Quantum nonlocality as the route for ever-lasting unconditionally secure bit commitment

Gláucia Murta,1, * Marcelo Terra Cunha,2, † and Adán Cabello3, 4, ‡

1Departamento de Física, Universidade Federal de Minas Gerais, Caixa Postal 702, 30123-970, Belo Horizonte, MG, Brazil
2Departamento de Matemática, Universidade Federal de Minas Gerais, Caixa Postal 702, 30123-970, Belo Horizonte, MG, Brazil
3Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain
4Universidade Federal de Minas Gerais, Caixa Postal 702, 30123-970, Belo Horizonte, MG, Brazil

(Dated: May 7, 2014)

We present a bit commitment protocol based on quantum nonlocality that seems to bring everlasting unconditional security. Although security is not rigorously proved, physical arguments and numerical simulations support this conclusion. The key point is that the proof of the commitment is forced to become classical data uncorrelated with anything else. This allows us to circumvent previous impossibility proofs in which it is assumed that classical data can be replaced by quantum data that may be entangled with the committer. The proposed protocol also recovers two features missing in recent relativistic quantum bit commitment protocols: (i) the committer can decide if and when she wants to reveal the commitment and (ii) the security of the commitment lasts for arbitrary long time.

PACS numbers: 03.65.Ud, 03.67.Dd, 42.50.Xa

Introduction.—Bit commitment (BC) constitutes the building block of a wide range of cryptographic tasks, including distant coin flipping [1], zero-knowledge proofs [2], oblivious transfer [3], and secure multi-party computation [4]. The BC scenario involves two mutually distrustful parties, Alice and Bob. Alice (the committer) has to carry out an action that commits her to a particular bit value and provide a proof of this action to Bob (the receiver). The purposes of a BC protocol are that, once committed to a bit value, Alice cannot change it (i.e., the protocol is binding) and Bob cannot learn anything about it (i.e., the protocol is concealing) until and if Alice decides to reveal it. A BC protocol is secure if it is simultaneously binding and concealing, and it is unconditionally secure if it is secure against any cheater, either Alice or Bob, even if they have unlimited computational power.

A BC protocol has three phases. The commitment phase, in which Alice and Bob communicate. At the end of this phase, Alice should be committed to a bit value. The holding phase, where Alice and Bob do not interact for a while. In this phase, Bob may attempt to read the commitment and Alice may try to prepare a cheat. Finally, the revealing phase, that starts if and when Alice decides to reveal her commitment, allowing Bob to check its authenticity.

Unconditionally secure BC is impossible with classical resources only. The classical BC protocols are based on “one way” functions and on presumed limitations of the computational power of Bob. In this Letter we propose a protocol where quantum nonlocality provides such limitation, suggesting unconditional security.

While quantum key distribution became a success [5, 6], the question of whether quantum theory could provide unconditionally secure BC has been always controversial. Initial attempts to construct a quantum BC protocol (see, e.g., [5, 7]) were finally discarded by the impossibility proofs of Lo and Chau [8] and Mayers [9].

By taking advantage of the nonsignalling constraint imposed by Minkowski space-time, Kent showed that it is possible to guarantee security [10, 11]. The idea behind these relativistic protocols is to split each party into multiple agents that cannot communicate with each other, at least in some steps of the protocol. The main point is that, even if the agents collectively have enough information to cheat, no single agent can cheat alone, and thus the impossibility argument is avoided [12]. In Ref. [10], Kent proposes a quantum BC protocol where security is guaranteed by spacelike separation between agents of each party. Later, Kent proposed another protocol [11] which requires less resources. These ideas have recently been experimentally implemented [13, 14].

Despite the success of these so called “relativistic” protocols, one important restriction of these schemes is that unconditional security is guaranteed only for a finite period of time. A previous protocol that could last for as long as the parties desire was also proposed by Kent [15]. However, this protocol requires the parties to keep communicating continuously in order to sustain the commitment.

Here we address the question of whether quantum nonlocality, a single quantum resource that naturally includes both ingredients in a relativistic protocol (namely, quantum measurements in a scenario in which communication is restricted by relativistic causality), can be enough for unconditionally secure BC.
We present a protocol that is conjectured to give the positive answer to this question. More interestingly, this protocol allows us to identify which assumptions in previous "impossibility proofs" are not necessarily satisfied.

