Practical Relativistic Bit Commitment

T. Lunghi,[1] J. Kaniewski,[2,3] F. Bussières,[1] R. Houlmann,[1] M. Tomamichel,[2,4] S. Wehner,[2,3] and H. Zbinden[1]
[1]Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, CH-1211 Genève 4, Switzerland
[2]Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore
[3]QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, Netherlands
[4]School of Physics, The University of Sydney, Sydney 2006, Australia
(Received 19 November 2014; published 13 July 2015)

Bit commitment is a fundamental cryptographic primitive in which Alice wishes to commit a secret bit to Bob. Perfectly secure bit commitment between two mistrustful parties is impossible through an asynchronous exchange of quantum information. Perfect security is, however, possible when Alice and Bob each split into several agents exchanging classical information at times and locations suitably chosen to satisfy specific relativistic constraints. In this Letter we first revisit a previously proposed scheme [C. Crépeau *et al.*, Lect. Notes Comput. Sci. 7073, 407 (2011)] that realizes bit commitment using only classical communication. We prove that the protocol is secure against quantum adversaries for a duration limited by the light-speed communication time between the locations of the agents. We then propose a novel multiround scheme based on finite-field arithmetic that extends the commitment time beyond this limit, and we prove its security against classical attacks. Finally, we present an implementation of these protocols using dedicated hardware and we demonstrate a 2 ms-long bit commitment over a distance of 131 km. By positioning the agents on antipodal points on the surface of Earth, the commitment time could possibly be extended to 212 ms.

DOI: 10.1103/PhysRevLett.115.030502 PACS numbers: 89.70.-a, 03.30.+p, 03.67.Dd, 03.67.Hk

Bit commitment is a fundamental primitive with several applications, such as coin tossing [1], secure voting [2], contract signing, and honesty-preserving auctions [3]. In a bit commitment protocol, Alice commits a secret bit to Bob which she can choose to reveal some time later. Security here means that if Alice is honest, then her bit is perfectly concealed from Bob until she decides to open the commitment and reveal her bit. Furthermore, if Bob is honest, then it should be impossible for Alice to change her mind once the commitment is made. That is, the only bit she can unveil is the one she originally committed herself 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 studying asynchronous quantum bit commitment, for which perfect security was ultimately shown to be impossible [4–7]. Note, however, that arbitrarily long commitments are possible if one makes the assumption that the quantum memory of the dishonest party is bounded [8,9] or noisy [10,11].

Alternatively, bit commitment with split agents exchanging classical information was proposed as early as 1988 [12]. Security against classical attacks was proved under the condition that no communication was possible between some of the agents. This protocol was later simplified [13], and the new scheme called simplified-BGKW, sBGKW [12] was proven secure against classical and a restricted class of quantum attacks. The possibility of enforcing the no-communication condition using relativistic constraints on the timing of the classical communication was formulated in Ref. [14]. This later led to the proposal of relativistic protocols based on the exchange of quantum and classical information [15,16], which were proved to be secure against quantum adversaries [17,18]. Such protocols were experimentally demonstrated recently [19,20]. However, the commitment time achievable using these protocols is fundamentally bounded by half of the time required to send light signals between the remote agents, i.e., at most ∼21 ms if they are constrained to be on the surface of Earth.

The possibility of extending the commitment to an arbitrary duration was proposed in 1999 [14]. It relies on positioning one agent of Alice $\mathcal{A}_1$ near an agent of Bob $\mathcal{B}_1$ at an agreed upon location, and similarly agents $\mathcal{A}_2$ and $\mathcal{B}_2$ at another location. Carefully timed classical communication between $\mathcal{A}_i$ and $\mathcal{B}_i$ allows Alice to commit to a bit that she later reveals at a time of her choosing. This requires several rounds of communication, and the amount of communication increases exponentially with the number of rounds making it impractical. This limitation was later mitigated, at least in principle, using a compression scheme that requires only a constant communication rate [21]. The security argument against classical adversaries presented in Ref. [21] is of an asymptotic nature and, therefore, is not sufficient for implementation purposes.

