Experimental Bit Commitment Based on Quantum Communication and Special Relativity

T. Lunghi,[1] J. Kaniewski,[2] F. Bussières,[1,*] R. Houlmann,[1] M. Tomamichel,[2] A. Kent,[3,4]
N. Gisin,[1] S. Wehner,[2] and H. Zbinden[1]

[1] *Group of Applied Physics, University of Geneva, CH-1211 Genève 4, Switzerland*
[2] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[3] *Centre for Quantum Information and Foundations, DAMTP, Centre for Mathematical Sciences,
University of Cambridge, Cambridge CB3 0WA, United Kingdom*
[4] *Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario N2L 2Y5, Canada*

(Received 18 July 2013; published 1 November 2013)

Bit commitment is a fundamental cryptographic primitive in which Bob wishes to commit a secret bit to Alice. Perfectly secure bit commitment between two mistrustful parties is impossible through asynchronous exchange of quantum information. Perfect security is however possible when Alice and Bob split into several agents exchanging classical and quantum information at times and locations suitably chosen to satisfy specific relativistic constraints. Here we report on an implementation of a bit commitment protocol using quantum communication and special relativity. Our protocol is based on [A. Kent, Phys. Rev. Lett. **109**, 130501 (2012)] and has the advantage that it is practically feasible with arbitrary large separations between the agents in order to maximize the commitment time. By positioning agents in Geneva and Singapore, we obtain a commitment time of 15 ms. A security analysis considering experimental imperfections and finite statistics is presented.

DOI: 10.1103/PhysRevLett.111.180504 PACS numbers: 03.67.Dd, 03.67.Hk

Bit commitment is a fundamental primitive with several applications such as coin tossing [1] and secure voting [2]. In a bit commitment protocol, Bob commits a secret bit to Alice at a given instant which he can choose to reveal some time later. Security here means that if Bob is honest, then his bit is perfectly concealed from Alice until he decides to open the commitment and reveal his bit. Furthermore, if Alice is honest, then it should be impossible for Bob to change his mind once the commitment is made. That is, the only bit he can reveal is the one he originally committed himself to. Information-theoretically secure bit commitment in a setting where the two mistrustful parties exchange classical messages in an asynchronous fashion is impossible. An extensive amount of work was devoted to study asynchronous quantum bit commitment, for which perfect security was ultimately shown to be impossible [3,4] as well (see also Refs. [5,6]). This does not preclude the existence of protocols with partial (but less-than-complete) bias [7–10], which have been the subject of related experimental work [11–13]. Bit commitment was also demonstrated experimentally using the assumption of noisy quantum storage [14]. Alternatively, perfectly secure relativistic protocols based on the exchange of quantum and classical bits have been proposed [15–18]. We focus here on the protocol [18], which is proven secure in the ideal case (i.e., with perfect devices) [19] and in the presence of loss [20]. In this Letter, we present the first experimental implementation of a secure bit commitment protocol that is based on quantum communication and relativistic constraints, along with a security proof taking into account its experimental imperfections and finite-size effects.

Let us briefly describe the original protocol [18]. Figure 1(a) shows the evolution of the protocol in a space-time diagram. Bob wants to commit a bit b to Alice. The protocol starts when Alice sends a group of N

