Spacetime-constrained oblivious transfer

Damián Pitalúa-García$	extsuperscript{1,2,}$

$^1$Laboratoire d’Information Quantique, CP 224, Université libre de Bruxelles, Av. F. D. Roosevelt 50, 1050 Brussels, Belgium
$^2$IRIF, CNRS, Université Paris Diderot, Paris, France

(Dated: July 4, 2016)

In 1-out-of-2 oblivious transfer (OT), Alice inputs numbers $x_0, x_1$, Bob inputs a bit $b$ and outputs $x_b$. Secure OT requires that Alice and Bob learn nothing about $b$ and $x_b$, respectively. We define spacetime-constrained oblivious transfer (SCOT) as OT in Minkowski spacetime in which Bob must output $x_b$ within $R_b$, where $R_0$ and $R_1$ are fixed spacelike separated spacetime regions. We show that unconditionally secure SCOT is impossible with classical protocols in Minkowski (or Galilean) spacetime, or with quantum protocols in Galilean spacetime. We describe a quantum SCOT protocol in Minkowski spacetime, and we show it unconditionally secure.

I. INTRODUCTION

Relativistic quantum cryptography$\textsuperscript{[1–28]}$ is a recent branch of physics-based cryptography in which the combined power of quantum physics and relativity is exploited to guarantee security. It opens up possibilities for novel cryptographic tasks that do not have analogues in nonrelativistic settings$\textsuperscript{[2] 1, 11, 12, 14}$. Furthermore, it motivates the investigation of security for tasks that were shown impossible in nonrelativistic quantum scenarios. For example, unconditionally secure protocols for bit commitment$\textsuperscript{[29, 30]}$, ideal coin tossing$\textsuperscript{[31]}$, strong coin tossing with arbitrarily small bias$\textsuperscript{[32, 33]}$, all-or-nothing oblivious transfer$\textsuperscript{[34]}$, 1-out-of-2 oblivious transfer$\textsuperscript{[35]}$, and more general two-party classical computation$\textsuperscript{[2] 32, 33}$ have been shown impossible in nonrelativistic quantum settings. Although these impossibility proofs also apply to relativistic quantum settings for most of these tasks$\textsuperscript{[2] 1, 6, 36}$, they do not apply to bit commitment$\textsuperscript{[1, 3]}$, and ideal and strong coin tossing$\textsuperscript{[2]}$, for which unconditionally secure relativistic protocols have been found$\textsuperscript{[1, 3, 13, 17, 22, 23]}$.

Here we introduce a novel cryptographic task in Minkowski spacetime, which we motivate with the following problem. We consider a particular reference frame $F$ agreed a priori by Alice and Bob. Alice has two passwords $x_0, x_1 \in \{0, 1\}^n$ at the spacetime point $P = (0,0,0,0)$, defined in $F$, permitting the access to one of two computers: $C_0$ or $C_1$. The computer $C_i$ can be accessed if the password $x_i$ is input in the spacetime region $R_i$, for $i \in \{0, 1\}$, where $R_0$ and $R_1$ are spacelike separated and within the future light cone of $P$. Here we consider that $R_i$ is the intersection of the future light cone of $Q_i = (h, -1)h, 0, 0)$ and the set of spacetime points $T_i = \{(t, x, y, z) | h \leq t \leq h + v, x + (-1)^i h^2 + y^2 + z^2 \leq v^2 \}$ for $i = 0, 1$, defined in the reference frame $F$, where $v > 0$ is a small parameter, $h > 0$, the first entry in a four vector is temporal, and we use units in which the speed of light is $c = 1$ (see Fig. $\textsuperscript{1}$). The password $x_i$ is stored securely in the computer $C_i$ in the past light cone of $Q_i$. The computer $C_i$ is secure from Alice and accepts the password only in the region $R_i$. Thus, the password $x_i$ is only useful within $R_i$. Bob pays Alice at $P$ for one of the passwords. The deal is that Bob can have access to $x_0$ in $R_0$, that Bob cannot access $x_1$ in $R_0$, and that Alice should be oblivious to Bob’s choice $b \in \{0, 1\}$, anywhere in spacetime. We define the cryptographic task that complies with the previous conditions as spacetime-constrained oblivious transfer (SCOT).

