We propose a new classical bit commitment protocol using the relativistic constraint that signals cannot travel faster than the speed of light $c$. This protocol is unconditionally secure against both classical or quantum attacks. The sender (Alice) and the receiver (Bob) each controls two secure stations separated by a large distance $d$, and they communicate by exchanging classical information only. Alice commits by sending from her stations two causally independent encrypted messages to the neighboring Bob's stations, after that the protocol is out of her control and she plays no role in the unveiling phase. The commitment remains concealed for a period of $\Delta t = d/2c$. This protocol requires only limited communication resources and is readily implementable with current technologies.

PACS numbers: 03.67.Dd
Keywords: bit commitment, cryptography
can be taken to be infinity. The principle of relativity however dictates that nothing can travel faster than the speed of light. Using this constraint, Kent has successfully constructed a classical bit commitment scheme which can be shown to be unconditionally secure \[23\]. Apart from using relativistic physics, this protocol departs from the standard bit commitment scenario in that Alice (A) and Bob (B) are allowed to set up trusted stations located far away from themselves. This additional feature is also present in all other versions of relativistic bit commitment protocols proposed in recent years \[26, 28\].

In the latest 2012 proposal \[27\], Alice and Bob each control three secure stations, \((A_1, A_2, A_3)\) and \((B_1, B_2, B_3)\), respectively. The sender stations \(A_2\) and \(A_3\) are located far away on opposite sides of \(A_1\), and each \(A_i\) has a receiver station \(B_i\) located adjacent to it. \(B_1\) sends \(A_1\) a number of randomly chosen BB84 qubits \[1\], depending on the value of \(b\) she wants to commit. \(A_1\) measures the qubits in one of the two BB84 bases and sends the measurement outcomes securely to \(A_2\) and \(A_3\), who then unveil by revealing the outcomes to \(B_2\) and \(B_3\) respectively. This protocol is experimentally feasible and has been successfully implemented recently \[29, 30\] with a commitment time of 15ms. Note that this protocol involves quantum communications and measurements which greatly increase the complexity of security analysis theoretically \[28\]. Moreover, when implemented in the real world, one also need to consider the systematic errors in the preparation and transmission of the quantum particles by Bob, and also in the measurements executed by Alice. The purpose of this paper is to present a new relativistic bit commitment protocol which requires the exchange of classical information only. Due to the absence of quantum transmissions and measurements, this protocol can be shown to be unconditionally secure in a relatively transparent manner. Moreover it can also be readily implemented in realistic situations.

Let Alice controls two secure stations \((A_1, A_2)\), and Bob controls another two \((B_1, B_2)\). \(B_1\) and \(B_2\) are separated by a large distance \(d\), but the distance between \(B_1\) and \(A_1\) is negligible compared with \(d\), so is that between \(B_2\) and \(A_2\). We assume that there are only classical communication channels between Alice and Bob, but the same cannot be guaranteed for internal communications between \(A_1\) and \(A_2\), or \(B_1\) and \(B_2\). We shall make the idealization that information transmits along all channels at the speed of light \(c\). Since \(A_1\) is adjacent to \(B_1\) \((i = 1, 2)\), for simplicity we shall take the time required to transmit information between them to be negligible, so is the time required to process information at each station. Let \((n_0, n_1, m_0, m_1, \eta)\) be random but distinct bit-chains of length \(l\) \((i.e.,\ they\ are\ numbers\ between\ 0\ and\ 2^l - 1\ in\ the\ binary\ form)\). It is understood that \((n_0, n_1)\) are generated on demand by \(B_1\), and \((m_0, m_1)\) by \(B_2\) independently. \(\eta\) is a secret key shared by \(A_1\) and \(A_2\), it can be pre-established by any secure quantum key distribution protocol, such as BB84 \[1\]. The new protocol can be specified as follows.

**Commit:**

1. Alice \((A_1, A_2)\) decides the value of \(b \in \{0, 1\}\).
2. At time \(t = 0\), \(B_1\) sends to \(A_1\) two distinct random bit-chains \((n_0, n_1)\), and \(A_1\) commits by returning the number \(N_b = (\eta \text{xor} n_b)\) to \(B_1\). Independently also at \(t = 0\), \(B_2\) sends \(A_2\) two distinct random bit-chains \((m_0, m_1)\), and \(A_2\) commits by returning \(M_b = (\eta \text{xor} m_b)\) to \(B_2\).
3. \(B_1\) sends \((\lambda_0, \lambda_1)\) to \(B_2\), where \(\lambda_i = (N_b \text{xor} n_i)\). Similarly, \(B_2\) sends \((\zeta_0, \zeta_1)\) to \(B_1\), where \(\zeta_i = (M_b \text{xor} m_i)\).