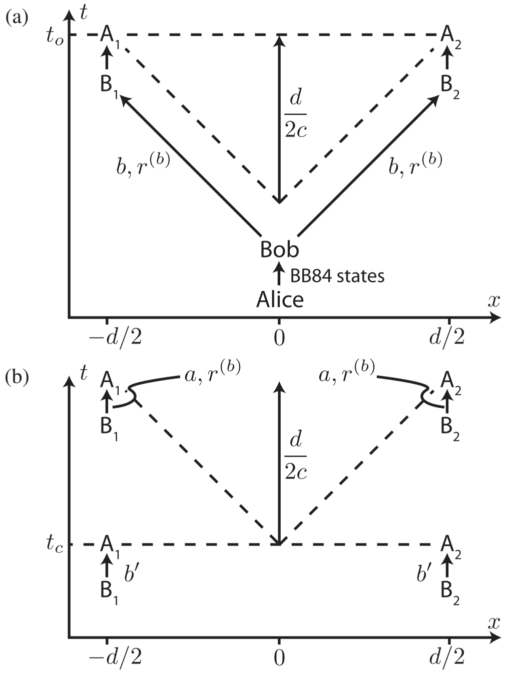

FIG. 1. (a) Space-time (x-t) diagram of the protocol of Ref. [18]. (b) The relativistic portion of a modified version of (a). The quantum exchange between Alice and Bob happens much before and is not shown.

single photons to Bob (all photons arrive to Bob at the same time). The quantum state of each photon is chosen at random among the four BB84 states. Bob then immediately and simultaneously measures all photons in the $\{|0\rangle, |1\rangle\}$ basis to commit to $b = 0$, or in the $\{|+\rangle, |-\rangle\}$ basis to commit to $b = 1$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. This constitutes the commitment phase. Let us now denote by $r_i^{(b)}$ the measurement result of the ith photon. Bob then immediately sends at light speed the array $r^{(b)} = \{b, r_1^{(b)}, \ldots, r_N^{(b)}\}$ to trusted agents B_1 and B_2 that are symmetrically located on each side of Bob and that are separated by a straight-line distance d. Communication from Bob to each agent is authenticated and encrypted using preshared key material. Once agents B_1 and B_2 have received $r^{(b)}$, they can (if they choose) later simultaneously communicate $r^{(b)}$ to the trusted agents of Alice A_1 and A_2, who are sitting right next to B_1 and B_2, respectively. This opens the commitment. The commitment is accepted when A_1 and A_2 later verify (using authenticated channels) they have indeed received the same strings at the same time, and that the measurement results are consistent with the states she sent. To quantify security for honest Alice we find an upper bound of the form $p_0 + p_1 \leq 1 + \epsilon$, where p_b is the probability that Bob successfully unveils b in the open phase (see Sec. A-4-b of the Supplemental Material [21] for details). In the ideal case we would have $\epsilon = 0$, which means that Bob can open the honest bit perfectly, while his attempt to open the other bit will always fail. We show that for our implementation ϵ decays exponentially in N (see Sec. A-5-c of the Supplemental Material [21]). The duration of the commitment is $d/2c$, where c is the speed of light. Note that Bob's agents do not have to open the commitment as soon as they receive the string $r^{(b)}$; they can wait for as long as they wish. However, Alice has to consider that a cheating Bob could have stored the qubits in a quantum memory and retrieved them at the very last instant for the measurement. Hence, Alice's agents can only be sure that Bob was committed between $t_o - d/2c$ and t_o, where t_o is the instant when they received $r^{(b)}$.

This original protocol presently appears impractical for terrestrial implementations with existing devices for direct bit commitments. The main reason is that imperfect preparation of true single photon states, combined with inefficient and slow single-photon detectors, seems unlikely to allow Alice to send, and Bob to detect, sufficiently many high-quality qubits in a time that is negligibly small compared to $d/2c$ (i.e., at most 21.25 ms for d bounded by Earth's diameter). Another problem is that it seems difficult for an honest Bob to communicate $r^{(b)}$ to his agents at near light speed unless there is a free-space line-of-sight communication channel between them, which requires $d \lesssim 200$ km or so on Earth. One could also envision using neutrino pulses sent through Earth for the communication, but this would require expensive technology that is not widely available.