SCOT is a relativistic version of 1-out-of-2 oblivious transfer (OT)$\textsuperscript{[37]}$. OT is an important cryptographic task that can be used to implement more sophisticated
tasks [38]. As mentioned above, OT cannot be implemented with unconditional security in nonrelativistic, or relativistic, quantum cryptography [3, 33]. The main argument in the proof of the no-go theorem for OT is that the fact that Bob must learn Alice’s message $x_0$ with probability equal to (or very close to) unity and that, in a secure protocol, Alice does not have any information (or has very little information) about Bob’s input $b$, implies that there exists a unitary operation that Bob can apply to his systems after learning $x_0$ that transforms his systems into a state that allows him to learn $x_1$ with probability equal to (or very close to) unity too [33]. Similar arguments apply in the proofs that unconditionally secure quantum bit commitment and classical deterministic two party computation are impossible [20, 31, 36].

We note that these Mayers-Lo-Chau quantum attacks [29, 30, 35] and more general impossibility proofs [6, 39] do not apply to SCOT, because, due to Minkowski causality, a nonlocal unitary acting on systems in $R_0$ and $R_1$ cannot be completed outside the intersection of the future light cones of $R_0$ and $R_1$, hence, it cannot be completed within $R_0$ or $R_1$. More generally, these no-go theorems do not apply to \textit{spacetime-constrained multi-party computation}, which is defined as an extension of multi-party computation [5, 6] in which the inputs and outputs are constrained to be input and output within fixed constrained regions of spacetime, respectively, a research problem initially outlined by Kent [14].

Our results are the following. We show that unconditionally secure SCOT cannot be achieved with classical protocols in Minkowski or Galilean spacetime, or with quantum protocols in Galilean spacetime. Then, after describing the general setting of relativistic quantum cryptography, we give a quantum protocol for SCOT in Minkowski spacetime, and we show it unconditionally secure.

Interestingly, to the best of our knowledge, SCOT is the second cryptographic task with classical inputs and outputs that is proved unconditionally secure with relativistic quantum protocols, but whose unconditional security is known impossible with classical or nonrelativistic quantum protocols, location-oblivious data transfer being the first one [14]. In particular, there are relativistic classical bit commitment protocols that are provably unconditionally secure for a single round [1, 3, 22, 23], that is, for a duration limited by the time that light takes to travel between the labs of the participating agents.

We note that the first security proof for single-round relativistic classical bit commitment protocols was given by Kent (see Lemma 3 of Ref. [3]). There are conjectured unconditionally secure [1, 3, 22] relativistic classical bit commitment protocols with multiple rounds, whose duration can be extended arbitrarily long for a fixed distance between the labs of the agents. These have been shown secure against arbitrary classical attacks [1, 3, 22, 23, 27], but remain to be shown secure against arbitrary quantum attacks. Proving arbitrarily long relativistic, classical or quantum, bit commitment protocols unconditionally secure against arbitrary quantum attacks remains as an important open problem.

II. SCOT IS IMPOSSIBLE IN A CLASSICAL OR GALILEAN WORLD

We consider arbitrary SCOT protocols taking place in a finite region of spacetime, hence, with $R_0$ and $R_1$ having a finite separation. We show that classical SCOT protocols of this form cannot be unconditionally secure, in Minkowski or Galilean spacetime. Then we argue that unconditionally secure SCOT is impossible in a Galilean quantum world, as follows from Lo’s no-go theorem [35] for nonrelativistic quantum OT.

In general we can consider that Alice and Bob have several agents who participate in the protocol at different points of spacetime. In particular, the protocol involves communication events from an agent of Alice to an agent of Bob or vice versa at various spacetime points. Without loss of generality we reduce the number of communication events to three, occurring at $P, Q_0$ and $Q_1$, respectively, where we assume that Alice and Bob have adjacent labs of negligible extension. We consider first that spacetime is Minkowski and Alice and Bob perform a classical protocol. We assume there exists a classical SCOT protocol that is secure against Alice. We show that this protocol must be insecure against Bob.