In this Letter, we first revisit the sBGKW bit commitment protocol [13] that uses classical communication only. We show that successful cheating is equivalent to winning a nonlocal game analyzed in Ref. [22], thereby proving the security of this protocol against quantum adversaries. To the best of our knowledge, this is the first entirely classical protocol to be proven secure against arbitrary quantum adversaries. To extend the duration of the commitment beyond the communication time between the locations of the agents (which constitutes the relativistic constraint in the sBGKW scheme), we introduce a novel multiround scheme based on finite-field arithmetic and we prove its security against classical adversaries. Our scheme is simple and efficient and the security argument leads to a natural, algebraic problem for which we prove explicit and quantitative bounds [see Proposition B.2 in the Supplemental Material (SM) [23]]. Finally, we present practical implementations of both the sBGKW scheme and the multiround variant, and we show how this could be used to realize commitments of a duration reaching up to ∼212 ms.

Security definition.—We take $n \in \mathbb{N}$ to be the security parameter and we interpret n-bit strings as elements of the finite field $\mathbb{F}_{2^n}$ (for compactness, we write 0 to denote $0^n = 00\ldots0$). We denote addition by $\oplus$ (in this case, it is just the bitwise XOR) and multiplication by $*$. Moreover, if d is a bit and b is an n-bit string, then we define

$$d \cdot b = \begin{cases} 0 & \text{if } d = 0, \\ b & \text{if } d = 1. \end{cases}$$

All of the secret strings used in the protocol are chosen uniformly at random from $\{0,1\}^n$.

Let Alice (who makes the commitment) and Bob (who receives the commitment) have agents at two distinct locations ($\mathcal{A}_1$ and $\mathcal{B}_1$ at location 1; $\mathcal{A}_2$ and $\mathcal{B}_2$ at location 2) and let $d \in \{0,1\}$ be the bit that honest Alice wants to commit to. The protocol consists of multiple rounds which alternate between the two locations, and the timing is chosen such that every two consecutive rounds are spacelike separated. Hence, no message sent during a certain round from one location can reach the other location in time for the next round.

Security for honest Alice is quantified by Bob's ability to guess her commitment *immediately before* the open phase (assuming he might deviate arbitrarily from the honest protocol). All of the protocols considered in this Letter are *perfectly hiding*, which means that Bob remains completely ignorant about Alice's commitment (his guessing probability equals $1/2$).

Security for honest Bob is quantified through a scenario in which Alice performs an arbitrary action in the commit phase and is *immediately after* challenged to open one of the bits. Given a particular strategy adopted by Alice in the commit phase, we define p_d to be the optimal probability of successfully unveiling d. The protocol is ε *binding* if

$$p_0 + p_1 \leq 1 + \varepsilon$$

for all strategies of dishonest Alice in the commit phase. Note that this is a weak, noncomposable definition of security. In Appendix C we discuss how to formalize these definitions in the relativistic setting. (For a general overview, see Ref. [17].)

Security of the sBGKW scheme.—We now present the scheme proposed in Ref. [13] and we prove its security against quantum adversaries. Before the protocol begins, $\mathcal{A}_1$ and $\mathcal{A}_2$ must share a secret n-bit string a. Note that $\mathcal{B}_1$ also needs a secret string b, but it can be generated before or during the protocol. The protocol consists of two rounds: 1. (commit) $\mathcal{B}_1$ sends b to $\mathcal{A}_1$. $\mathcal{A}_1$ returns $(d \cdot b) \oplus a$ to $\mathcal{B}_1$. 2. (open) $\mathcal{A}_1$ unveils the committed bit d to $\mathcal{B}_1$, while $\mathcal{A}_2$ sends a to $\mathcal{B}_2$.To check whether the commitment should be accepted, $\mathcal{B}_1$ and $\mathcal{B}_2$ need to communicate (e.g., through an authenticated channel) and verify that the string returned by $\mathcal{A}_1$ in the commit phase equals $(d \cdot b) \oplus a$.

Security for honest Alice comes from the fact that the only message that Bob receives in the commit phase is a uniformly random string.

Security for honest Bob in the classical case is fairly intuitive: in order for $\mathcal{A}_2$ to be able to unveil both commitments, she would need to know both a and $a \oplus b$; hence, she would know b. However, since b is chosen uniformly at random by Bob, this must be difficult. This argument can be made rigorous [13] to show that the protocol is ε binding for $\varepsilon = 2^{-n}$ (and this is actually tight: the trivial strategy of always outputting 0 gives $p_0 = 1$ and $p_1 = 2^{-n}$). Unfortunately, this reasoning does not work against quantum adversaries since $\mathcal{A}_2$ could have two distinct measurements that reveal a and $a \oplus b$, respectively, but since they could be incompatible this would not have direct implications on her ability to guess b.