In a nutshell, the protocol introduced here is based on the following ideas. During the commitment phase, Alice (the committer) and Bob (the receiver) are close to each other. Alice has one trusted agent and Bob has another one. Both agents are close to each other and spacelike separated from Alice and Bob. The proof of Alice’s commitment is an element of a subset of the group $S_n$ of all permutations of $n$ elements. The commitment phase starts with this permutation applied to an entangled pure state that Alice and her agent transfer to Bob and his agent. Bob is forced to perform local measurements on these particles. This makes the proof of the commitment to be equal encoded at random classical data that remains hidden by statistical security even when Bob and his agent come together. It is this "classicalization" what makes the protocol immune to Lo, Chau, and Mayers’ impossibility arguments [8, 9].

Security is provided by the fact that there does not exist a local model capable of producing the correlations that Bob and his agent observe and the only quantum state capable of generating, for sure, such results is the specific permutation applied by Alice to a set of maximally entangled bipartite states, thus preventing that Alice and her agent can successfully cheat.

**Fully nonlocal quantum correlations.**—One important ingredient in our protocol is the existence of bipartite Bell inequalities in which the maximum quantum mechanical violation equals the algebraic bound. Reaching this bound requires perfect correlations between all the measurements [16, 17].

To introduce these quantum correlations, called fully nonlocal [16], consider two spatially separated parties that we call Bob and Bob’s agent. Each of them can choose randomly one out of three experiments to perform: $B_0, B_1, B_2$ for Bob, and $b_0, b_1, b_2$ for Bob’s agent. Each experiment has four possible outcomes, denoted $++$, $+-$, $-+$, and $--$

For this scenario, we can write the expression

\[
\beta = \langle B_0^{(10)} b_0^{(10)} \rangle + \langle B_0^{(01)} b_1^{(01)} \rangle + \langle B_0^{(11)} b_2^{(10)} \rangle \\
+ \langle B_1^{(10)} b_0^{(01)} \rangle + \langle B_1^{(01)} b_1^{(01)} \rangle + \langle B_1^{(11)} b_2^{(01)} \rangle \\
+ \langle B_2^{(10)} b_0^{(11)} \rangle + \langle B_2^{(01)} b_1^{(11)} \rangle - \langle B_2^{(11)} b_2^{(11)} \rangle,
\]

where $\langle B_1^{(10)} b_0^{(01)} \rangle$ is the mean value of the product of the first bit of the result of measuring $B_1$ by the second bit of the result of $b_0$, $\langle B_2^{(01)} b_1^{(11)} \rangle$ is the mean value of the product of the second bit of the result of measuring $B_2$ by the first and second bits of the result of $b_1$, and analogously for the other terms.

This expression has the following property:

\[
\beta_{\text{LHV}} \leq 7 \leq 9,
\]

where $\leq 7$ indicates that, for any local hidden variable theory, $\beta$ is upper bounded by 7 and $\leq 9$ indicates that, for any theory satisfying nonsignalling, $\beta$ is upper bounded by 9. The interesting point is that, with a particular choice of quantum state and measurements, it is possible to reach the maximum value $\beta = 9$ [17].

For the particular local observables that we will use in the protocol (see [18]), $\beta$ reaches the value 9 for the quantum state $\ket{\xi}$ given by

\[
\ket{\xi} = \ket{\Phi^+}_{12} \otimes \ket{\Phi^+}_{34},
\]

where $\ket{\Phi^+}$ is the following two-qubit maximally entangled state:

\[
\ket{\Phi^+} = \frac{1}{\sqrt{2}} \left( \ket{00} + \ket{11} \right).
\]

Subindexes 12 and 34 remind us that Bob holds qubits 1 and 3, while Bob’s agent holds qubits 2 and 4.

