Arbitrarily Long Relativistic Bit Commitment

Kaushik Chakraborty, André Chailloux, Anthony Leverrier

Arbitrarily long relativistic bit commitment

Kaushik Chakraborty, André Chailloux, Anthony Leverrier
Inria, EPI SECRET, B.P. 105, 78153 Le Chesnay Cedex, France

We consider the recent relativistic bit commitment protocol introduced by Lunghi *et al* [*Phys. Rev. Lett.* 2015] and present a new security analysis against classical attacks. In particular, while the initial complexity of the protocol scaled double-exponentially with the commitment time, our analysis shows that the correct dependence is only linear. This has dramatic implications in terms of implementation: in particular, the commitment time can easily be made arbitrarily long, by only requiring both parties to communicate classically and perform efficient classical computation.

Over the last decades, which witnessed the rapid expansion of quantum information, a new trend has developed: trying to obtain security guarantees based solely on the laws of physics. Perhaps the most compelling example is quantum key distribution [1, 2] where two distant parties can exploit quantum theory to extract unconditionally secure keys provided that they have access to an untrusted quantum channel and an authenticated classical channel. However, many cryptographic applications cannot be obtained only with secure key distribution. One important example is two-party cryptography, which deals with the setting where Alice and Bob want to perform a cryptographic task but do not trust each other. This is in contrast with key distribution where Alice and Bob cooperate and fight against a possible eavesdropper.

Two-party cryptography has numerous applications, ranging from authentication to distributed cryptography in the cloud. These protocols are usually separated into building blocks, called *primitives*. One of the most studied primitives is *bit commitment*, which often gives a strong indication of whether two-party cryptography is possible or not in a given model of security. For example, many constructions of bit commitment protocols are secure under computational assumptions [3–6]. It is then natural to ask whether quantum theory can provide security for bit commitment. A general no-go theorem was proved in 1996 by Mayers and Lo-Chau [7, 8]. Several attempts were made to circumvent this impossibility result by limiting the storage possibilities of the cheating party [9, 10]. An alternative approach to obtain secure primitives, pioneered by Kent [11], consists in combining quantum theory with special relativity, more precisely with the physical principle that information cannot propagate faster than the speed of light. This has opened the way to new, secure, bit commitment protocols [12–15], which have been recently implemented [16, 17]. In these protocols, both parties has several agents located far from each other, but each one standing close to an agent of the opposing party. The protocols then work by carefully synchronizing the action of each agent in such a way that the agents of a cheating party do not have the time to coordinate and adapt their strategy on the fly. A main caveat, however, is that the commitment time is not arbitrarily long in general but depends critically on the physical distance between the agents or on the number of agents involved.

A major open question of the field is therefore to design a secure practical bit commitment protocol, for which the commitment time can be increased arbitrarily at a reasonable cost in terms of implementation complexity. In this paper, we examine a protocol due to Lunghi *et al.* [18], which is itself adapted from an earlier proposal of Simard [19]. In their recent breakthrough paper, Lunghi *et al.* showed that it was possible to extend the commitment time by using a multi round generalization of the Simard protocol, and established its security against classical adversaries. Unfortunately, the required resources scale double exponentially with the commitment time, making the protocol impractical for realistic applications. For instance, with the optimal configuration on Earth (meaning that each party has agents occupying antipodal locations on Earth), the commitment time is limited to less than a second. Here, we provide a new security analysis establishing that the dependence is in fact linear, provided that the dishonest player is classical. This implies that arbitrary long commitment times can be achieved even if both parties are only a few kilometers apart. We first present the relativistic bit commitment scheme studied by Lunghi *et al.* and we will then establish its security.

The Lunghi *et al.* protocol.— We first recall the protocol as well as the security definitions used and timing constraints. Both players, Alice and Bob, have agents $\mathcal{A}_1, \mathcal{A}_2$ and $\mathcal{B}_1, \mathcal{B}_2$ present at two spatial locations 1 and 2. Let us consider the case where Alice makes the commitment. The protocol (followed by honest players) consists of 4 phases: preparation, commit, sustain and reveal. The sustain phase is itself composed of many rounds, and each such round involves a pair of agents (alternating between locations 1 and 2) referred to as the active players. Overall the bit commitment protocol goes as follows.

1. *Preparation phase*: $\mathcal{A}_1, \mathcal{A}_2$ (resp. $\mathcal{B}_1, \mathcal{B}_2$) share k random numbers $a_1, \ldots, a_k$ (resp. $b_1, \ldots, b_k$) $\in \mathbb{F}_q$, for even k. Here, q is a prime power p^n for some prime p and $\mathbb{F}_q$ refers to the Galois field of order q.