To find an explicit bound on $p_0 + p_1$, we formulate cheating as a nonlocal game in which $\mathcal{A}_1$ receives b, $\mathcal{A}_2$ receives d (the bit she is required to unveil) and the XOR of their outputs is supposed to equal $d \cdot b$. Winning such a game with a probability p_{win} corresponds to a cheating strategy that achieves $p_0 + p_1 = 2p_{\mathrm{win}}$. More concisely, the rules of the nonlocal game are [13] 1. $\mathcal{A}_1$ receives $b \in \{0,1\}^n$, $\mathcal{A}_2$ receives $d \in \{0,1\}$ (both chosen uniformly at random).2. $\mathcal{A}_1$ outputs $a_1 \in \{0,1\}^n$, $\mathcal{A}_2$ outputs $a_2 \in \{0,1\}^n$ and they win if and only if $a_1 \oplus a_2 = d \cdot b$. This game was considered in Ref. [22] under the name CHSH_n, and it was shown that

$$p_{\mathrm{win}}(n) \leq \frac{1}{2} + \frac{1}{\sqrt{2^{n+1}}},$$

which is sufficient for our purposes, as it implies that

$$p_0 + p_1 \leq 1 + \sqrt{2} \times 2^{-n/2}$$

for all strategies of dishonest Alice. Therefore, the protocol is ε binding, with $\varepsilon = 2^{(1-n)/2}$ decaying exponentially in n

(but note that the decay rate is half of the decay rate against classical adversaries).

The two-round protocol is mapped onto a nonlocal game precisely because of the assumption of no communication. More specifically, we require that $\mathcal{A}_1$ outputs the answer outside of the future of $\mathcal{A}_2$ receiving the input, and vice versa.

A new multiround protocol.—To extend the commitment time, we propose a multiround protocol and prove its security against classical adversaries. In principle, the commitment time can be made arbitrarily long. However, security depends on the number of rounds of the protocol, which is proportional to the length of the commitment. Therefore, the longer the commitment, the more resources (randomness and communication bandwidth) are required to achieve a given level of security.

Suppose that Alice and Bob want to execute the protocol with $m+1$ rounds and we use k as a label for the round under consideration. Then, $\mathcal{A}_1$ and $\mathcal{A}_2$ must share m secret strings denoted by $\{a_k\}_{k=1}^m$. Similarly, Bob's agents need one secret string for every round denoted by $\{b_k\}_{k=1}^m$ but, again, these can be generated locally during the protocol. All of the rounds before the open phase ($1 \leq k \leq m$) have the same communication pattern: first, $\mathcal{B}_i$ sends an n-bit string to $\mathcal{A}_i$ and then she replies with another n-bit string. In the last round, $\mathcal{A}_i$ sends $\mathcal{B}_i$ a bit (her commitment) and an n-bit string (proof of her commitment). We will denote the n-bit string announced by Bob (Alice) in the kth round by x_k (y_k) regardless of whether he or she is honest or not. The protocol is 1. (commit, $k=1$) $\mathcal{B}_1$ sends $x_1 = b_1$ to $\mathcal{A}_1$. $\mathcal{A}_1$ returns $y_1 = d \cdot x_1 \oplus a_1$. 2. (sustain, $2 \leq k \leq m$) $\mathcal{B}_i$ sends $x_k = b_k$ to $\mathcal{A}_i$. $\mathcal{A}_i$ returns $y_k = (x_k * a_{k-1}) \oplus a_k$. 3. (open, $k = m+1$) $\mathcal{A}_i$ sends d and $y_{m+1} = a_m$ to $\mathcal{B}_i$. To check to see whether the commitment should be accepted, $\mathcal{B}_1$ and $\mathcal{B}_2$ communicate and verify the following relation:

$$\begin{aligned} y_{m+1} = y_m \oplus b_m * y_{m-1} \oplus b_m * b_{m-1} * y_{m-2} \oplus \ldots \\ \ldots \oplus b_m * b_{m-1} * \ldots * b_2 * y_1 \oplus d \cdot b_m * b_{m-1} * \\ \ldots * b_1. \end{aligned}$$

Security for honest Alice is a direct consequence of the fact that every message she announces is masked by a fresh secret n-bit string, which implies that the transcripts corresponding to $d=0$ and $d=1$ are statistically indistinguishable (see Sec. C.1 in the SM [23]).