We give below the main physical arguments of the proof. Some mathematical details of the proof are given in Appendix A. Let $G, G_0$ and $G_1$ be the sets of possible communication events between Alice and Bob at the spacetime points $P, Q_0$ and $Q_1$, respectively. Let $P(g|x_0, x_1, b)$ be the probability that the communication event $g = (g_0, g_1) \in G = G \times G_0 \times G_1$ occurs in the honest protocol, in general depending on Alice’s inputs $x_0, x_1$ and on Bob’s input $b$. Since $g$ is classical, Alice and Bob can produce perfect copies of it, use some copies in the protocol and keep others for record. In particular, Alice’s agents at $P, Q_0$ and $Q_1$ can send a copy of $g_0$ and $g_1$ to her agents at the other spacetime points at the speed of light, respectively. Since the protocol occurs in a finite region of spacetime, the copies of $g_0$ and $g_1$ arrive to all of Alice’s agents after a finite time. Since we assume that the protocol is secure against Alice, for any fixed inputs $x_0, x_1$, Alice can guess Bob’s bit $b$ with a bounded probability

$$P^c_A \leq \frac{1}{2} + \delta,$$  \hspace{1cm} (1)

for some $0 \leq \delta << 1$, where the labels “c” and “A” denote “cheating Alice.” We show in Appendix A that (1) implies

$$\sum_{g \in G} |P(g|x_0, x_1) - P(g|x_0, x_1, 0)| \leq 4\delta. \hspace{1cm} (2)$$

On the other hand, following the honest protocol with any input $b \in \{0, 1\}$, Bob’s agents must be able to use
the obtained value \( g \) and process it with some extra classical resources \( E \) in order to output \( x_b \) in \( R_b \) with some probability

\[
P_{b}^{h} \geq 1 - \epsilon, \tag{3}
\]

for some \( 0 \leq \epsilon << 1 \), where the labels “\( h \)” and “\( B \)” denote “honest Bob.” Bob’s agents can prepare and distribute two copies of \( E \) before the protocol. Bob’s agents can produce two perfect copies of the exchanged messages \( g, g_0 \) and \( g_1 \). Since the communication events \( g \) occur with probabilities \( P(g|x_0, x_1, b) \) that are very close for different values of \( b \in \{0, 1\} \), as given by (2). Bob’s agents can run two simultaneous protocols, one with input \( b = 0 \) and the other one with input \( b = 1 \) and thus output both \( x_0 \) in \( R_0 \) and \( x_1 \) in \( R_1 \) with probability \( P_{b}^{h} \) very close to unity, satisfying

\[
P_{b}^{h} \geq 1 - 2\epsilon - 4\delta, \tag{4}
\]

as we show in Appendix A where the labels “\( c \)” and “\( B \)” denote “cheating Bob.” Thus, the SCOT protocol is insecure against Bob, as claimed. This result trivially holds in Galilean spacetime because in this case Alice’s agents can instantaneously communicate the values of \( g, g_0 \) and \( g_1 \).

Now we consider arbitrary quantum SCOT protocols in Galilean spacetime. In principle, Alice’s and Bob’s agents can communicate classical information instantaneously. They can also transmit quantum states between distant locations instantaneously via quantum teleportation [39]. Thus, we can consider the region of three-dimensional space in which the protocol takes place as two big labs adjacent to each other, one controlled by Alice and the other one by Bob. The output regions \( R_0 \) and \( R_1 \) become irrelevant in this scenario because if Bob can output \( x_b \) anywhere in his lab then he can output \( x_b \) in \( R_0 \). This is the scenario of nonrelativistic quantum 1-out-of-2 oblivious transfer. Therefore, Lo’s no-go theorem stating that secure OT is impossible in nonrelativistic quantum cryptography applies [22]. It follows that secure SCOT is impossible in a Galilean quantum world.

### III. THE SETTING FOR RELATIVISTIC QUANTUM CRYPTOGRAPHY

We describe the setting for relativistic quantum cryptography that applies to the protocol we present here [12, 13]. Alice and Bob consist of three different agents, each controlling a secure laboratory. We denote Alice’s agents by \( A, A_0 \) and \( A_1 \), and Bob’s agents by \( B, B_0 \), and \( B_1 \). Agents \( A \) and \( B \) have secure laboratories at space regions adjacent to the point \( L = (0, 0, 0) \), while agents \( A_i \) and \( B_i \) have secure laboratories at space regions adjacent to the points \( L_i = (-1)^i h, 0, 0 \), for \( i \in \{0, 1\} \). For clarity of the presentation we assume that Alice’s and Bob’s laboratories have negligible extension and are located exactly at \( L, L_0 \) and \( L_1 \) (see Fig. 1).