The condition $\beta = 9$ implies that each term in $\beta$ has to be equal to $-1$ or $+1$, depending on the sign with which the corresponding mean value appears in $\beta$. This means that, for any measurements Bob and his agent choose to perform, they obtain a perfectly correlated pair of bits. For example, for maximizing $\beta$ the condition $\langle B_0^{(01)} b_1^{(10)} \rangle = 1$ has to be satisfied. This implies that, if Bob measures $B_0$ and his agent measures $b_1$, then the second bit of Bob’s outcome has to be equal to the first bit of Bob’s agent’s outcome. For clarity, Table I illustrates all Bob’s agent’s possible results for the case Bob had chosen to measure $B_0$. Analogous relations occur for Bob’s other choices of measurements.

| $B_0$ | $b_0$ | $b_1$ | $b_2$ |
|-------|-------|-------|-------|
| $++$  | $++$  | $++$  | $++$  |
| $-+$  | $-+$  | $-+$  | $-+$  |
| $-+$  | $-+$  | $-+$  | $-+$  |
| $++$  | $++$  | $++$  | $++$  |

**TABLE I:** The first column of the table shows the possible results Bob can obtain when the measurement $B_0$ is performed. The next three columns show Bob’s agent’s possible results if they share the state $\ket{\xi}$.

The protocol.—Now we make use of the previously described Bell inequality to introduce the proposed BC protocol. It goes as follows (see Fig. 1):

1. We assume that Alice and her agent share $n$ pairs of particles (qubits or pairs of ququarts) in the entangled state $\ket{\xi}$, and that Alice and Bob agree on an inertial reference frame and two spacelike separated points of space-time, $x_1$ and $x_2$, where the commitment will be made.
2. The commitment phase starts with Alice meeting Bob at point \(x_1\), while Alice’s agent meets Bob’s agent at point \(x_2\).

3. Alice’s agent is supposed to send the particles to Bob’s agent in the same order they were previously arranged, while Alice, who is the responsible for making the commitment, chooses one permutation among a subset \(A_{n,r}\) of the set \(S_n\) of permutations of \(n\) elements, and changes the order of the particles accordingly before sending them to Bob. The permutation chosen by Alice will be the proof of her commitment.

4. For each ququart Bob receives, he is supposed to choose one among three four-outcome measurements to perform, \(B_0\), \(B_1\), and \(B_2\). Analogously Bob’s agent chooses among \(b_0\), \(b_1\), and \(b_2\) to perform.

5. Each time Bob receives one ququart, he has to inform Alice back which was the obtained outcome. In order to certify that Bob is really performing the local measurements on his system, Alice shall randomly insert, among the \(n\) ququarts described above, some particles in pure states known to her and which generate definite answer for some \(B_j\). Then, for each check particle, after Bob informs Alice the outcome she asks him about the measurement performed. It is sufficient to introduce this check between Alice and Bob: Alice’s agent will just deliver the particles to Bob’s agent, who will not provide her with any information. This is the end of the commitment phase.

6. After the commitment, during the holding phase, Alice and Bob as well as their agents can split and do whatever possible with their systems.

7. In the revealing phase, which happens when and if Alice decides to, she reveals to Bob which was the sent permutation.

8. Bob can check with his agent if the unveiled permutation maximally violate the Bell inequality, certifying Alice’s commitment.

The encoding alphabet.—Another main point in our protocol is the use of permutations to encode the bit value.

By construction of the protocol, whenever a permutation fix a system, the (anti-)correlation will be perfect; otherwise, the results are independent. This suggests the following choice of alphabet: Let \(A_{n,r} \subset S_n\) be a maximal random set formed by permutations that obeys:

\[
\sigma_i, \sigma_j \in A_{n,r} \Rightarrow d(\sigma_i, \sigma_j) \geq r, \forall i \neq j, \quad (4)
\]

where \(1 < r \leq n\), and \(d(\cdot,\cdot)\) represents the Hamming distance (number of permuted positions) between two permutations. Therefore, all the possible permutations Alice can choose in the protocol differ from each other by at least \(r\) positions.

The association of each permutation to a bit value is made by the use of a suitably chosen function that uniformly distributes the bit values 0 and 1 over the elements of random subsets of the set \(A_{n,r}\). Parity seems to be a good choice.

Security against Alice.—The maximal violation of the Bell inequality assures that Alice must have been honest in the state sent during the commitment phase, since \(|\xi\rangle\) is the only state that maximally violates the Bell inequality \(\beta \leq 7\), and therefore the only state capable of generating for sure consistent results.

Another possible cheat is that Alice can reveal a wrong permutation. However, since our alphabet is restricted to \(A_{n,r}\), the best she can do is to try to reveal a permutation that is \(r\) positions distant from the original one, which gives her a probability of success bounded by \(2^{-r}\).