Proving security for honest Bob is a more challenging task because we require security immediately after the round $k=1$. We first state the main result and then outline the idea behind the proof (for details, refer to Secs. B.2 and C.2 in the SM [23]). The multiround protocol with $m+1$ rounds is ε binding for an $\varepsilon = c_m$ defined as

$$c_m = \begin{cases} 2^{-n} & \text{for } m = 1, \\ \frac{1}{2^{n+1}} + \sqrt{c_{m-1}} & \text{for } m \geq 2. \end{cases} \quad (1)$$

The security argument is conceptually simple: in the classical scenario the *sequential* cheating game in the multiround protocol is *equivalent* to a game in which multiple players act *in parallel*, which allows us to disregard the causal structure of the protocol. We show that cheating in a protocol with $m+1$ rounds is at least as difficult as winning the following m-player game. Let $X_1, X_2, \ldots, X_m$ be independent random variables drawn uniformly from the set of n-bit strings $\{0,1\}^n$, while the kth player receives all the variables except for X_k and outputs an n-bit string. The game is won if the XOR of the outputs equals $X_1 * X_2 * \ldots * X_m$. The bounds we obtain decay exponentially in $n/2^m$. This means that they become significantly weaker as the number of players increases, which ultimately limits the maximum number of rounds that can be implemented in practice. The tightness of these bounds is an interesting open problem and it is briefly discussed in Appendix B. Note that no explicit cheating strategy is known whose winning probability would approach our security bounds.

Implementation.—We implemented the two-round and multiround protocols described above. Each party has agents at two distinct locations: one at the Group of Applied Physics of the University of Geneva and one at the Institute of Applied Physics of the University of Berne. The straight-line distance between the two locations is $s = 131$ km, corresponding to a time separation of 437 μs. The hardware installed in Geneva is conceptually represented in Fig. 1(a) and is identical to the one in Berne. 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

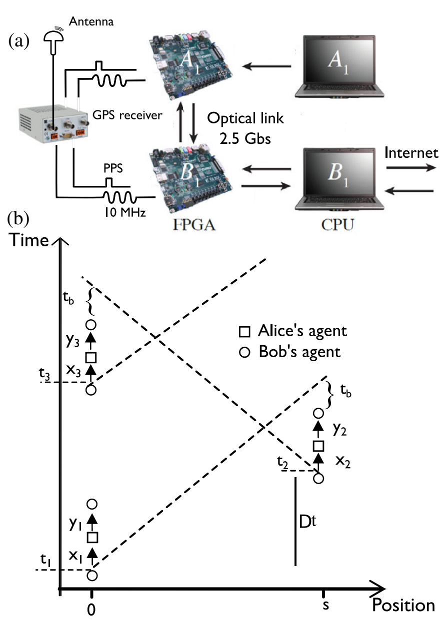

FIG. 1 (color online). (a) Experimental setup. (b) Space-time diagram of the experimental setup.

is synchronized to Coordinated Universal Time via a Global Positioning System (GPS) clock, which consists of a GPS receiver and an oven-controlled quartz-crystal oscillator (OCXO) generating a 10 MHz sinusoidal waveform. Through its GPS connection, the receiver outputs one electronic pulse per second (PPS), which is used to discipline the OCXO. The receiver is locked to the GPS signal with a time accuracy better than 150 ns. The 10 MHz signal generated by the OCXO is fed into the FPGA board and is used to generate a 125 MHz signal using a phase-locked loop. This 125 MHz signal then serves as the time basis for the computations performed on the FPGA. The FPGA also receives the PPS signal to monitor the synchronization with the GPS clock. In particular, the number of cycles between two successive PPS signals is confirmed to be 125×10^6 plus or minus one, where each cycle corresponds to 8 ns. Therefore, the FPGA tolerates fluctuations up to 24 ns on the arrival time of the PPS synchronization signal. The GPS clock also provides the FPGA with a universal time stamp of every PPS signal, allowing Alice and Bob to locate their actions in time.

Before either the two-round or the multiround protocol starts, $\mathcal{A}_1$ and $\mathcal{A}_2$ (and, similarly, $\mathcal{B}_1$ and $\mathcal{B}_2$) share an appropriate number of random n-bit strings. At time t_1, which was agreed upon by both parties, $\mathcal{B}_1$ sends the random string x_1 through the optical link. For a string of 512 bits communicated through the 2.5 Gbps optical link, this requires 205 ns. $\mathcal{A}_1$'s FPGA then computes the string y_1 and sends it to $\mathcal{B}_1$; see Fig. 1(b). The relativistic constraint requires spacelike separation between every two consecutive rounds, which means that the entire second round must be outside of the future light cone of the first bit of x_1 leaving the FPGA of $\mathcal{B}_1$. The commitment begins when the last bit of y_1 is recorded by the FPGA of $\mathcal{B}_1$. With $n = 512$ bits, the security parameter of the two-round protocol is $\varepsilon \approx 10^{-77}$.