2. *Commit phase*: $\mathcal{B}_1$ sends b_1 to $\mathcal{A}_1$, who returns $y_1 = a_1 + (d * b_1)$ where $d \in \{0, 1\}$ is the committed bit.

3. *Sustain phase*: at round i, active Bob sends $b_i \in \mathbb{F}_q$ to active Alice, who returns $y_i = a_i + (a_{i-1} * b_i)$.

4. *Reveal phase*: $\mathcal{A}_1$ reveals d and a_k to $\mathcal{B}_1$. $\mathcal{B}_1$ checks that $a_k = y_k + (a_{k-1} * b_k)$.

Here, $+$ and $*$ refer to the field addition and multiplication in $\mathbb{F}_q$.

Security definition.— We follow the definitions of Ref. [18]. The security requirements differ in the case of honest Alice and honest Bob. In the former case, Bob should not be able to guess the committed value right before the reveal phase. The protocol should therefore be *hiding*, and it will actually be perfectly hiding here, meaning that Bob cannot guess the committed bit value better than with a random guess. Security for honest Bob is defined differently: the protocol should be *binding*, meaning that Alice should not be able to decide the value of the committed bit after the commit phase. We follow the standard definition for bit commitment (also used in [18]). Let p_d the probability that the Alice successfully reveals bit value d. We say that the protocol is ε-binding if $p_0 + p_1 \leq 1 + \varepsilon$.

Timing constraints for the protocol.— The two pairs $(\mathcal{A}_1, \mathcal{B}_1)$ and $(\mathcal{A}_2, \mathcal{B}_2)$ are at a certain distance D (see Fig. 1). At each round j, there is an *active* (Alice, Bob) pair that performs the protocol while the other, *passive*, pair waits. At the end of round j, they switch roles and perform round $j+1$.

We require that round j finishes before any information about b_{j-1} reaches the other Alice. For any j, we therefore have the following : active Alice has no information about b_{j-1}. This means that y_j is independent of b_{j-1}. This will be crucial in order to show security of the protocol.

One important thing to notice is that d, the bit Alice wants to reveal can be decided just after the commit phase. Therefore, y_1 is independent of d but all the other messages $y_2, \ldots, y_k$ can depend on d.

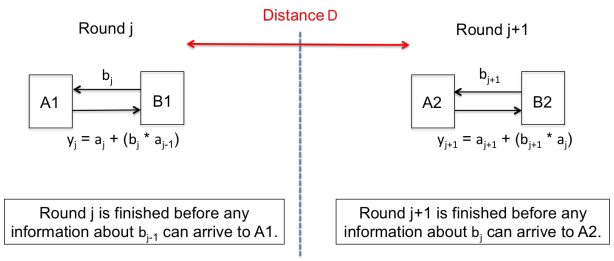

Figure 1: Description of Rounds j and $j+1$ of the bit commitment protocol. Both rounds take place at spatial locations separated by a distance D.

Our result.— Our main contribution is to present an improved security proof for this protocol. In particular, this allows for implementations of this protocol that last for an (almost) arbitrary amount of time while the previous implementations were only secure for (much less than) a second [18].

In order to prove the security of the protocol, we present an inductive argument on the number of rounds of the protocol and show that at each round, the cheating parameter for Alice increases by at most $2^{-(N-1)/2}$, where N is the number of transmitted bits per round. Interestingly, the proof involves the study of CHSH_q, which is a generalization of the CHSH game in the field $\mathbb{F}_q$. Lunghi *et al.* also studied an extension of the CHSH_q game, which they called "Number on the Forehead game". However, their security proof quickly becomes inefficient as the number of rounds increases.

The CHSH_q game.— A crucial tool of our security proof is the analysis of the CHSH_q game introduced by Buhrman and Massar [20]. This game is a natural generalization of the CHSH game to the field $\mathbb{F}_q$, where two non-communicating parties, Alice and Bob, are each given an input x and y chosen uniformly at random from $\mathbb{F}_q$, and must output two numbers $a, b \in \mathbb{F}_q$. They win the game whenever the condition $a+b = x*y$ is satisfied. The CHSH_q game has been much less studied in the literature [18, 20, 21] than its $q = 2$ variant (see [22] for a recent review on nonlocality). A recent result by Bravarian and Shor [23] establishes rather tight bounds on the classical and quantum values of the CHSH_q game. In particular, for prime or odd power of prime q , the classical and quantum values, ω and ω^*, of the game, corresponding respectively to the maximum winning probabilities for players sharing randomness or given access to a bipartite entangled state, satisfy:

$$\omega(\mathrm{CHSH}_q) = O(q^{-1/2-\varepsilon_0}),\ \omega^*(\mathrm{CHSH}_q) \leq \frac{q-1}{q}\frac{1}{\sqrt{q}} + \frac{1}{q},$$

for some absolute constant $\varepsilon_0 > 0$.