The protocol does not prevent Alice from committing to a superposition of bits, but her probabilities of revealing 0 or 1 are fixed during the commitment phase and then it is considered fair [19] (in order to describe the procedure of committing to a superposition we need a more subtle formalism that is out of the scope of this Letter and will be discussed elsewhere, for more discussion about the coherent commitment, see [18]).

Security against Bob.—Bob has no way to cheat while he is spacelike separated from his agent. Since Alice’s
verification in the commitment phase forces Bob to perform the local measurements, after Bob and his agent come together, they still have a very small probability of finding out the commitment, given the large number of permutations consistent with the recorded data. Since the alphabet $A_{n,r}$ is huge (a very simple estimation shows $#A_{n,r} > \frac{2n!}{rn^r}$), the number of permutations consistent with Bob’s data is very large (e.g.: for $n = 100, r = 60$ the number is above a million). In the Supplementary Material [18] we discuss in more detail some estimations and numerical results. However, the delicate point is to guarantee that Bob cannot distinguish the original permutation among the set of consistent permutations. That is, the set of consistent permutations has to have (almost) no structure. Our numerical simulations support that concealing can be reached by suitable choices of $n$ and $r$, but this is still an open point [18].

Quantum state.—In order to show that it is enough to check that Bob performs the local measurements, we analyse the quantum state of the system after the commitment phase, considering that Alice and Bob played their part, but that Bob’s agent can keep his particles for future use.

Denote by $M_{j,o}$ the measurement operator acting on both systems when Bob measures $B_j$ and obtains the outcome $o$, i.e., $M_{0,++} = |00\rangle \langle 00| \otimes I$, ..., $M_{2,--} = |\omega^-\rangle \langle \omega^-| \otimes I$, with the pure states’ choice, $|00\rangle, \ldots, |\omega^-\rangle$, detailed in Supplementary Material [18]. It is important to recognize that $M_{j,o} |\xi\rangle$ is a pure product state, $|\psi_{j,o}\rangle$, which depends on $j$ and $o$. The quantum state of the hole system of $n$ ququarts (discarding the check particles introduced by Alice) after step 5 of the protocol is

$$|\Psi_{\sigma_A}^{(j_k),(o_k)}\rangle = \prod_{k} M_{j_k,o_k}^{(\sigma_A^{-1}(k))} |\xi\rangle \otimes^n,$$  

(5)

where $(o_k)$ is the sequence of outcomes obtained when Bob measured the sequence of observables $(B_{j_k})$ on his particles in the state obtained after Alice applied the permutation $\sigma_A$ to $|\xi\rangle \otimes^n$.

The most important point is that such quantum state strongly depends on $\sigma_A$, $(j_k)$, and $(o_k)$, where the first is unknown to Bob (to make the protocol concealing) and the second is unknown to Alice (to make it binding), while the third is public. The best description of the global quantum state, available to Bob’s agent while space-separated from Bob and Alice is given by

$$\rho_{(j_k),(o_k)} = \sum_{\sigma \in A_{n,r}} p(\sigma, (j_k), (o_k)) \left|\Psi_{(j_k),(o_k)}^{\sigma}\right\rangle \left\langle \Psi_{(j_k),(o_k)}^{\sigma}\right|,$$  

(6a)

where $p(\sigma, (j_k), (o_k))$ denotes this joint probability. In case the protocol is followed this will be

$$p(\sigma, (j_k), (o_k)) = \frac{1}{#A_{n,r}} \frac{1}{3^n} \frac{1}{4^n}.$$  

(6b)

On the other hand, Bob knows $(j_k)$ and $(o_k)$, which makes his best description of the state be

$$\rho_{(j_k),(o_k)}^B = \sum_{\sigma \in A_{n,r}} p(\sigma) \left|\Psi_{(j_k),(o_k)}^{\sigma}\right\rangle \left\langle \Psi_{(j_k),(o_k)}^{\sigma}\right|.$$  

(6c)

This is also the description after Bob and his agent meet.

The von Neumann entropy of these states is generally very high. In case $(j_k)$ is a typical sequence, the scalar product $\left|\Psi_{(j_k),(o_k)}^{\sigma}\right\rangle \left\langle \Psi_{(j_k),(o_k)}^{\sigma}\right|$ is upper-bounded by a decreasing function of the Hamming distance between the two permutations. The choice of $A_{n,r}$ has impact also here. Even more important than this, a state discrimination attack aiming to learn about the permutation is also very ineffective when large $n$ is used, since all permutations which fix equal measurement settings and results will originate the same quantum state; in other words, the same quantum state for Bob’s agent system will be obtained for many different allowed permutations.