We also assume that the processing of classical and quantum information at each laboratory is secure, perfect and instantaneous. We assume that the transmission of classical or quantum systems between laboratories is free of errors and at the speed of light. Bob has secure and error-free quantum channels between his laboratories. Alice has secure and error-free classical channels between hers. There are not any losses of the transmitted classical or quantum states. Finally, we require that the spacetime regions \( R_0 \) and \( R_1 \) at which Bob needs to produce his outputs are secure from Alice.

### IV. UNCONDITIONALLY SECURE SCOT

We present an unconditionally secure quantum SCOT protocol in Minkowski spacetime. Alice’s input \( x_i = (x_0^i, x_1^i, \ldots, x_{n-1}^i) \in \{0, 1\}^n \) is generated randomly and securely by \( A \) in the past light cone of \( P \), and stored securely in the computer \( C_i \) in the past light cone of \( Q_i \), for \( i = 0, 1 \).

In the past light cone of \( P \), \( A \) prepares \( r = (r_0, r_1, \ldots, r_{n-1}) \in \{0, 1\}^n \) and \( s = (s_0, s_1, \ldots, s_{n-1}) \in \{0, 1\}^n \) randomly, and \( n \) qubits \( A_0, \ldots, A_{n-1} \) in BB84 states. \( A_i \) is prepared in \( |\psi_{0,i}^j\rangle \) for \( j = 0, 1, \ldots, n-1 \), where \( |\psi_{0,i}^k\rangle = |k\rangle \), and \( |\psi_{1,i}^j\rangle = \frac{1}{\sqrt{2}} (|0\rangle + (-1)^k|1\rangle) \), for \( k \in \{0, 1\} \), and where \( |0\rangle = 0 \). \( A \) gives \( B \) the qubits \( A_i \) with their labels \( j \) at \( P \). Using her secure classical channels, \( A \) sends \( s \) and \( t_i = r \oplus x_i \) to \( A_i \), who receives them at \( Q_i \), where \( \oplus \) denotes bitwise sum modulo two. \( A_i \) gives \( s \) and \( t_i \) to \( B_i \) at \( Q_i \), as required.

Immediately after receiving the qubits \( A_j \) from \( A \) at \( P \), \( B \) sends them through his secure quantum channel to \( B_0 \), in a consecutive order according to their labels \( j \). At \( Q_j \), for each \( j = 0, 1, \ldots, n-1 \), \( B_j \) measures \( A_j \) in the basis \( D_{x_j} = \{|\psi_{0,j}^x\rangle, |\psi_{1,j}^x\rangle\} \), obtaining the bit outcome \( r_j \). Then, \( B_j \) computes \( r \oplus t_j \), which equals \( x_j \). Thus, \( B_b \) outputs \( x_b \) at \( Q_b \), as required.

We discuss in Appendix E how this protocol can be modified to allow for a small fraction of errors \( \gamma < 0.015 \). We give in Appendix C an unconditionally secure protocol for SCOT, a slight variation of this protocol, in which the geometry of the output regions \( R_i \) are defined differently: the bit \( x_j^i \) must be output at the spacetime point \( Q_j^i = (h + j\delta, -(−1)^j h, 0, 0) \) for \( j = 0, 1, \ldots, n-1 \), where \( \delta > 0 \).

#### A. Security against Alice

Our protocol is clearly secure against Alice given our assumptions that Bob’s laboratories and quantum channels are secure.
B. Security against Bob