The protocol can be made more practical using a delayed-choice commitment [see Fig. 1(b)]. Specifically, the protocol starts when Alice and Bob exchange quantum bits, but the measurement basis of Bob, denoted b, is chosen at random and is not correlated with the bit he wishes to commit to. In this way, the quantum exchange can happen at any time and location before the commitment phase (defined below). In our implementation, after measuring all the quantum bits, Bob privately communicates the measurement results to agents B_1 and B_2 separated by d, and also tells Alice which of the qubits she sent yielded a click in one of his detectors. This is important: Alice needs to know before the commitment phase which qubits were detected by Bob; otherwise, he could measure half of Alice's qubits in one basis and the other half in the other, and reveal either basis at the opening phase without introducing additional errors in the results (and then avoid being caught cheating). Bob's agents are now ready to start the commitment. For this, in our implementation, they simultaneously send at instant t_c a bit $b' = b \oplus a$ to the nearby agents A_1 and A_2 of Alice, where a is the bit that Bob actually wants to commit himself to and b is the randomly committed bit. Note that as b is random, it effectively forms a one-time pad with which Bob encrypts a, and hence Alice cannot learn a from b'. At time $t_c + d/2c$, B_1 and B_2 simultaneously reveal a and $r^{(b)}$, and A_1 and A_2 can check if the measurement results are consistent with b. The time t_c is chosen by Bob's agents.

Security against a malicious Alice in the ideal case is obvious, since Bob does not reveal any information about his quantum measurement until the opening of the commitment. Security against a malicious Bob follows from communication constraints imposed by special relativity and the no-cloning theorem. A cheating Bob attempts to choose b after time t_c, i.e., at a time when his agents B_1 and B_2 are separated [cf. Fig. 1(b)]. Let us assume that Bob tries to open $b = 0$. Then, to convince A_1 and A_2 that the commitment is valid, B_1 and B_2 must determine—independently—the state that Alice sent for all rounds in which either $|0\rangle$ or $|1\rangle$ was used. This is similar for $b = 1$ with $|+\rangle$ and $|-\rangle$. By delaying the measurement until b is decided, a single agent (e.g., B_1) can determine these states perfectly for both values of b. However, the no-cloning theorem prohibits that both agents have access to a good copy of the quantum system after t_c, and hence this strategy does not work. In fact, we show that any cheating strategy must fail because the amount of quantum information about Alice's state held by B_1 and B_2 is restricted by the monogamy of entanglement (for details see Sec. A of the Supplemental Material [21]). Note that our protocol can be modified to use three (or more) separated agents of Bob's in a way that requires only one agent to decide what should be the commitment (for details see Sec. F of the Supplemental Material [21]).

It is important to realize that in the security proof it is enough to use the communication constraints imposed by special relativity. Specifically, it is based on the assumption that no communication between B_1 and B_2 is possible after the commitment phase is completed. This model is interesting because, while imposing minimum communication constraints necessary to evade the impossibility proof in the asynchronous model, it is also sufficiently strong to allow for secure quantum bit commitment [19]. Moreover, quantum communication gives the advantage that Alice does not need to share any secret data with her agents A_1 and A_2. On the other hand, if she tells them what quantum states were used in the commitment phase (using a one-time-pad encrypted channel), then the dishonest Bob will be instantaneously caught cheating at the unveiling. For more details about the quantum advantage in these scenarios please refer to Sec. E of the Supplemental Material [21].

In the two-site protocol implemented, our security proof relies on the fact that not only is communication between B_1 and B_2 impossible between commitment and unveiling, but no other agent of Bob's can send classical or quantum information generated at any location after t_c that reaches them both by $t_c + (d/(2c))$. Hence in the open phase B_1 and B_2 must generate their answers using disjoint quantum systems, which cannot have been jointly acted upon by any agent of Bob's after t_c.