Finally, we could consider what Alice knows about such state. Since she is not aware of $(j_k)$, she must describe the system by

$$\rho_{\sigma_A}^{A} = \sum_{(j_k)} p ((j_k)) \left|\Psi_{(j_k),(o_k)}^{\sigma}\right\rangle \left\langle \Psi_{(j_k),(o_k)}^{\sigma}\right|.$$  

(6d)

which has, again, very high entropy.

On the nonapplicability of the impossibility proofs.—There are two impossibility proofs of unconditionally secure BC: the “classical” proof, that shows that it is impossible using classical data, and the Lo-Chau-Mayers proof, that shows that it is also impossible with the help of quantum states. Here we explain how our protocol evades both.

The Lo-Chau-Mayers proof assumes that the proof of Alice’s commitment that is delivered to Bob can always be replaced by a quantum state, nondiscriminable by Bob, which may possibly be only a part of an entangled state with the other part kept by Alice. This allows her to later purify and cheat. A key point in our protocol is to make this impossible. At step 5, Alice’s part of the quantum state is destroyed and forced to produce classical data that cannot be correlated with Alice (otherwise the Bell inequality would not be maximally violated).

This “classicalization” at step 5 certifies that Bob is performing local measurements (instead of collecting quantum states), without giving Alice enough information that she could use to cheat. Alice needs to be sure that the quantum state was destroyed by Bob’s measurement. At the same time, Bob needs to be sure that Alice is not keeping correlated systems that allow her to change the commitment without being discovered. Using a completely quantum description: At first, the quantum state factors between Bob and his agent and the rest of the world (since Bob and his agent share an entangled pure state). Then, as Bob is forced to measure, Bob also
factors out from his agent, and the final quantum state (alone) does not hold enough information to discriminate among many possible permutations equally distributed between the two possible bit values.

After step 5, the data is classical. Why then the classical impossibility argument does not apply? The reason is because each pair of outcomes is perfectly correlated and, together, violate a Bell inequality up to its algebraic maximum. Therefore, no classical (local) model can account for the correlations observed by Bob and his agent. This means that the data where the permutation is encoded after step 5 is unavailable to Alice (given that Bob avoid any leak), since it was not available prior to Bob’s measurements.

This shows that nonlocality and the “classicalization” at step 5 are essential ingredients to escape from previous arguments against the possibility of an unconditionally secure BC and that quantum theory can provide a natural “one way function” that limitates Bob’s power to extract the encoded permutation from the available data which serves to confirm authenticity.

Conclusions.—We have presented a BC protocol based on quantum nonlocality which bypass the two strongest objections against unconditionally secure BC. By imposing a “classicalization” procedure (namely, measurement), we can take benefit from the best of two worlds: data cannot be copied nor hidden since it was generated by quantum randomness, and the proof of the commitment cannot be purified, since it is already encoded in classical form. Even in the absence of a complete proof of security, a virtue of the protocol presented here is to identify an assumption in Lo-Chau-Mayers proofs of impossibility of unconditionally secure BC that is not necessarily satisfied.

In addition, the protocol presented here has the following advantages over relativistic protocols [10, 11]: It requires less agents than Ref. [11], it does not need the transmission of classical or quantum information at nearly the speed of light [10], it does not need to sustain communication during all the phases of the protocol, and, more importantly, the security is not limited to a brief amount of time.

We still cannot claim that our protocol solves the problem of unconditionally secure BC, since we do not have a complete proof of security. We only have a proof of security against a specific list of attacks which include some attacks that break previous protocols (see [18] for more details). Moreover, our proof is based on a conjecture that is only supported by numerical evidence, namely, that concealing is guaranteed by the (conjectured) impossibility of distinguishing the “right” permutation among the many permutations consistent with the randomly generated data, even when Bob and his agent come together (see [18] for more details). However, the observation that there is a way to bypass the two standard objections against unconditionally secure BC opens new perspectives and shows that we can be, for the second time [6], in a situation where quantum nonlocality paves the way for a paradigmatic cryptographic task.