In the two-round protocol, $\mathcal{A}_2$ unveils the commitment in the second round, at time $t_2 = t_1 + \Delta t$. She does so by sending the string a_1 to $\mathcal{B}_2$, along with the committed bit d. $\mathcal{B}_2$ checks that the last bit of a_1 is received outside of the future light cone of the beginning of the protocol. If this is the case, $\mathcal{B}_2$ communicates a_1 and d to $\mathcal{B}_1$ through an authenticated channel. Finally, $\mathcal{B}_1$ verifies that $y_1 \oplus a_1 = d \cdot x_1$ and accepts the commitment. If the relativistic constraint is not respected, or if $\mathcal{B}_1$'s verification fails, the protocol aborts.

In the multiround protocol, $\mathcal{A}_1$ and $\mathcal{A}_2$ successively sustain the commitment until the last round. All rounds (except for the first and the last) proceed as follows. Let us consider the kth round, with k even (odd rounds are similar). Between rounds k and $k-2$, the string x_k is loaded in the memory of $\mathcal{B}_2$'s FPGA, and strings a_{k-1} and a_k are loaded in $\mathcal{A}_2$'s FPGA. At time $t_k = t_1 + (k-1)\Delta t$, $\mathcal{B}_2$ communicates x_k through the optical link. Then $\mathcal{A}_2$ sustains the commitment by computing y_k with the FPGA and sending it to $\mathcal{B}_2$. The time between the communication of x_k and the reception of y_k is 6.1 μs. $\mathcal{B}_2$ checks to see that the reception of y_k is outside of the future light cone of the beginning of the communication between $\mathcal{B}_1$ to $\mathcal{A}_1$ that happened in round $k-1$. We used $\Delta t = 400\ \mu$s (see Fig. 1), which is 37 μs shorter than the light-speed separation between the Berne and Geneva locations. Considering the 6.1 μs, the absolute inaccuracies of the GPS clock (≤ 150 ns), and the tolerance in the fluctuations of the synchronization signals (≤ 24 ns), the round is completed $\approx$30.7 μs before the relativistic constraint expires. In the final $(m+1)$th round, $\mathcal{A}_1$ (or $\mathcal{A}_2$) opens the commitment at time t_{m+1} by sending the string a_{m+1} along with the committed bit d. To verify the commitment, $\mathcal{B}_2$ sends to $\mathcal{B}_1$ all of the strings communicated by $\mathcal{A}_2$ through an authenticated channel. $\mathcal{B}_1$ then checks to see if the commitment should be accepted as outlined above. Authentication is based on an information-theoretic secure message-authenticator code which consists of a combination of polynomial hashing and a strongly universal family of hash functions [27].

In the multiround scheme, we aimed to maximize the number of rounds with a reasonable value for the security parameter ε. The limit of $n = 512$ bits and $m + 1 = 6$ rounds was ultimately set by the performance that we could achieve with the FPGA at our disposal. This yields a security parameter of $\varepsilon \approx 2.3 \times 10^{-10}$. Using these parameters, we realized a commitment of 2 ms duration, which extends beyond the 437 μs limit of the two-round protocol. Because synchronizing rounds over longer durations is a simple task for our hardware, it is straightforward to achieve significantly longer commitment times using more distant agents. For example, 150 ms could be easily achieved using Geneva and Singapore as the locations (these locations were used in our previous demonstration of quantum-relativistic bit commitment [19]), while 212 ms could be achieved using antipodal locations on Earth.

Summary.—We have shown that classical relativistic protocols allow us to implement information-theoretically secure commitment schemes in a straightforward fashion.

The commitment scheme we implemented belongs to the class of timed commitments, i.e., commitments that expire after a certain period of time. Even though they cannot be used to implement primitives whose security is required to hold forever (e.g., oblivious transfer), they are known to have other important applications, e.g., contract signing, honesty-preserving auctions, and secure voting [2,3] (see also Appendix A).