We note that Bob could easily output $x_0$ in $R_0$ and $x_1$ in $R_1$, if $R_0$ and $R_1$ were allowed to be timelike separated. For example, if $R_0$ is defined as above, but $R_1$ is allowed to be the intersection of the future light cone of $Q = (2 h, 0, 0, 0)$ (see Fig. 1) and a small neighborhood of $Q$ in the frame $F$, Bob can play a honest strategy to output $x_0$ at $Q_0$ and also output $x_1$ at $Q$. Agent $B_0$ obtains $r$ at $Q_0$, outputs $x_0$ at $Q_0$ and sends $r$ to $B$ at the speed of light. After receiving $t_1$ at $Q_1$, $B_1$ sends $t_1$ to $B$ at the speed of light. Agent $B$ receives $r$ and $t_1$, where he computes $r \oplus t_1$, which equals $x_1$. Thus, $B$ outputs $x_1$ at $Q$. This cheating strategy is consistent with the general Mayers-Lo-Chau quantum attacks $24,25,33$: Bob can learn $x_0$ at $Q_0$ and then implement a nonlocal unitary on the systems held by his agents that allows him to learn also $x_1$ at some spacetime point $Q$. However, due to Minkowski causality, this nonlocal unitary cannot be completed outside the intersection of the future light cones of $Q_0$ and $Q_1$, hence, $Q$ cannot be spacial-like separated from $Q_0$ as required by the definition of SCOT. Thus, in general, the spaciallike separation of the spacetime points $Q_0$ and $Q_1$, at which Bob’s outputs must be produced guarantees the security of our protocol, as we show below.

Consider an arbitrary cheating strategy by Bob in which he outputs $x_0$ at $Q_0$ and $x_1$ at $Q_1$ with probability $p_n$. Since in a honest strategy, Bob achieves $p_n = 2^{-n}$ by randomly guessing $x$, ideally, unconditional security would be defined by satisfaction of a bound $p_n \leq 2^{-n} + f(m)$, where $m$ is a security parameter independent of $n$ such that $f(m) \to 0$ as $m \to \infty$. In practice, given the motivation for SCOT in which $x$ is a password that the computer $C_i$ accepts as correct if input within $R_i$, we define unconditional security by satisfaction of

$$p_n \leq f(m), \quad (5)$$

where the security parameter $m$ is allowed to be $m = n$, and where $f(m) \to 0$ as $m \to \infty$. We show below that our SCOT protocol is unconditionally secure according to definition $53$ by taking $m = n$. Importantly, we show that $f(n) \to 0$ exponentially in $n$.

An arbitrary cheating strategy by Bob is as follows. At the spacetime point $P$, agent $B$ applies a unitary operation $U$ on $A = A_0 A_1 \cdots A_{n-1}$ and some ancillary system $B$ in a fixed pure state $|\psi\rangle$, then he sends the subsystem $B_0$ of $AB$ to $B_0$ and the other subsystem, $B_1$, to $B_1$, who receive them at the respective spacetime points $Q_0$ and $Q_1$. The Hilbert spaces of $B_0$ and $B_1$ have arbitrary finite dimensions. After receiving $s$ and $t_i = x_i \oplus r$ at $Q_i$, $B_i$ implements a measurement $M_{i,s} = \{\Pi_{r,s}^i\}_{r,s \in \{0,1\}^n}$ on $B_i$ chosen according to the value of $s$, obtaining the output $r_i = (r_0, r_1, \ldots, r_{n-1}) \in \{0,1\}^n$. Finally, at the spacetime point $Q_i$, $B_i$ outputs $y_i = r_i \oplus t_i$, which equals $x_i$ if $r_i = r$.

We argue that a general cheating strategy is as described above. Any measurement implemented by $B$ at $P$ can be delayed until the spacetime points $Q_i$. The measurement implemented by $B_i$ at $Q_i$ in general depends on $s$ but not on $t_i = x_i \oplus r$, because the state $|\psi_i^{r,s}\rangle$ of qubit $A_j$ depends on $s_j$ but not on $t_j$, the $j$th entry of $t$, which is random. Similarly, in general, the goal of this measurement is to output a $n$-bits string $r_i$ which must equal $r$ with high probability because of the encoding $x_i = t_i \oplus r$.

We show below that

$$p_n \leq \tilde{p}_n, \quad (6)$$

where $\tilde{p}_n \equiv (\frac{1}{2} + \frac{1}{2^m})^n$. Thus, unconditional security, as defined by $\tilde{p}_n$, follows. We note that the bound $\tilde{p}_n$ is achieved by the following simple strategy. Agent $B$ prepares $A_j$ in the Breidbart basis $\{|\omega_0\rangle, |\omega_1\rangle\}$, where $|\omega_0\rangle = \cos(\frac{\pi}{4}) |0\rangle + \sin(\frac{\pi}{4}) |1\rangle$ and $|\omega_1\rangle = -\sin(\frac{\pi}{4}) |0\rangle + \cos(\frac{\pi}{4}) |1\rangle$. Then, $B$ sends the outcome to $B_1$, who outputs it as $r_j^i$, for $j = 0, 1, \ldots, n - 1$ and for $i = 0, 1$.