We now discuss how experimental imperfections are taken into account in the security proof. Full details are given in Sec. A of the Supplemental Material [21]. In practice, qubits sent by Alice can come from attenuated laser pulses yielding a Poisson distribution of the photon number with mean μ. Pulses containing two or more photons can be split and measured by a malicious Bob in both bases, allowing his agents to successfully reveal both commitments. Losses from Alice to Bob thus become important: to ensure security, the majority of all pulses sent by Alice that will yield a click in Bob's detectors must come from single-photon pulses. Let us assume that Alice sends N pulses of light each containing on average μ photons. Bob later declares that n of these pulses generated clicks in one of his detectors (and their labels, so that Alice knows the state she sent for each detection). Let $p_{\mathrm{det}} = n/N$ be the estimated detection probability declared by Bob. After Bob reveals $r^{(b)}$, Alice calculates the number of bits n' for which the preparation and measurement bases were the same, as well as the number of errors n_{err} on these bits (with respect to the states she sent). The qubit error rate (QBER) is defined as n_{err}/n'. In the limit $N \to \infty$, the protocol is secure if

$$p_{\mathrm{det}} > \frac{1 - e^{-\mu}(1 + \mu)}{1 - \frac{\mathrm{QBER}}{\lambda}}, \tag{1}$$

where $\lambda = \frac{1}{2}(1 - 1/\sqrt{2}) \approx 0.146$.

To account for finite statistics, Alice and Bob agree on a maximal QBER value, denoted δ, and a minimal detection probability, denoted γ. Alice will abort the protocol if Bob declares $p_{\mathrm{det}} < \gamma$ as security cannot be ensured in this case (as explained above). Moreover, at the end of the protocol, Alice accepts Bob's commitment only if QBER $< \delta$. The choice of suitable thresholds (δ and γ) is a trade off between robustness and security. We want to maximize security while ensuring that the honest scenario succeeds with almost certainty. To account for statistical fluctuations, we thus choose the thresholds suitably bounded away from the theoretical expectation of the QBER and p_{det}. See Sec. A of the Supplemental Material [21] for a complete finite size security analysis.

We implemented the modified protocol described above [see Fig. 1(b)]. Thanks to its simplification, the quantum part can be implemented with a quantum key distribution (QKD) system using weak coherent pulses. We used a commercial quantum key distribution system, Vectis 5100 by ID Quantique. This system is based on the "plug-and-play" configuration [22]: trains of light pulses travel back and forth from Bob to Alice, then back to Bob, through a short optical fibre with negligible loss. The two-way implementation allows for an automatic compensation of detrimental fluctuations of the system. When the pulses arrive on Alice's side, she uses them to prepare several qubits and attenuates their intensity down to the desired μ. In order to prevent trojan-horse attacks, the incoming power is continuously monitored [23]. The system was installed in an office at the University of Geneva (see Fig. 2). We note that with our modified protocol, the quantum boxes could be located anywhere, provided the quantum exchange between Alice and Bob happens sufficiently in advance to allow Bob communicating the measurement results to his agents. The optical setup is divided in two quantum boxes that are respectively controlled by Alice and Bob, and that are connected by an optical fibre only. The quantum box of Alice (or Bob) records the relevant information for the protocol and communicates with agents A_1 and A_2 (or B_1 and B_2) through the Internet. The classical communication between Bob (or Alice) and B_1 and B_2 (or A_1 and A_2) is authenticated [24,25] and one-time-pad encrypted using preshared keys generated from a certified quantum random generator from ID Quantique. We note that authentication and ciphering are used before

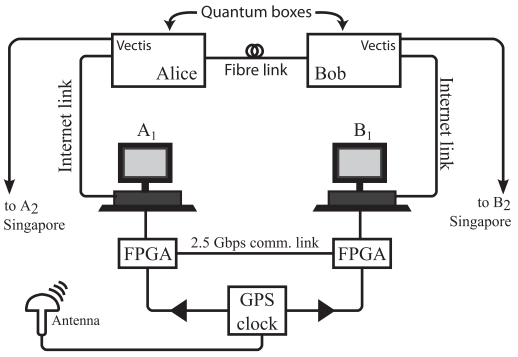

FIG. 2. Experimental setup located in Geneva. The setup located in Singapore is the same except for A_1 and B_1 that are replaced by A_2 and B_2, and that there is no QKD system.

or after the commitment region defined on Fig. 1(b) and do not affect the commitment time in any way.

