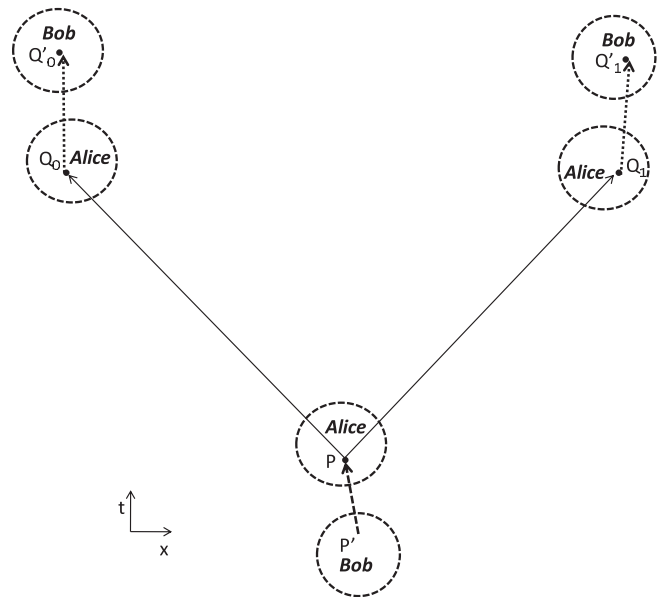

FIG. 1. A nonideal implementation of the protocol in $1 + 1$ dimensions. (Not to scale.) Alice and Bob control disjoint regions of space-time, representing their respective secure laboratories. Bob generates random BB84 quantum states at P' and sends them (dashed arrow) to Alice at point P, where she measures them in her chosen basis. She reports the results (solid arrows) via secure classical (near) light-speed channels to her agents at the points Q_i, who relay them (dotted arrows) to Bob's agents at the nearby points Q_i'.

probability of producing data at Q_1 consistent with a successful unveiling of either bit value i there. In particular, if she follows the instructions of strategy S_0 on $(P, Q_0]$, and the instructions of strategy S_1 on $(P, Q_1]$, she has probabilities p_i of producing data consistent with a successful unveiling of bit value i at Q_i, and, hence, a probability at least δ of producing data consistent with a successful unveiling of bit value 0 at Q_0 and with a successful unveiling of bit value 1 at Q_1.

This means that, with probability of at least δ, by combining her data at Q_0 and Q_1 at some point in their joint causal future, Alice can produce data consistent with both sets of measurements in complementary bases. Thus, for example, for each state $|\psi_i\rangle$, she can identify a subset of 2 states from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, one from each basis, which must include $|\psi_i\rangle$. By choosing the security parameter N large enough, Bob can ensure Alice's overall success probability, for correctly identifying such a subset for each of the N states, is smaller than δ, for any given $\delta > 0$, i.e., that Alice has no cheating strategy of the type described. Hence the protocol is also secure against Alice.

Discussion.—We now have a variety of practical schemes for bit commitment—the one described above and those of Refs. [11,13]—including two distinct intrinsically quantum and practical schemes with complete security proofs, solving a problem once thought unsolvable. The interesting open questions now seem to be understanding the full variety of techniques and schemes, comparing the resources they require, and identifying the most practical in any given context.

The protocol given here has some significant practical advantages. Unlike the protocol of Ref. [11], it does not require Alice to preshare data and coordinate her commitment timings in advance between agents at spacelike separated points. Compared to the protocol of Ref. [13], it requires significantly less advanced quantum technology: it needs reasonably reliable preparation (by Bob) and measurement (by Alice) of single qubits, but no entanglement, no collective measurements, and no secure quantum communication channels for either party. Note also that the protocol remains secure even if Alice has a low detection efficiency for the transmitted qubits, so long as (i) she can carry out reasonably reliable measurements on those she does detect, and (ii) she can report quickly back to Bob (i.e., at or close to P) which qubits were detected and measured.

Of course, Bob needs to be able to generate randomly chosen quantum states securely in his lab, but once they are generated it does not matter significantly if Alice is able to carry out quantum operations on them immediately: the only effect is to slightly alter the space-time region in which Bob is confident Alice is committed. Alice also requires secure classical communication channels: these could be implemented using sufficiently long preshared one time pads, or by shorter preshared pads expanded indefinitely using quantum key distribution.

As noted above, in a realistic implementation, Alice and Bob's agents would have nonzero separation from the space coordinate of P, and likewise from Q_0 and Q_1. This affects the discussion only in that the causal geometry is a little more complex [13]. For example, Bob cannot guarantee that Alice was committed at any point in the interior of the intersections of the past light cones of the points Q_0^B and Q_1^B where he actually receives her unveiling data.

Like the protocol of Ref. [13], our protocol is immune to a Mayers-Lo-Chau attack [4,6], and for similar reasons. Mayers-Lo-Chau's arguments correctly imply that there is a unitary operation on a spacelike hyperplane through Q_0 and Q_1 that, mathematically, maps quantum data consistent with a 0 commitment and unveiling to data consistent with a 1, and vice versa. However, this operation cannot be implemented physically on the hyperplane: doing so would violate Minkowski causality.