**Unveil:**

1. The protocol unveils when \(B_1\) receives \((\lambda_0, \lambda_1)\) and \(B_2\) receives \((\zeta_0, \zeta_1)\) at \(t = d/c\) \[31\].
2. The committed value of \(b\) is obtained from the conditions \(\lambda_0 = \zeta_0\) and \(\lambda_1 - b \neq \zeta_1 - b\). If neither \(b = 0\) nor \(b = 1\) satisfies these conditions, then Alice is cheating.

The unveiling mechanism can be understood as follows. Without loss of generality, suppose \(A_1\) and \(A_2\) commit to \(b = 0\), then \(N_0 = \eta \text{xor} n_0\) and \(M_0 = \eta \text{xor} m_0\). It follows that

\[
\lambda_0 = (\eta \text{xor} n_0) \text{xor} n_0 = \eta, \quad (1)
\]

\[
\lambda_1 = (\eta \text{xor} m_0) \text{xor} m_0 = \eta, \quad (2)
\]

so that \(\lambda_0 = \zeta_0\). However

\[
\lambda_1 = (\eta \text{xor} n_0) \text{xor} n_1, \quad (3)
\]

\[
\zeta_1 = (\eta \text{xor} m_0) \text{xor} m_1, \quad (4)
\]

are uncorrelated random numbers, so that \(\lambda_1 \neq \zeta_1\). Nevertheless in principle one cannot strictly rule out the possibility that \(\lambda_1 = \zeta_1\) by chance, in which case the unveiled result is ambiguous. However the probability for this to happen is \(1/2^l\), which can be made as small as desired by adopting a large \(l\).

Next we show that this protocol is unconditionally secure. Clearly, \(N_b\) and \(M_b\) are respectively encryptions of \(n_b\) and \(m_b\), with \(\eta\) being the common encryption key or one-time pad. It is well known in cryptography that, without the knowledge of \(\eta\) and before \(B_1\) and \(B_2\) have time to exchange information, \(N_b\) and \(M_b\) are nothing but random numbers from which no information of \(b\) can be extracted. Hence the commitment is concealed for \(0 < t < d/c\). Here we have implicitly assume that Bob sets up
only two stations ($B_1$ and $B_2$) as stipulated by the protocol. However in principle nothing can prevent him from setting up a secret station $B_3$ somewhere else. The optimal location for $B_3$ is half way between $B_1$ and $B_2$. Then the information sent by $B_1$ and $B_2$ at $t = 0$ (step 3 of Commit) will both arrive $B_3$ at $t = d/2c$, and the commitment is unveiled. Therefore, for unconditional security, the length of the commitment period ($\Delta t$) should be taken to be $d/2c$ instead of $d/c$.

Next we consider the issue of binding. As we saw, $A_1$’s commitment is separated from $A_2$’s by a space-like interval, the principle of relativity dictates that these two events are causally independent. Hence a dishonest Alice has only two choices before making the commitment: (1) Do $A_1$ and $A_2$ commit to the same $b$? and (2) Do they use the same $\eta$? Now since $A_1$ and $A_2$ must commit at the same moment $t = 0$, it does not make sense logically for them to commit to different values of $b$. It is easy to show that, if $A_1$ and $A_2$ commit to different values of $b$, then the conditions $\lambda_b = \zeta_b$ and $\lambda_{1-b} = \zeta_{1-b}$ will not be satisfied by neither $b = 0$ nor $b = 1$, independent of whether they use the same $\eta$ or not. Given that $A_1$ and $A_2$ commit to the same $b$, they must use the same $\eta$, otherwise the unveiling process will again be unsuccessful, even if they choose to be honest. The argument is more transparent and straightforward from the following point of view. Notice that the protocol is completely out of Alice’s control after she commits and she does not play any role in the unveiling phase. This fact already implies that Alice cannot cheat. The reason is that, no matter which value of $b$ is revealed in the unveiling phase, it is a direct consequence of what Alice did when she committed, not what she might have done afterward. We conclude that the protocol is safe against classical attacks.