In bit commitment, Alice and Bob are mistrustful, whereas in QKD they are collaborators. Consequently, the operation of the QKD system had to be adapted to our protocol. Specifically, the software of the system was modified to eliminate all the classical communication used for the key sifting, except for the reporting of which of the pulses sent by Alice generated a click in one of Bob's detectors. One side-channel attack then needs to be considered. Indeed, the probability $p_{\rm det}$ of Bob's honest apparatus might depend on the basis in which he measures. Alice could then exploit this difference to gain information about Bob's measurement basis [14]. To eliminate this attack, Bob can test his system for an imbalance, and correct it. In practice, we monitored during 40 hours the detection probability for each measurement basis, and found a ratio $R = (95 \pm 1)\%$. We then programmed Bob's quantum box to declare a detection in the more probable basis with probability R.

Classical agents A_1 and B_1 were located in an office at the University of Geneva, while A_2 and B_2 were in an office on the campus of the National University of Singapore. The straight-line distance (through Earth) between the two locations is about 9354 km, corresponding to a commitment time of $d/2c = 15.6$ ms. This is close to the theoretical maximal value of $\approx$21.2 ms achievable with antipodal points on the surface of Earth. A representation of the experimental setup is depicted in Fig. 2. Each of the classical agents is a stand-alone computer equipped with a field-programmable gate array (FPGA) programmed to execute the necessary steps of the protocol. Each FPGA is synchronized to universal time using a global positioning system clock. Communication between B_1 and A_1 (and similarly for B_2 and A_2) is done over a 2.5 Gbps optical link. The time required to communicate 7000 bits [a typical length for the string $r^{(b)}$] is about 3 μs, which is effectively negligible compared to 15 ms.

We realized 50 bit commitments by measuring in basis $b = 0$, and 50 more in basis $b = 1$, all of these with $\mu = (5.0 \pm 0.5) \times 10^{-2}$. Figure 3 shows the observed QBERs with $b = 0$. The optical transmission from Alice to Bob, including detector efficiency, was of the order of 6%, yielding a mean detection probability $p_{\rm det}$ of 0.32% (this includes the contribution of dark counts and multiphoton pulses). The QBER varied between 2.8% and 4.3% and averaged at 3.4%. For details see Sec. G of the Supplemental Material [21].

Given the characterization described above, we choose to set the maximal tolerable value of the QBER to $\delta = 5\%$, which, when combined with the average μ, yields a value of 0.16% for the right-hand side of the asymptotic security condition [Eq. (1)]. For the minimum tolerable detection probability γ, we choose a value of 0.2% with $N = 220 \times 10^4$ pulses sent by Alice. The number of detections declared by Bob was about 7000 per commitment. The security parameter with these numbers is $\epsilon \leq 5.5 \times 10^{-8}$ (see Sec. A-5-c of the Supplemental Material [21] for the explicit computation of the upper bound). The inset of Fig. 3 shows the trade off between $p_{\rm det}$ and μ imposed by our security proof. Experimental points are shown and are well within the secure region, which highlights the robustness of the implementation.

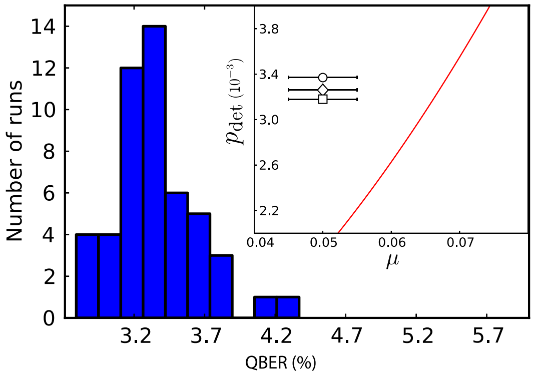

FIG. 3 (color online). Histogram of the observed QBER from the set of 50 commitments with measurement basis $b = 0$. Inset: the circle, diamond and square points are experimental values of $p_{\rm det}$ corresponding to the highest, average, and lowest values of the set (all for the same value of μ). The solid line is the boundary of the region for which our proof guarantees security (left side) in the asymptotic limit [Eq. (1)]. The uncertainty on μ corresponds to slightly overestimated daily fluctuations.