These results hold only for a uniform input distribution. In order to use our inductive technique, we need to bound the value of this game for unbalanced inputs. It appears that the result of Bavarian and Shor doesn't easily extend to this setting. We therefore developed new proof techniques that are based on using non-signaling constraints for the study of classical strategies.

Let us consider a family of games, denoted by $\mathrm{CHSH}_q(p)$, where games are parametrized by the probability distribution $\{p_x\}_{x\in\mathbb{F}_q}$ for Alice's input x satisfying the constraint $\max_x p_x \leq p$. For these games, Bob's input distribution is uniform over $\mathbb{F}_q$. In particular, $\mathrm{CHSH}_q(1/q) = \{\mathrm{CHSH}_q\}$. The special case with $q = 2$ was considered in [21] where the following results are proved:

$$\omega(\mathrm{CHSH}_2(p)) = (1+p)/2,$$
$$\omega^*(\mathrm{CHSH}_2(p)) \leq (1+\sqrt{p^2+(1-p)^2})/2.$$

Note that for $q = 2$, Alice's input distribution is entirely determined by the value of p. In order to prove upper bounds on the value of games in $\mathrm{CHSH}_q(p)$, we show that if Alice and Bob can win such a game with high probability then Alice has a method to obtain some information about Bob's input, something that is prohibited by the

non-signaling principle. This technique doesn't directly extend to the quantum setting because Alice's method requires her to perform her game strategy for different inputs, which could disturb the underlying shared entangled state.

Our main technical result is an upper bound on the classical value for games in $\mathrm{CHSH}_q(p)$.

Lemma 1. *For any game $G \in \mathrm{CHSH}_q(p)$, we have*

$$\omega(G) \leq p + \sqrt{\frac{2}{q}}. \tag{1}$$

Proof. Fix a game $G \in \mathrm{CHSH}_q(p)$. As usual, the classical value of the game can always be achieved with a deterministic strategy, meaning that without loss of generality, Alice and Bob's strategies can be modeled by functions f and g, namely: $a = f(x)$ and $b = g(y)$. Define the variable r_x^y equal to 1 if $f(x) + g(y) = x * y$ and 0 otherwise.

Our proof is by contradiction: if $\omega(G)$ is too large, then Alice could use her box to obtain some information about y, which is prohibited by non signaling. More precisely, consider the following strategy for Alice: pick a random pair of distinct inputs x, x' according to the distribution $\{p\}_{x\in\mathbb{F}_q}$, i.e. with probability $p_x p'_x/d$ where $d = \sum_{x\neq x'} p_x p'_x$, and output the guess $\hat{y}$ for y defined by $\hat{y} = (f(x) - f(x')) * (x - x')^{-1}$. Denote by S_y the probability of correctly guessing the value y. Non signaling imposes that $\mathbb{E}_y[S_y] = 1/q$, since the value y is uniformly distributed in $\mathbb{F}_q$.

On the other hand, we note that if the game G is won for both inputs (x, y) and (x', y), then Alice's strategy outputs the correct value for y. Indeed, winning the game implies that $f(x)-f(x') = (x-x')*y$ and therefore $\hat{y} = y$. One immediately obtains a lower bound on S_y:

$$S_y \geq \frac{1}{d} \sum_{x\neq x'} p_x r_x^y p'_x r_{x'}^y \geq \sum_{x\neq x'} p_x r_x^y p'_x r_{x'}^y.$$

Consider the quantity $\omega^y = \sum_x p_x r_x^y$. It satisfies:

$$(\omega^y)^2 \leq \sum_x p_x^2 (r_x^y)^2 + 2S_y = \sum_x (p_x)^2 r_x^y + 2S_y \leq p\omega^y + 2s_y,$$

where we used that $(p_x)^2 \leq (\max_x\{p_x\})\, p_x \leq p p_x$. This implies that

$$\omega^y \leq \frac{1}{2}\left(p + \sqrt{p^2 + 8S_y}\right) \leq p + \sqrt{2S_y},$$

where the last inequality results from the concavity of the square-root function.

