# Coin Tossing is Strictly Weaker than Bit Commitment

Adrian Kent*
*Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Silver Street, Cambridge CB3 9EW, United Kingdom*
(Received 13 July 1998; revised manuscript received 14 October 1999)

We define cryptographic assumptions applicable to two mistrustful parties who each control two or more separate secure sites between which special relativity ensures a time lapse in communication. We show that, under these assumptions, unconditionally secure coin tossing can be carried out by exchanges of classical information. We then show that, under standard cryptographic assumptions, coin tossing is strictly weaker than bit commitment. That is, no unconditionally secure bit commitment protocol can be built from a finite number of invocations of a secure coin-tossing black box together with finitely many additional classical or quantum information exchanges.

PACS numbers: 03.67.Dd, 89.70.+c

The problem of remote coin tossing was introduced into the cryptographic literature in a classic 1981 paper by Blum [1]. A coin-tossing protocol involves two mistrustful separated parties who wish to use an information channel—e.g., a phone line—to generate a bit in whose randomness both are confident.

Coin tossing is a simple cryptographic primitive with many applications in more complicated tasks. To give a well known example, it can be used to authenticate a remote user, say to their bank, as follows. The user's $N$ digit passkey is known to both user and bank. Whenever the user logs in, a series of coin tosses between the user and bank are used to generate a random $n$ digit substring of the $N$ digits, where $n$ is significantly smaller than $N$. The user is then required to reveal only those $n$ digits of the passkey, and is accepted if they agree with the bank's records. This has the virtue that neither an eavesdropper nor someone impersonating the bank can obtain very much of the passkey during a small number of logins; in particular, neither has much chance of subsequently successfully convincing the bank that he is the user. By changing the passkey at appropriate intervals, security can thus be maintained.

Coin tossing also raises interesting theoretical questions, in that its relation to other primitives has not so far been resolved.

Bit commitment is another well known cryptographic primitive of great theoretical and practical interest, also involving two mistrustful parties. In a bit commitment protocol, one party, Alice, supplies an encoded bit to another, Bob. Alice tries to ensure that Bob cannot decode the bit until she reveals further information, while convincing Bob that she was genuinely committed all along. That is, Bob must be convinced that the protocol does not allow two different decodings of the bit which leave Alice free to reveal either 0 or 1, as she wishes.

It is well known that secure coin tossing can easily be implemented given a secure bit commitment protocol (see, e.g., Ref. [2]). Alice commits a random bit to Bob, who makes a random guess at it. Alice then unveils the bit, and the parties generate (say) a 0 if Bob's guess was correct, and a 1 otherwise.

This raises the question of whether the reverse is possible. As is by now well understood, quantum information has very different properties from classical information. In particular, some important cryptographic tasks can be implemented securely using quantum information, but not using classical information [3,4]. Thus, the question of the relation of coin tossing and bit commitment subdivides into at least two independently interesting questions: whether secure bit commitment can be built on top of secure coin tossing using (i) classical or (ii) quantum information exchanges. Both questions appear to have remained open to date (see, e.g., Ref. [5]).

There are many forms of security, of which the strongest and most interesting is *unconditional security*: an unconditionally secure protocol relies only on the known laws of physics to ensure that the probability of successful cheating by either party can be made arbitrarily small. Under standard nonrelativistic cryptographic assumptions, unconditionally secure quantum bit commitment is impossible [5–9]. We follow general usage in referring to this result as the Mayers-Lo-Chau no-go theorem or MLC theorem.

Unconditionally secure ideal coin tossing—that is, coin tossing with probabilities precisely one-half—has also been shown to be impossible by Lo and Chau [9]. However, it is not known whether nonideal coin tossing, in which the probabilities are bounded by $(\frac{1}{2} \pm \epsilon)$, and $\epsilon$ can be made arbitrarily small, can be implemented with unconditional security in quantum theory. Clearly, if it can be shown that quantum bit commitment can be built on top of coin tossing, then unconditionally secure quantum coin tossing must be impossible. Conversely, if it can be shown that quantum bit commitment cannot be built on top of coin tossing, we have no conclusive argument showing that an unconditionally secure quantum coin tossing protocol cannot be found. Such a protocol would be very useful.