We have demonstrated for the first time the possibility of implementing practical and secure bit commitment using quantum communication and special relativity. Our implementation also demonstrates the possibility of implementing such commitments in real time for data acquired at a single location. This kind of system could potentially be useful in the high-speed trading stock market where short term commitments are sufficient. One of its main advantages is that the quantum part of the protocol can happen at any time before the committing phase. Hence, quantum data can be accumulated and communicated to agents located far away.

This work was supported in part by the NCCR-QSIT, the European IP-SIQS, the Ministry of Education (MOE), and National Research Foundation Singapore through Tier 3 Grant No. MOE2012-T3-1-009, and by the John Templeton Foundation. We thank ID Quantique and Oscilloquartz for useful discussions and technical help. We thank B. Sanguinetti, N. Walenta, C. C. W. Lim, P. Trinkler, M. Legré, and D. Caselunghe for useful discussions.

Note added.—After the conclusion of this project, we learned of an independent experiment implementing the original protocol of Kent [26].

*felix.bussieres@unige.ch

[1] M. Blum, *Coin Flipping by Telephone: A Protocol for Solving Impossible Problems*, in Advances in Cryptology: A Report on CRYPTO'81 Vol 82 (Santa Barbara, California, 1981), pp. 11–15.

[2] A. Broadbent and A. Tapp, in *Proceedings of the IAVoSS Workshop On Trustworthy Elections (WOTE 2008)*, http://eprint.iacr.org/2008/266.

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

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

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

[6] S. Winkler, M. Tomamichel, S. Hengl, and R. Renner, Phys. Rev. Lett. **107**, 090502 (2011).

[7] D. Aharonov, A. Ta-Shma, U. Vazirani, and A. C.-C. Yao, in *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, Portland, Oregon, USA, 2000* (ACM, New York, 2000), pp. 705–714.

[8] R. W. Spekkens and T. Rudolph, Phys. Rev. A **65**, 012310 (2001).

[9] A. Kitaev, *Quantum Coin-Flipping* (Mathematical Sciences Research Institute, Berkeley, CA, 2002).

[10] A. Chailloux and I. Kerenidis, in *Proceedings of the 52nd Annual Symposium on Foundations of Computer Science, IEEE, Palm Springs, California, 2011* (IEEE, New York, 2011), pp. 354–362.

[11] A. T. Nguyen, J. Frison, K. P. Huy, and S. Massar, New J. Phys. **10**, 083037 (2008).

[12] G. Berlín, G. Brassard, F. Bussières, N. Godbout, J. A. Slater, and W. Tittel, Nat. Commun. **2**, 561 (2011).

[13] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, arXiv:1306.3368.

[14] N. H. Y. Ng, S. K. Joshi, C. C. Ming, C. Kurtsiefer, and S. Wehner, Nat. Commun. **3**, 1326 (2012).

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

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

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

[18] A. Kent, Phys. Rev. Lett. **109**, 130501 (2012).

[19] J. Kaniewski, M. Tomamichel, E. Hanggi, and S. Wehner, IEEE Trans. Inf. Theory **59**, 4687 (2013).

[20] S. Croke and A. Kent, Phys. Rev. A **86**, 052309 (2012).

[21] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.111.180504 for the detailed security analysis, remarks on the quantum advantage and complete experimental results.

[22] G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Electron. Lett. **34**, 2116 (1998).

[23] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).

[24] J. L. Carter and M. N. Wegman, J. Comput. Syst. Sci. **18**, 143 (1979).

[25] M. N. Wegman and J. L. Carter, J. Comput. Syst. Sci. **22**, 265 (1981).

[26] 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, and J.-W. Pan, arXiv:1306.4413.