Finally, $\omega(G) = \mathbb{E}_y[\omega^y]$ by definition, and therefore:

$$\omega(G) \leq p + 2\mathbb{E}_y[\sqrt{S_y}] \leq p + \sqrt{2}\sqrt{\mathbb{E}_y[S_y]} \leq p + \sqrt{2/q},$$

which concludes the proof. □

Security of the protocol.— The perfect hiding property of this protocol has already been discussed in [18]. Indeed, at any point before the reveal phase, the Bobs have no information about the committed bit d. Our main contribution is the following binding property of this protocol.

Theorem 1. *This relativistic bit commitment scheme is ε-binding with $\varepsilon \leq 2k\sqrt{\frac{2}{q}}$ where k is the number of rounds used in the protocol.*

Proof. We present here the main elements of the proof. The technical details can be found in the Appendix. Let us fix a cheating strategy for Alice, which consists of the messages y_j that the agents will send depending on the current history and the bit d she wants to decommit to. During the reveal phase, Alice successfully reveals d if $\mathcal{A}_1$ sends the correct a_k to Bob. For a fixed cheating strategy, a_k is a function of $d, b_1, \ldots, b_k$. However, during the reveal phase, $\mathcal{A}_1$ has no information about b_k. Therefore, $\mathcal{A}_1$ will not be able to reveal a_k if it has too much dependence in b_k on average on d . We show that this is indeed the case.

Let P_j^d the maximal probability that the passive players guesses a_j, given d. We have by definition

$$P_k^0 + P_k^1 = 1 + \varepsilon.$$

In order to prove our statement, we show the following:

- $P_1^0 + P_1^1 \leq 1 + 2\sqrt{\frac{2}{q}}$.
- For any d and j, $P_j^d \leq P_{j-1}^d + \sqrt{\frac{2}{q}}$.

To prove the first point, the idea is to reduce $\mathcal{A}_2$'s strategy for guessing a_1 into a strategy for $\mathrm{CHSH}_q(1/2)$. $\mathcal{A}_1$ receives b_1 and outputs y_1 which is independent of d. $\mathcal{A}_2$ knows d and outputs a_1. $\mathcal{A}_2$ outputs the correct a_1 when $a_1 + y_1 = d * b_1$. For an average d, this can happen with probability at most $\mathrm{CHSH}_q(1/2) \leq \frac{1}{2} + \sqrt{\frac{2}{q}}$. Therefore, we have

$$\frac{1}{2}\left(P_1^0 + P_1^1\right) \leq \mathrm{CHSH}_q(1/2) \leq \frac{1}{2} + \sqrt{\frac{2}{q}}$$

which gives the desired result.

Similarly, fix a round j and d. We can reduce passive Alice's strategy for guessing a_j to a strategy for winning $\mathrm{CHSH}_q(P_{j-1}^d)$. Indeed, active Alice knows b_j and outputs y_j. Passive Alice knows a_{j-1} and outputs a guess a_j. She outputs the correct value if and only if $a_j + y_j = b_j * a_{j-1}$.

This corresponds to an instance of CHSH_q where $b_j \in \mathbb{F}_q$ is random and where active Alice (we consider here active Alice at round j, which is the passive Alice at round $j-1$) can guess a_{j-1} with probability P_{j-1}^d. This means that we can reduce passive Alice's strategy for guessing a_j to a strategy for winning a certain game in $\mathrm{CHSH}_q(P_{j-1}^d)$. Using Proposition1 proven in the supplemental material,

we obtain $P_j^d \leq P_{j-1}^d + \sqrt{\frac{2}{q}}$. Putting all this together, we can conclude that $P_k^0 + P_k^1 = 1 + 2k\sqrt{\frac{2}{q}}$. □

Experimental perspectives and open questions.— Let us discuss the security of the protocol in realistic conditions. Theorem 1 shows that $\varepsilon\sqrt{q/8}$ rounds can be performed for a given level of security ε. In particular, if the distance between $\mathcal{A}_1/\mathcal{B}_1$ and $\mathcal{A}_2/\mathcal{B}_2$ is D, then the commitment can be sustained for a time

$$T = (D/c)\ \varepsilon\sqrt{q/8},$$

where c is the speed of light. In particular, provided that $q \gg 1/\varepsilon^2$, the commitment time can be made arbitrary long. For instance, taking 128 bits of security, i.e. $\varepsilon = 2^{-128}$ and $q = 2^{350}$ gives $T \approx 5 \cdot 10^{13}(D/c)$, that is approximately 200 years for a distance $d = 100$ km. In this example, the messages sent at each round only consist of 350 bits.