We show $\tilde{p}_n$. The proof follows from the result of Ref. $41$. Tomamichel et al. $40$ consider the following task, which they call $G^\times_{BB84}$. Two parties, Bob and Charlie, prepare a tripartite quantum state $|\xi\rangle_{ABC}$. Bob and Charlie keep the respective systems $B$ and $C$, whose Hilbert spaces have arbitrary finite dimensions, and send the system $A = A_0 A_1 \cdots A_{n-1}$ to another party, Alice, where each system $A_j$ is a qubit. After the preparation of $|\xi\rangle_{ABC}$, Bob and Charlie are not allowed to communicate. Alice randomly generates $s = (s_0, \ldots, s_{n-1}) \in \{0,1\}^n$ and measures $A_j$ in the BB84 basis $D_{s_j}$, obtaining the outcome $r_j \in \{0,1\}$, for $j = 0, 1, \ldots, n - 1$. Alice announces $s$ to Bob and Charlie. Bob and Charlie apply measurements $M_{0,s}$ and $M_{1,s}$, which in general depend on $s$, on systems $B$ and $C$, obtaining the $n$-bit outcomes $r_0$ and $r_1$, respectively. Bob and Charlie win the game if $r_0 = r_1 = r$, where $r = (r_0, r_1, \ldots, r_{n-1})$. It is shown in $40$ that the maximum probability to win the $G^\times_{BB84}$ game, optimized over all allowed quantum strategies by Bob and Charlie, is given by $\tilde{p}_n$.

We relate a cheating strategy by Bob in our SCOT protocol to a strategy by Bob and Charlie in the $G^\times_{BB84}$ game. In our SCOT protocol, it is equivalent if $A$ prepares $n$ Bell states $|\Phi^+\rangle_{A'A'} = \otimes_{j=0}^{n-1} |\phi^+\rangle_{A'_j A'_j}$, she sends $A = A_0 A_1 \cdots A_{n-1}$ to $B$ and measures qubit $A'_j$ in the basis $D_{s_j}$. If Alice obtains outcome $r_j$ for qubit $A'_j$, then qubit $A_j$ projects into the state $|\psi_i^{r,s}\rangle$. Consider a $G^\times_{BB84}$ game in which Bob and Charlie initially prepare $|\xi\rangle_{A'B'} = (|1A'_0 \otimes U_{AB}|\Phi^+\rangle_{A'A'})|\chi\rangle_B$ and send $A'$ to Alice, Bob keeps $B_0$ and Charlie keeps $B_1$, where $AB = B_0 B_1$, and where $U$ and $|\chi\rangle$ are the unitary operation and the state used in the cheating strategy by Bob in our SCOT protocol. Then, by identifying agents $B_0$ and $B_1$ in our SCOT protocol with Bob and Charlie in the $G^\times_{BB84}$ game, it follows that Bob’s cheating probability in our SCOT protocol is upper bounded by $p_n \leq \tilde{p}_n$, as claimed.
V. DISCUSSION

Here we defined the cryptographic task of spacetime-constrained oblivious transfer (SCOT). We showed that unconditionally secure SCOT cannot be achieved with classical protocols in Minkowski or Galilean spacetime, or with quantum protocols in Galilean spacetime. We gave a quantum SCOT protocol in Minkowski spacetime that we proved unconditionally secure.

It is straightforward to see that our SCOT protocol can be used to implement unconditionally secure bit commitment. Bob commits to a bit $b$ at the spacetime point $P$. Assuming that Alice reads the passwords that Bob inputs into the computers $C_i$, Bob unveils his commitment by introducing the password $x_b$ into $C_b$ within the required spacetime region $R_b$.