For the sBGKW scheme we obtain an explicit, quantitative security bound by making a connection to a nonlocal game that was analyzed previously. We also propose a multiround scheme which is secure against classical adversaries. We note that the number of rounds that we implemented here could have been higher using better optimized hardware. However, the scaling of the security bound with the number of rounds (1) prohibits a much larger number of rounds. An important challenge is therefore to find a multiround protocol whose security exhibits better scaling with the number of rounds or, ideally, no dependence at all. This would allow us to obtain longer (or maybe even arbitrarily long) commitments while only using simple, commercially available digital devices.

We thank Mohammad Bavarian, Gilles Brassard, Iordanis Kerenidis, Raghav Kulkarni, Troy Lee, Laura Mančinska, Miklos Santha, and Sarvagya Upadhyay for the useful discussions. J. K. especially thanks Igor Shparlinski for sharing his ideas about Proposition B.2 of the SM [23] and subsequent discussions. We thank André Stefanov and Daniel Weber for helping to install the setup in Berne. J. K., M. T., and S. W. are funded by the Ministry of Education (MOE) and National Research Foundation Singapore, as well as MOE Tier 3 grant "Random numbers from quantum processes" (Grant No. MOE2012-T3-1-009). Financial support is provided by the Swiss NCCR QSIT. T. L. is the first experimental author and J. K. is the first theoretical author.

[1] M. Blum, "Coin Flipping by Telephone," in *Advances in Cryptology: A Report on CRYPTO 81* (International Association for Cryptologic Research, Santa Barbara, California, USA, 1981), pp. 11–15, see http://www.iacr.org/cryptodb/data/paper.php?pubkey=917.
[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. Boneh and M. Naor, in *Proceedings of the 20th Annual International Cryptology Conference (CRYPTO 2000), Santa Barbara, CA, 2000*, Lecture Notes in Computer Science Vol. 1880 (Springer-Verlag, Berlin, 2000), p. 236254.
[4] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
[5] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
[6] G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner, Phys. Rev. A **76**, 032328 (2007).
[7] S. Winkler, M. Tomamichel, S. Hengl, and R. Renner, Phys. Rev. Lett. **107**, 090502 (2011).
[8] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, in *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science, Pittsburgh, PA, 2005* (IEEE, New York, 2005), p. 449.
[9] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, in *Proceedings of the 27th Annual International Cryptology Conference (CRYPTO 2007), Santa Barbara, CA, 2007* (Springer-Verlag, Berlin, 2007), p. 360.
[10] S. Wehner, C. Schaffner, and B. M. Terhal, Phys. Rev. Lett. **100**, 220502 (2008).
[11] R. König, S. Wehner, and J. Wullschleger, IEEE Trans. Inf. Theory **58**, 1962 (2012).
[12] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Widgerson, in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC 1988), Chicago, 1988* (ACM Press, New York, 1988), p. 113.
[13] C. Crépeau *et al.*, Lect. Notes Comput. Sci. **7073**, 407 (2011).
[14] A. Kent, Phys. Rev. Lett. **83**, 1447 (1999).
[15] A. Kent, New J. Phys. **13**, 113015 (2011).
[16] A. Kent, Phys. Rev. Lett. **109**, 130501 (2012).
[17] J. Kaniewski, M. Tomamichel, E. Hänggi, and S. Wehner, IEEE Trans. Inf. Theory **59**, 4687 (2013).
[18] S. Croke and A. Kent, Phys. Rev. A **86**, 052309 (2012).
[19] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden, Phys. Rev. Lett. **111**, 180504 (2013).
[20] 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, T.-Y. Chen, C.-Z. Peng, Q. Zhang, A. Cabello, and J.-W. Pan, Phys. Rev. Lett. **112**, 010504 (2014).
[21] A. Kent, J. Cryptol. **18**, 313 (2005).
[22] J. Sikora, A. Chailloux, and I. Kerenidis, Phys. Rev. A **89**, 022334 (2014).
[23] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.115.030502, for the detailed security analysis and few remarks about the practical interests of a relativistic bit commitment, which includes Refs. [24–26].
[24] H. Buhrman and S. Massar, Phys. Rev. A **72**, 052103 (2005).
[25] M. Bavarian and P. W. Shor, Information causality, Szemerédi-Trotter and algebraic variants of CHSH, *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science* (ACM, New York, USA, 2015), pp. 123–132.
[26] J. Ford and A. Gál, Comput. Complex. **22**, 595 (2013).
[27] J. Carter and M. N. Wegman, J. Comput. Syst. Sci. **18**, 143 (1979).