We now consider quantum attacks. As mentioned before, all the information exchanged between Alice and Bob in the commitment phase are restricted to be classical in nature. That is, the numbers $n_0, n_1, m_0, m_1, N_b, M_b$ are all concrete classical numbers without any ambiguities to the respective receivers. Bob has no quantum cheating strategy because he must send classical numbers $(n_0, n_1, m_0, m_1)$ to Alice, and also receives classical numbers $(N_b, M_b)$ in return. Alice does not have much freedom either because the numbers $N_b$ and $M_b$ she sends to Bob in the commitment phase are restricted to be classical. It is well known that quantum attacks depend on the fact that the dishonest party can leave all undisclosed parameters undetermined at the quantum level [13, 14]. Now the only parameter that Alice keeps secret is $\eta$. Although $\eta$ is not known to Bob before unveiling, it is clear that Alice cannot leave it undefined at the quantum level when she commits, otherwise she won’t be able to produce the two classical numbers $N_b$ and $M_b$ to be sent to Bob. This point is also obvious from the fact that Alice does not play any role in the unveiling phase of protocol, that is, she is not required to specify the unknown parameter $\eta$ when the protocol unfolds. This fact clearly implies that she has no freedom to leave it undefined when she commits. We conclude that neither Alice nor Bob has a viable quantum cheating strategy.

Furthermore since Bob sends to Alice classical descriptions of $(n_0, n_1)$ and $(m_0, m_1)$, and she must send back classical numbers $(N_b, M_b)$ in return, Alice can only make classical commitments. That is, she has no freedom to commit to a superposition of $b = 0$ and $b = 1$. That means when our protocol is used as a subprotocol in a more complicated task, one can be sure that $b$ has a definite classical value before the protocol is opened [27].

For simplicity, we have made the idealization that information are transmitted at light speed $c$, and that the distance between $A_1$ and $B_2$ is negligible, so is the time required for the agents to process information. There is no difficulties to take into account the actual limitations when implemented in the real world. Realistically we can specify that Alice’s commitments must be completed at $t = \delta << d/c$. The length of the commitment time remains $\Delta t = d/2c$, starting from $t = \delta$ until $t = \delta + d/2c$. The actual speed of information transmission between $B_1$ and $B_2$ may be less than the speed of light, but Alice cannot be sure of that, so $\Delta t = d/2c$ can be regarded as an unconditionally safe lower bound.

Notice that in the protocol proposed above, $A_1$ and $A_2$ play symmetric roles, so do $B_1$ and $B_2$. However in some applications it may be more convenient or advantageous to have one of Alice’s and Bob’s stations (say $A_2$ and $B_2$) play subordinate roles only. Such a protocol is also possible and can be specified as follows.

**Commit**: (1) $A_1$ decides the value of $b \in \{0, 1\}$. (2) At time $t = 0$, $B_1$ sends to $A_1$ two distinct random bit-chains $(n_0, n_1)$, and $A_1$ commits by returning the number $N_b = (\eta \ xor n_b)$ to $B_1$. At the same time ($t = 0$), $A_2$ sends $\eta$ to $B_2$, and $B_2$ sends $\eta$ to $B_1$.

**Unveil**: (1) The protocol unveils when $B_1$ receives $\eta$ at $t = d/c$ from $B_2$ [31]. (2) The committed value of $b$ is obtained from the condition $n_b = \eta \ xor N_b$.

In this protocol, $A_2$ does not need to know the value of $b$ to be committed, her only role is to deliver the encryption key $\eta$ to $B_2$. From the discussion we have gone through earlier, the security of this alternative protocol is quite obvious: (1) $B_1$ cannot extract any information from $N_b$ until he receives the key $\eta$ from $B_2$. (2) Alice cannot cheat because the protocol is out of her control after she commits. (3) The unconditionally secure commitment time is again $\Delta = d/2c$ as before.

To summarize, we have proposed a new unconditionally secure bit commitment protocol base on
the relativistic restriction that signals cannot travel faster than the speed of light. This protocol does not involve any quantum particles so that the theoretical security analysis is relatively simple and transparent, moreover it can be readily implemented experimentally. Alice commits by making two encryptions separated by a space-like interval. Security against Bob is guaranteed by the fact that an encrypted message contains no extractable information without the key. One special feature of the protocol is that Alice does not play a role in the unveiling phase, in fact she has no control over the protocol after she commits; this feature clearly implies that Alice cannot cheat by classical or quantum means. In addition to the original one, we have also proposed an alternative protocol where one of Alice’s stations plays only a subordinate role. This protocol is also unconditionally secure, and it may be more convenient or advantageous in certain cryptographic applications.