The authors thank M. Curty, R. Drumond, L. Guerini, A. Kent, J.-A. Larsson, M. Pawlowski, and J. van de Graaf for helpful discussion and for pointing some mistakes in previous versions. MTC and AC thank the International Institute of Physics (UFRN – Brazil) for hospitality. This work was supported by the Spanish Ministry of Economy and Competitiveness through Project No. FIS2011-29400, the Brazilian program Science without Borders, the Brazilian National Institute for Science and Technology of Quantum Information, and the Brazilian agencies Capes, CNPq, and Fapemig.
Supplementary material to “Quantum nonlocality as the route for ever-lasting unconditionally secure bit commitment”

Gláucia Murta,1,* Marcelo Terra Cunha,2,† and Adán Cabello3,4,‡

1Departamento de Física, Universidade Federal de Minas Gerais, Caixa Postal 702, 30123-970, Belo Horizonte, MG, Brazil
2Departamento de Matemática, Universidade Federal de Minas Gerais, Caixa Postal 702, 30123-970, Belo Horizonte, MG, Brazil
3Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain
4Universidade Federal de Minas Gerais, Caixa Postal 702, 30123-970, Belo Horizonte, MG, Brazil

(Dated: May 7, 2014)

Here we detail the observables that lead to the maximal violation of the Bell inequality used in the protocol for bit commitment presented in Ref. [1] and discuss the security of this protocol against some specific attacks.

PACS numbers: 03.65.Ud,03.67.Dd,42.50.Xa

The notation used is the one introduced in Ref. [1].

Optimal observables. —The observables that lead to the maximal violation of inequality \(\beta\) for the state \(|\xi\rangle\) are the following:

\[
B_0 = r_+ |00\rangle\langle0| + r_- |01\rangle\langle1| \tag{1a}
\]

\[
B_1 = r_+ |10\rangle\langle+| + r_- |1-\rangle\langle-| \tag{1b}
\]

\[
B_2 = r_+ |\chi^+\rangle\langle\chi^+| + r_- |\chi^-\rangle\langle\chi^-| \tag{1c}
\]

where

\[
|\pm\rangle = \frac{1}{\sqrt{2}} (|0\rangle \pm |1\rangle), \tag{2a}
\]

\[
|\chi^\pm\rangle = \frac{1}{\sqrt{2}} (|0\rangle \pm |1\rangle), \tag{2b}
\]

\[
|\omega^\pm\rangle = \frac{1}{\sqrt{2}} (|1\rangle \pm |0\rangle). \tag{2c}
\]

While:

\[
b_0 = r_+ |0+\rangle\langle0| + r_- |0-\rangle\langle0| \tag{3a}
\]

\[
b_1 = r_+ |1+\rangle\langle1| + r_- |1-\rangle\langle1| \tag{3b}
\]

\[
b_2 = r_+ |\phi^+\rangle\langle\phi^+| + r_- |\phi^-\rangle\langle\phi^-| \tag{3c}
\]

where

\[
|\phi^\pm\rangle = \frac{1}{\sqrt{2}} (|00\rangle \pm |11\rangle), \tag{4a}
\]

\[
|\psi^\mp\rangle = \frac{1}{\sqrt{2}} (|01\rangle \pm |10\rangle). \tag{4b}
\]

Security against Bob’s attacks.—We now present some estimations in order to discuss Bob’s possibilities of discovering Alice’s commitment.

First, by considering a sphere packing’s point of view, we made some estimations of the cardinality of the alphabet \(A_{n,r}\) and the set of permutations consistent with Bob’s results.

Let \(B_{n,\tilde{r}}\) be a ball of radius \(\tilde{r}\) in the set \(S_n\) (i.e., a set of permutations at a distance at most \(\tilde{r}\) from some given permutation). The cardinality of \(B_{n,\tilde{r}}\) is given by

\[
\#B_{n,\tilde{r}} = \sum_{k=0}^{\tilde{r}} \binom{n}{k} C_k, \tag{5a}
\]

where \(C_k\) is the number of chaotic permutations of \(k\) elements, i.e., permutations that do not fix any element:

\[
C_k = k! \sum_{j=0}^{k} \frac{(-1)^j}{j!}. \tag{5b}
\]

Then,

\[
\#B_{n,\tilde{r}} = \sum_{k=0}^{\tilde{r}} \binom{n}{k} C_k, \tag{5c}
\]