 0031-9007/99/83(25)/5382(3)$15.00 

The main result of this paper resolves the relation between the two protocols by showing that secure bit commitment cannot be built on top of secure coin tossing in any finite classical or quantum protocol. Though this result applies to standard nonrelativistic cryptography, its proof is inspired by considering cryptography in the context of relativity.

The standard nonrelativistic cryptographic scenario for two mistrustful parties is as follows. $A$ and $B$ each control a laboratory, which includes sending and receiving equipment, measuring devices and classical and perhaps quantum computers. The laboratories are separated and generally assumed to be small. $A$ and $B$ have faith in the integrity of their own equipment but trust nothing whatsoever outside their laboratories. In particular, neither of them has any way of ensuring that a message sent by the other was sent a certain time before receipt, and so an effectively simultaneous exchange of messages cannot be arranged. A standard cryptographic protocol thus prescribes a sequential exchange of messages between $A$ and $B$, in which message $i + 1$ is not sent until the sender has received message $i$.

We will also need to consider an alternative cryptographic scenario in which special relativity plays a role. Alice and Bob agree on a frame and global coordinates, and on the location of two sites $\underline{x}_1$, $\underline{x}_2$ whose neighborhoods Bob may control at all times. Alice is not allowed within a distance $\epsilon$ of either point at any time. Alice is, however, required to erect laboratories within a distance $\delta$ of the sites, where $\Delta x = |\underline{x}_1 - \underline{x}_2| \gg \delta > \epsilon$. The precise location of Alice's laboratories need not be disclosed to Bob: he need only test that signals sent out from either of his laboratories receive a response within time $2\delta$. Bob could, for example, build laboratories of radius $\epsilon$ around each of the $\underline{x}_i$, but the precise location of his laboratories need not be known to Alice. She need only test that any signal broadcast from one of her laboratories receives a reply within time $2\delta$, whenever, her laboratory is in the prescribed region. Let the laboratories near $\underline{x}_i$ be $A_i$ and $B_i$, for $i = 1$ or 2. We assume that the $A_i$ collaborate with complete mutual trust and with prearranged agreement, and identify them together simply as Alice; similarly the $B_i$ are identified as Bob. From the point of view of cryptographic analysis, any protocol in this scenario may be considered as a two-party cryptographic protocol. The only unusual cryptographic feature is that the parties each occupy disconnected laboratories, and even this is inessential: $A$ and $B$ could equally well occupy laboratories that are connected, long, thin, and adjacent on their longer side. The crucial difference from standard analyses is that the relativistic signalling constraints which this situation imposes are taken into account.

There is a very simple unconditionally secure classical protocol for ideal coin tossing under these circumstances. At a prearranged time $t$, $A_1$ generates a random bit and sends it to $B_1$; at the same time, $B_2$ generates a random bit and sends it to $A_2$. More precisely, since the time of sending cannot be checked directly, the bits are sent at or after time $t$, and so as to arrive before time $t + \delta$ in each case. The $A_i$ and $B_i$ then compare the bits they sent and received—which, of course, involves a delay of order $\Delta x$. If the two bits are equal, the protocol generates a 0; if unequal, a 1. The separation of the laboratories means that each party can be confident that the other's bit was sent in ignorance of their own. Each party can hence be confident of the randomness of the generated bit. Quantum attacks clearly do not affect the protocol's security, since it relies only on the causal relations of special relativity, so that the protocol also defines an unconditionally secure quantum coin-tossing protocol.

On the other hand, a simple application of the Mayers-Lo-Chau argument [5,8] shows that no classical or quantum bit commitment protocol that uses a finite sequence of messages can be permanently unconditionally secure in this scenario. By permanent security, we mean here that after the protocol is concluded, it remains indefinitely impossible for Alice or Bob to cheat, no matter how much information is transferred between the $A_i$ or between the $B_i$. Clearly, this cannot be attained by a finite protocol, since after the protocol is concluded, all data that the $A_i$ hold or receive can, after a finite time interval, be transferred to one representative, say $A_1$; similarly the $B_i$ can transfer all their data to $B_1$. At this point, the situation is identical to that after the implementation of a quantum bit commitment protocol in the standard scenario.