[1] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India, 1984), p. 175.
[2] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. 11, 075003 (2009).
[3] M. Blum, SIGACT News, 15, 23 (1983); in Proceedings of the 24th IEEE Computer Society International Conference (Compcon) (IEEE, New York, 1982), p.133.
[4] C. H. Bennett, G. Brassard, C. Crépeau, and M. H. Skubiszewska, in Advances in Cryptology — Proceedings of CRYPTO’91, edited by J. Feigenbaum (Springer, Berlin, 1991), p. 351.
[5] C. Crépeau, J. Mod. Opt. 41, 2455 (1994).
[6] A. C. C. Yao, in Proceedings of the 27th ACM Symposium on Theory of Computing, edited by T. Leighton and A. Borodin (ACM, New York, 1995), p. 67.
[7] D. Mayers, in Advances in Cryptology — Proceedings of Crypto’96 (Springer, Berlin, 1996), p. 343.
[8] See, e.g., G. Brassard, Modern Cryptology: A Tutorial, Lecture Notes in Computer Science Vol. 325 (Springer-Verlag, New York, 1988).
[9] J. Kilian, in Proceedings of the 20th Annual ACM Symposium on Theory of Computing, edited by J. Simon (ACM, New York, 1988), p. 20.
[10] C. Crépeau, J. van de Graaf, and A. Tapp, in Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO’95), edited by D. Coppersmith, Lecture Notes in Computer Science, Vol. 963 (Springer, Berlin, 1995), p. 110.
[11] G. Brassard, C. Crépeau, R. Jozsa, and D. Laplais, in Proceedings of the 34th Annual IEEE Symposium on the foundation of Computer Science, (IEEE Computer Society Press, Los Alamitos, California, 1993), p. 362.
[12] For a review, see G. Brassard and C. Crépeau, SIGACT News 27, 12 (1996).
[13] D. Mayers, Phys. Rev. Lett. 78, 3414 (1997).
[14] H. K. Lo and H. F. Chau, Phys. Rev. Lett. 78, 3410 (1997).
[15] G. Brassard, C. Crépeau, D. Mayers, and L. Salvail, [arXiv:quant-ph/9712025]
[16] J. Bub, Found. Phys. 31, 735 (2001).
[17] C. Y. Cheung, Int. J. Mod. Phys. B 21, 4271 (2007).
[18] G. M. D’Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner, Phys. Rev. A 76, 032328 (2007).
[19] G. Chiribella, G. M. D’Ariano, P. Perinotti, D. M. Schlingemann, and R. F. Werner, Phys. Lett A 377, 1076 (2013).
[20] L. Magnin, F. Magniez, A. Leverrier, and N. J. Cerf, Phys. Rev. A 81, 010302(R) (2010).
[21] H. P. Yuen, [arXiv:0808.2040] [quant-ph].
[22] C. Y. Cheung, [arXiv:0910.2615] [quant-ph].
[23] G. P. He, Phys. Rev. A 74, 022332 (2006).
[24] G. P. He, J. Phys. A 44, 445305 (2011).
[25] A. Kent, Phys. Rev. Lett. 83, 1447 (1999).
[26] A. Kent, New J. Phys. 13, 113015 (2011).
[27] A. Kent, Phys. Rev. Lett. 109, 130501 (2012).
[28] S. Croke and A. Kent, Phys. Rev. A 86, 052309 (2012).
[29] T. Lunghi, J. Kaniewski, F. Bussieres, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden, Phys. Rev. Lett. 111, 180504 (2013).
[30] Y. Liu, Y. Cao, M. Curty, S-K. Liao, J. Wang, K. Cui, Y-H. Li, Z-H. Lin, Q-C. Sun, D-D. Li, H-F. Zhang, Y. Zhao, C-Z. Peng, Q. Zhang, A. Cabello, J-W. Pan, Phys. Rev. Lett. 112, 010504 (2014).
[31] For unconditional security, the protocol should be taken to be unveiled at $t = d/2c$. See discussions in the text.