It is also possible to reduce the distance between $\mathcal{A}_1/\mathcal{B}_1$ and $\mathcal{A}_2/\mathcal{B}_2$, at the condition that both the computation time and the communication time between $\mathcal{A}_i$ and $\mathcal{B}_i$ remains negligible compared to D/c. This is necessary to enforce the non-signaling condition of the CHSH_q game. For instance, if the computation time is on the order of the microsecond, then the distance D should be at least 300 meters.

Let us conclude by mentioning a few open questions. Certainly the most pressing one concerns the security of the protocol against quantum adversaries. A first step in that direction would be to obtain tight upper bounds on the entangled value ω^* of games in $\mathrm{CHSH}_q(p)$. Another outstanding problem is whether the bit-commitment protocol of [18] can be used to obtain a protocol for Oblivious-Transfer [24]. In particular, this would pave the way for arbitrary two-party cryptography with security based on the non-signaling principle. Finally, it would be particularly interesting to understand whether 2 agents are indeed necessary for each player, or whether the second agent could for instance be replaced by assuming that the spatial positions of Alice and Bob are known.

Note added.— In an independent and concurrent work, Fehr and Fillinger [25] proved a general composition theorem for two-prover commitments which implies a similar bound on the security of the Lunghi *et al.* protocol than the one derived here.

[1] C. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing **175** (1984).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009), URL `http://link.aps.org/doi/10.1103/RevModPhys.81.1301`.

[3] G. Brassard, D. Chaum, and C. Crépeau, Journal of Computer and System Sciences **37**, 156 (1988).

[4] M. Naor, Journal of Cryptology **4**, 151 (1991).

[5] S. Halevi and S. Micali, in *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings* (1996), pp. 201–215, URL `http://dx.doi.org/10.1007/3-540-68697-5_16`.

[6] S. Halevi, J. Cryptol. **12**, 77 (1999), ISSN 0933-2790, URL `http://dx.doi.org/10.1007/PL00003821`.

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

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

[9] I. B. Damgard, S. Fehr, L. Salvail, and C. Schaffner, SIAM J. Comput. **37**, 1865 (2008), ISSN 0097-5397.

[10] S. Wehner, C. Schaffner, and B. M. Terhal, Phys. Rev. Lett. **100**, 220502 (2008).

[11] A. Kent, Phys. Rev. Lett. **83**, 1447 (1999), URL `http://link.aps.org/doi/10.1103/PhysRevLett.83.1447`.

[12] A. Kent, New Journal of Physics **13**, 113015 (2011).

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

[14] A. Kent, Phys. Rev. Lett. **109**, 130501 (2012), URL `http://link.aps.org/doi/10.1103/PhysRevLett.109.130501`.

[15] J. Kaniewski, M. Tomamichel, E. Hanggi, and S. Wehner, Information Theory, IEEE Transactions on **59**, 4687 (2013).

[16] 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), URL `http://link.aps.org/doi/10.1103/PhysRevLett.111.180504`.

[17] 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, et al., Phys. Rev. Lett. **112**, 010504 (2014), URL `http://link.aps.org/doi/10.1103/PhysRevLett.112.010504`.

[18] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden, Phys. Rev. Lett. **115**, 030502 (2015), URL `http://link.aps.org/doi/10.1103/PhysRevLett.115.030502`.

[19] J.-R. Simard, Master's thesis, McGill University (2007).

[20] H. Buhrman and S. Massar, Phys. Rev. A **72**, 052103 (2005), URL `http://link.aps.org/doi/10.1103/PhysRevA.72.052103`.

[21] T. Lawson, N. Linden, and S. Popescu, arXiv preprint arXiv:1011.6245 (2010).

[22] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).

[23] M. Bavarian and P. W. Shor, in *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science* (ACM, New York, NY, USA, 2015), ITCS '15, pp. 123–132, ISBN 978-1-4503-3333-7, URL `http://doi.acm.org/10.1145/2688073.2688112`.

[24] J. Kilian, in *STOC '88: Proceedings of the twentieth annual ACM symposium on Theory of computing* (ACM Press, New York, NY, USA, 1988), pp. 20–31, ISBN 0-89791-264-0.

[25] S. Fehr and M. Fillinger, arXiv preprint arXiv:1507.00240v1 (2015).