We can upper bound the cardinality of \(A_{n,r}\) by

\[
\#A_{n,r} \leq \#S_n / \#B_{n,\lfloor \frac{n}{2}\rfloor}, \tag{6a}
\]

where \([ \bullet \) is the integer floor of \(\bullet\), i.e., the smallest integer greater than or equal to \(\bullet\). Then,

\[
\#A_{n,r} \leq \frac{1}{\sum_{k=0}^{\lfloor \frac{n}{2}\rfloor} \frac{1}{(n-k)!} \sum_{j=0}^{k} \frac{(-1)^j}{j!}}. \tag{6b}
\]

Using this approximation, we can associate a density to the set \(A_{n,r}\):

\[
\varrho_{n,r} = \frac{\#A_{n,r}}{n!} \leq \frac{1}{\#B_{n,\lfloor \frac{n}{2}\rfloor}}. \tag{7}
\]

Now we can estimate the number of elements in \(A_{n,r}\) at distance \(\tilde{r}\) from a fixed permutation \(\sigma_A\).
\[ \# \{ \sigma \in A_{n,r} , \, d(\sigma, \sigma_A) = \tilde{r} \} = \left[ \#B_{n,\tilde{r}} - \#B_{n,\tilde{r}-1} \right] \times \varrho_{n,r} \leq \frac{3n\tilde{r}}{2 \left\lfloor \frac{r-3}{2} \right\rfloor (n-1)^2}. \] (8)

To answer this question, we simulated the sets \( Bob_{n,r} \) for some small values of \( n \) and \( r \). For each consistent permutation \( \sigma \), we calculated the number of permutations in \( Bob_{n,r} \) distant from \( \sigma \) by \( \tilde{r} \) positions, for \( r \leq \tilde{r} \leq n \). We simulated \( Bob_{n,r} \) one thousand times for the case \( n = 10, \, r = 6 \). The average cardinality of the set \( Bob_{n,r} \) is about 8 elements, and even for these small numbers the results obtained look good. In some cases, the most highlighted permutation (meaning the one that has the greatest number of first neighbors) is not the one which Alice is committed to, sometimes we have more than one highlighted permutation, and on average just in 10% of the cases there was just one highlighted permutation and it was the one chosen by Alice (i.e., Bob would succeed in cheating).

With these numerical results for very small values of \( n \) and \( r \), we strongly believe that using larger values we can make the protocol as statistically secure as demanded.

**Security against Alice’s using quantum superpositions.**—In a quantum bit commitment protocol, Alice has the possibility of using a quantum superposition of commitments. Here we discuss what happens in our protocol when Alice uses a superposition of permutations.

The important question to be answered is whether the set \( Bob_{n,r} \) of consistent permutations with Bob and his agent’s results has some structure that allows to highlight the permutation chosen by Alice.

From Bob’s perspective, and assuming that he and his agent had already performed the required measurements, the only remaining attack is to try to obtain, from \( Bob_{n,r} \), the distinguished permutation \( \sigma_A \).

To discard this possibility, we have to consider the Hamming distance between the elements of \( Bob_{n,r} \). More formally: Let \( \sigma_A \) be the permutation Alice has chosen to encode her commitment and consider \( \sigma_C \), another permutation consistent with Bob and his agent’s results, such that \( d(\sigma_C, \sigma_A) = C \). The question to be answered is the following:

\[ \langle \# \{ \sigma \in Bob_{n,r} , \, d(\sigma, \sigma_C) = \tilde{r} \} \rangle \geq \langle \# \{ \sigma \in Bob_{n,r} , \, d(\sigma, \sigma_A) = \tilde{r} \} \rangle, \quad \forall \tilde{r}, \] (11)

where \( \langle \ldots \rangle \) denotes the expected value of the random variable.

When we talk about a specific permutation of \( n \) systems of maximally entangled ququarts, the Hilbert space associated with the whole system is well defined. We can write

\[ \mathcal{H} = (C^4_2 \otimes C^4_2)^n, \] (12)

where \( I \) represents the systems that later will be given to Bob and \( II \) the systems that will be given to Bob’s agent. Here we get a natural order associated with the systems

\[ \mathcal{H} = (C^4_2 \otimes C^4_2)_1 \otimes (C^4_2 \otimes C^4_2)_2 \otimes \cdots \otimes (C^4_2 \otimes C^4_2)_n, \] (13)

Then, by applying a permutation to one of the parties, it can be written as \( \sigma_I \otimes I_{II} \), where \( \sigma_I \) permutes the systems \( I \).