A realistic implementation must also allow for errors in Bob's preparations, the communication of the states to Alice, and Alice's measurements. So long as these errors are small, this makes no essential difference: Bob needs only to test that Alice's declared outcomes are statistically consistent with the measurements corresponding to one bit value commitment, and statistically inconsistent with the other.

Note that, like all technologically unconstrained quantum bit commitment protocols [18,19], the protocol here does not prevent Alice from committing to a quantum superposition of bits. She can simply input a superposition $\alpha|0\rangle + \beta|1\rangle$ into a quantum computer programmed to implement the two relevant quantum measurement interactions for inputs $|0\rangle$ and $|1\rangle$ and to send two copies of the quantum outcome data towards Q_0 and Q_1, and keep all the data at the quantum level until (if) she chooses to unveil. This gives her no advantage in stand-alone applications of bit commitment, for example for making a secret prediction: it does, however, mean that one cannot assume that in a task involving bit commitment subprotocols, any unopened bit commitments necessarily had definite classical bit values, even if all unveiled bit commitments produced valid classical unveilings.

As with the protocols of Refs. [11,13], the present protocols can be chained together in sequence, allowing longer term bit commitments and flexibility in the relation between the commitment and unveiling sites (in particular, they need not be lightlike separated). Full security and efficiency analyses for these chained protocols remain tasks for future work.

Relativistic quantum cryptography allows strategies that make no sense in nonrelativistic classical or quantum cryptography. For example, one intriguing and rather Zen-like feature that the present protocol shares with that of Ref. [13] is that Alice makes her commitment without giving any information, classical or quantum, to Bob. This departs from the usual way of thinking about bit commitment, in

which Alice commits herself by handing over data that is in some way encrypted, and unveils by handing over some form of decryption key. Instead, here, relativistic causality forces Alice to commit herself so that she can later make a valid unveiling. She could delay her measurement choice, but if she does she cannot get valid measurement outcomes to both unveiling points. In a sense, Bob receives the commitment and unveiling together, and the unveiling carries with it a guaranteed record of the past commitment.

More broadly, our picture of relativistic quantum cryptography is changing quite fast, from a field with some interesting niche applications [11,20,21] to a distinct branch of physics-based cryptography with a potentially very wide range of applications. These include interesting cryptographic tasks whose definition itself is intrinsically relativistic [14]. They also include unconditionally secure schemes for quantum tagging [22] (also called quantum position authentication), conditionally secure quantum tagging schemes [23–26] based on slightly weaker security assumptions, and more generally, a large class of schemes for more general tasks in position-based quantum cryptography [25]. We hope all these developments will stimulate further interest in the theory and practical implementation of relativistic quantum protocols.

[1] A. Broadbent and A. Tapp, arXiv:0806.1931.

[2] C. H. Bennett and G. Brassard, in *Proceedings of the International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[3] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois, in *Proceedings of the 34th Annual IEEE Symposium on the Foundation of Computer Science* (IEEE Comp. Soc., Los Alamitos, California, 1993), pp. 362–371.

[4] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).

[5] D. Mayers, in *Proceedings of the Fourth Workshop on Physics and Computation* (New England Complex System Inst., Boston, 1996), p. 226.

[6] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).

[7] H.-K. Lo and H. Chau, in *Proceedings of the Fourth Workshop on Physics and Computation* (New England Complex System Inst., Boston, 1996), p. 76.

[8] A. Kitaev, D. Mayers, and J. Preskill, Phys. Rev. A **69**, 052326 (2004).

[9] G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner, Phys. Rev. A **76**, 032328 (2007).

[10] A. Kent, Phys. Rev. Lett. **83**, 1447 (1999).

[11] A. Kent, J. Cryptol. **18**, 313 (2005).

[12] A. Kent, Quantum Inf. Process. (2012).

[13] A. Kent, New J. Phys. **13**, 113015 (2011).

[14] A. Kent, Phys. Rev. A **84**, 012328 (2011).

[15] A. Holevo, J. Multivariate Anal. **3**, 337 (1973).

[16] H. P. Yuen, R. S. Kennedy, and M. Lax, IEEE Trans. Inf. Theory **IT-21**, 125 (1975).

[17] S. Barnett and S. Croke, J. Phys. A **42**, 062001 (2009); S. Croke (private communication).

[18] A. Kent, Phys. Rev. A **61**, 042301 (2000).

[19] A. Kent, Quantum Inf. Process. **11**, 493 (2011).

[20] R. Colbeck and A. Kent, Phys. Rev. A **73**, 032320 (2006).

[21] E. Jeffrey, J. Altepeter, and P. Kwiat, Relativistic Quantum Cryptography, privately circulated manuscript (2011).

[22] A. Kent, Phys. Rev. A **84**, 022335 (2011).

[23] A. Kent, R. Beausoleil, W. Munro, and T. Spiller, U.S. Patent No. US20067075438 2006.

[24] R. A. Malaney, Phys. Rev. A **81**, 042319 (2010); Phys. Rev. A **81**, 042319 (2010).

[25] H. Buhrman *et al.*, arXiv:1009.2490v4.

[26] A. Kent, W. J. Munro, and T. P. Spiller, Phys. Rev. A **84**, 012326 (2011).