On the other hand, unconditionally secure SCOT cannot in general be obtained from unconditionally secure relativistic bit commitment. This follows because there are unconditionally secure classical relativistic bit commitment protocols $[13, 23, 22]$, but unconditionally secure SCOT cannot be achieved with classical protocols, as we proved here. It would be interesting to investigate under what general conditions unconditionally secure SCOT can be used to implement unconditionally secure relativistic bit commitment.

Furthermore, we note that our SCOT protocol seems quite similar to Kent’s quantum relativistic bit commitment protocol $[17]$, in that in both protocols random BB84 states are transmitted at the spacetime point $P$. An important difference between our SCOT protocol and Kent’s bit commitment protocol $[17]$ is that in our protocol, at the spacetime point $Q_i$, Bob’s agent $B_i$ is informed of the bases on which Alice prepared the transmitted qubits, while in Kent’s protocol the committer (who would be Bob in our notation, but is Alice in the notation of Refs. $[17, 13]$) is never revealed by the bases of the other party. This implies that the security proofs of Kent’s protocol $[17]$, for example the one by Croke and Kent $[18]$, cannot in general be adapted to show the security of our SCOT protocol, because in a general cheating strategy by Bob in our protocol, Bob’s agents $B_i$ apply measurements that depend on the bases on which Alice prepared the qubits, which is not possible in the cheating strategies in the bit commitment protocol $[17]$.

The defined task of SCOT can be generalized to settings in which Alice has $m$ inputs $x_0, x_1, \ldots, x_{m-1} \in \{0, 1, \ldots, d-1\}$ that Bob must output within spacelike separated regions $R_0, R_1, \ldots, R_{m-1}$ according to his input $b \in \{0, 1, \ldots, m-1\}$. One can also investigate different configurations of the geometry for the output and input regions (see an example in Appendix C). Additionally, one can relax the condition that Alice should not be able to learn Bob’s input $b$ anywhere in spacetime to the weaker requirement that Alice should not learn $b$ within some fixed particular region of spacetime.

It would be interesting to investigate whether SCOT protocols can be proved unconditionally secure from fundamental physical principles in more general models of spacetime or in postquantum theories of correlations. For example, can we find SCOT protocols that are provably unconditionally secure from the violation of Bell inequalities and the no-signaling principle (as recently done for relativistic quantum bit commitment protocols $[25]$)?

Finally, it is interesting to investigate whether SCOT can be combined with other cryptographic tasks to perform more general spacetime-constrained multi-party computation and other sophisticated cryptographic tasks.

ACKNOWLEDGMENTS

The author thanks Jonathan Silman, Serge Massar and Stefano Pironio for very helpful conversations. This work was mainly done at the Laboratoire d’Information Quantique, Université libre de Bruxelles, with financial support from the European Union under the project QALGO, from the F.R.S.-FNRS under the project DIQIP and from the InterUniversity Attraction Poles of the Belgian Federal Government through project Photonics@be. Part of this work was completed at IRIF, Université Paris Diderot, supported by the project ERC QCC.

Appendix A: Details of the impossibility proof for unconditionally secure classical protocols for SCOT

We show (2). For fixed given values of $x_0, x_1$, we define the sets $G^0 \equiv \{ g \in \bar{G} | P(g|x_0, x_1, 0) \geq P(g|x_0, x_1, 1) \}$ and $G^1 \equiv \{ g \in \bar{G} | P(g|x_0, x_1, 1) > P(g|x_0, x_1, 0) \}$. We consider a cheating strategy by Alice in which she first follows the honest protocol and then guesses that $b = i$ if a communication event $g \in G^i$ takes place. Alice’s probability to guess $b$ correctly, given her inputs $x_0, x_1$, is thus

$$P_A^c = \frac{1}{2} \sum_{i=0}^{1} \sum_{g \in G^i} P(g|x_0, x_1, i). \quad (A1)$$

It follows that

$$P_A^c = \frac{1}{2} + \frac{1}{2} \sum_{g \in G^i} \left( P(g|x_0, x_1, i) - P(g|x_0, x_1, \overline{i}) \right)$$

$$= \frac{1}{2} + \frac{1}{2} \sum_{g \in G^i} \left| P(g|x_0, x_1, i) - P(g|x_0, x_1, \overline{i}) \right|, \quad (A2)$$

for $i = 0, 1$, where in the second line we used that from the definition of $G^i$, we have that $P(g|x_0, x_1, i) \geq P(g|x_0, x_1, \overline{i})$ for all $g \in G^i$ and $i \in \{0, 1\}$. It follows from (A2) that

$$P_A^c = \frac{1}{2} + \frac{1}{2} \sum_{g \in G} \left| P(g|x_0, x_1, 0) - P(g|x_0, x_1, 1) \right|. \quad (A3)$$
Thus, we see from (A3) that satisfaction of (1) implies that (2) must hold.