To see this, note that the $A_i$ and $B_i$ can carry out every step in any relativistic protocol at the quantum level. In particular, any random choices required by the protocol can be kept at the quantum level by entangling suitably chosen "quantum dice"—ancillary systems in a state $\sum_i p_i |i\rangle$—with the transmitted states via a quantum computer. If both $A_i$ (or both $B_i$) are required to make the same random choice at spacelike separated points, they can do so, using previously constructed shared random dice, with states of the form $\sum_i p_i |i\rangle_1 |i\rangle_2$, where the $|\rangle_i$ states are under the control of the $i$th party. After the end of the finite protocol, all the quantum information held by $A_2$ can be given to $A_1$, and all the quantum information held by $B_2$ can be given to $B_1$. We then have a situation in which $A_1$ and $B_1$ share some pure state $|\psi\rangle$ lying in the tensor product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A$ and $\mathcal{H}_B$ describe the degrees of freedom under the control of $A_1$ and $B_1$, respectively. This is precisely the situation analyzed by Mayers, Lo, and Chau, and their theorem applies: either $B_1$ can cheat by distinguishing the commitments of 0 and 1 with nonzero probability before revelation, or else $A_1$ can follow the protocol for committing a 0 and then cheat to reveal a 1 with nonzero probability, and the two cheating probabilities cannot simultaneously be small [6,9].

It follows that coin tossing is a weaker primitive than bit commitment in the relativistic scenario outlined. Perhaps more surprisingly, it follows also that coin tossing is weaker under standard cryptographic assumptions. For suppose there were a finite standard bit commitment protocol which was provably secure modulo the security of a coin-tossing black box. That is, Alice and Bob have some trusted way of generating random bits between them, and build up a secure bit commitment protocol by a finite sequence of classical or quantum communications interspersed with finitely many invocations of the random bit generation. Any such protocol could be transferred to the relativistic scenario, by replacing the classical and quantum communications between $A$ and $B$ by identical communications between $A_1$ and $B_2$, and replacing the coin-tossing black box by implementations of the above secure quantum coin-tossing protocol involving the $A_i$ and $B_i$. So long as the messages are carried out in the same sequence, the bit commitment protocol would necessarily remain secure in the relativistic scenario. But we have seen that no secure finite bit commitment protocol exists in this scenario. Hence the initial assumption must be impossible: there is no finite permanently secure standard bit commitment protocol built on a secure coin-tossing black box.

It has recently been shown that unconditionally secure bit commitment protocols based on an indefinite exchange of messages do exist in the relativistic scenario [10,11]. We have seen here another intriguing aspect of the interplay between relativity and information: relativistic cryptography appears to provide not only new practically useful protocols—of which the coin tossing protocol above is an example—but also a useful perspective on standard cryptographic relations. It should be noted, however, that while relativistic considerations motivate the proof, they are not essential in establishing the result. The only essential relativistic ingredient we have used is the guarantee of a time delay in communicating between certain representatives of $A$ and $B$, and the proof can be recast abstractly using only this property.

Finally, it is worth noting that cryptographic tasks give a way of calibrating the properties of information in *any* physical theory, correct or not, by asking whether or not any given task can be securely implemented. The fact that coin tossing is strictly weaker than bit commitment means they define distinct calibrations of physical information. It would be interesting, and perhaps theoretically useful, to use the hierarchy of cryptographic protocols as a way of isolating different properties of information which can be realized in different physical models.

I am very grateful to Claude Crépeau, Hoi-Kwong Lo, David Mermin, Asher Peres, Louis Salvail, and, especially, Peter Goddard and Sandu Popescu for very helpful comments, as well as to the Royal Society for financial support.

*Electronic address: apak@damtp.cam.ac.uk

[1] M. Blum, in *Proceedings of the 24th IEEE Computer Conference, Compcon* (IEEE, New York, 1982), pp. 133–137.
[2] J. Kilian, *Uses of Randomness in Algorithms and Protocols* (MIT Press, Cambridge, MA, 1990), p. 68.
[3] S. Wiesner, SIGACT News **15**, 78 (1983).
[4] C. H. Bennett and G. Brassard, in *Proceeedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), p. 175.
[5] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
[6] D. Mayers, quant-ph/9603015.
[7] D. Mayers, in *Proceedings of the Fourth Workshop on Physics and Computation* (New England Complex System Inst., Boston, 1996), p. 226.
[8] H.-K. Lo and H. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
[9] H.-K. Lo and H. Chau, Physica (Amsterdam) **120D**, 177 (1998).
[10] A. Kent, Phys. Rev. Lett. **83**, 1447–1450 (1999).
[11] A. Kent, quant-ph/9906103 (to be published).