One way of “committing to a superposition” is to take two distinct permutations \( \sigma \) and \( \pi \), promote them to operators acting on \( \mathcal{H} \) as \( \sigma_I \otimes I_{II} \) and \( \pi_I \otimes I_{II} \), and then superposing like \( (c_{\sigma} \sigma_I + c_{\pi} \pi_I) \otimes I_{II} \). Such “non-commitment”, however, presents no advantage for Alice, since the resulting quantum state would generate results that may not be consistent with any of these two permutations.

Analogously, we can obtain lower bounds to the cardinality of the set \( A_{n,r} \):

\[ \# A_{n,r} \geq \frac{\# S_n}{\# B_{n,r}}, \] (9a)

that leads to

\[ \varrho_{n,r} \geq \frac{1}{\# B_{n,r}}. \] (9b)

This allows us to estimate:

\[ \# \{ \sigma \in A_{n,r} , \, d(\sigma, \sigma_A) = \tilde{r} \} \geq \frac{(n-\tilde{r}+1)^{\tilde{r}-r}}{3r}. \] (10)

The number of permutations at distance \( \tilde{r} \) from a fixed permutation, \( \sigma_A \), increases with \( \tilde{r} \).
In the same way, the trick of introducing some ancilla and entangle it with the system by associating different permutation operators to different states of the ancilla will not help, since Alice would not have control on the ancilla’s result, so this case corresponds to commit to a mixture. Such strategy is allowed in bit commitment discussions (and actually cannot be avoided in quantum protocols) since the sum of the probability of successfully unveil 0 plus the probability of successfully unveil 1 is not greater than $1 + \epsilon$, where $\epsilon$ can be made arbitrarily small [2].

The totally quantum description.— As described in Ref. [1], the quantum state of the hole system of $n$ ququarts (discarding the check particles introduced by Alice) after step 5 of the protocol is

$$|\Psi^{\sigma_A}_{(j_k),(o_k)}\rangle = \prod_k M_{j_k,o_k}^{(\sigma^{-1}_A(k))} |\xi\rangle \otimes^n.$$  

(14)

One can now include in such description a register for Alice and a register for Bob’s measurements and outcomes, which would generate the complete description

$$|\Phi^{\sigma_A}_{(j_k),(o_k)}\rangle = |\sigma_A\rangle \langle (j_k) | (o_k) \rangle |\Psi^{\sigma_A}_{(j_k),(o_k)}\rangle,$$  

(15)

where the first register belongs to Alice, second and third to Bob, and the last part is pure product state shared by Bob and his agent, with no participation of Alice’s agent, who has acquired no information during the process.

Such all quantum description helps in two different aspects: one is to recognize, once again, that Lo-Chau-Mayers’s argument does not apply, since Alice’s register is factored from rest of the system. The other is related to committing to a superposition. Now we would have

$$|\Phi^{(\psi)}_{(j_k),(o_k)}\rangle = \alpha |\sigma\rangle \langle (j_k) | (o_k) \rangle |\Psi^{\sigma}_{(j_k),(o_k)}\rangle$$  

$$+ \beta |\pi\rangle \langle (j_k) | (o_k) \rangle |\Psi^{\pi}_{(j_k),(o_k)}\rangle,$$  

(16)

which is an entangled state of Alice’s register consistent with either permutation $\sigma$ or $\pi$ and Bob’s agent state capable of generating data consistent with a proof of the respective permutation. In this case, we can say that Alice resign her right of choosing, but the protocol still works afterwards, in the sense that the Alice’s register for the permutation will read a permutation consistent with the maximal violation of the Bell inequality.

* Electronic address: glaucia@fisica.ufmg.br
† Electronic address: tcunha@mat.ufmg.br
‡ Electronic address: adan@us.es

[1] G. Murta, M. Terra Cunha, and A. Cabello, arXiv:1307.0156.
[2] P. Dumais, D. Mayers, and L. Salvail, in Advances in Cryptology – EUROCRYPT 2000, edited by B. Preneel (Springer, Berlin, 2000), p. 300.