We show (4). The probability that Bob outputs $x_i$ at $Q_i$ correctly following the honest protocol with input $b = i$ is given by

$$P_{i}^{h} = \frac{1}{2^n} \sum_{x_0, x_1 : g \in G} P_{i}^{h}(x_i | g, x_0, x_1, i) P(g | x_0, x_1, i),$$

where $P_{i}^{h}(x_i | g, x_0, x_1, i)$ is the probability that Bob guesses the value of $x_i$ correctly at the spacetime point $Q_i$ following the honest protocol with input $b = i$ given that Alice’s inputs are $x_0, x_1$ and the communication event $g \in G$ takes place, for $i \in \{0, 1\}$. From (3), the probability that Bob succeeds in the honest protocol satisfies

$$P_{i}^{h} \geq 1 - \epsilon.$$  

Consider a cheating strategy by Bob in which he initially sets his input $b = i$ and runs a honest protocol, obtaining communication events $g, g_0$ and $g_1$ at $P, Q_0$ and $Q_1$, respectively. Bob thus outputs $x_i$ at $Q_i$ with probability $P_{i}^{h}$. However, in addition to following the honest protocol with input $b = i$, Bob’s agents perform the following actions. They produce perfect copies of the communicated messages $g, g_0$ and $g_1$ at $P, Q_0$ and $Q_1$, respectively. They use these copies to simultaneously run a honest protocol with the other input $b = \bar{i}$, obtaining the output $x_{\bar{i}}$ at $Q_{\bar{i}}$ with some probability $P_{\bar{i}}^{h}$. The success probability of this simultaneous protocol is given by

$$P_{i}^{B} = \frac{1}{2^n} \sum_{x_0, x_1 : g \in G} P_{i}^{h}(x_i | g, x_0, x_1, i) P(g | x_0, x_1, i)$$

$$= P_{i}^{h} + \frac{1}{2^n} \sum_{x_0, x_1 : g \in G} \sum_{g_0, g_1} P_{i}^{h}(x_i | g, x_0, x_1, i) \Delta(g, x_0, x_1, i)$$

$$\geq P_{i}^{h} - \frac{1}{2^n} \sum_{x_0, x_1 : g \in G} \sum_{g_0, g_1} |\Delta(g, x_0, x_1, i)|$$

$$\geq P_{i}^{h} - 4 \delta,$$

where $\Delta(g, x_0, x_1, i) \equiv P(g | x_0, x_1, i) - P(g | x_0, x_1, \bar{i})$, in the second line we used $P(g | x_0, x_1, i) = P(g | x_0, x_1, \bar{i}) + \Delta(g, x_0, x_1, i)$ and expression (A3), and in the last line we used (2). It follows from (A5) and (A6) that Bob’s success probability in this simultaneous protocol satisfies $P_{B}^{h} \geq 1 - \epsilon - 4 \delta$. Since $\epsilon << 1$ and $\delta << 1$, Bob obtains both $x_0$ at $Q_0$ and $x_1$ at $Q_1$ with a probability $P_{B}^{h}$ close to unity: $P_{B}^{h} \geq P_{i}^{h} + P_{i}^{h} - 1 \geq 1 - 2\epsilon - 4 \delta$, for any $i \in \{0, 1\}$, which shows (4).

**Appendix B: Allowing for errors**

The SCOT protocol described in the main text can be modified to allow for a small fraction of errors $\gamma < 0.015$.

A password $y_i$ is accepted as valid by $C_i$ if it differs from $x_i$ in at most $\gamma n$ bit entries. Under this condition, the probability $p_{i}^{w}$ that both $B_0$ and $B_1$ input valid passwords into $C_0$ and $C_1$, respectively, is bounded by $p_{i}^{w} \leq \left(2^{2h(\gamma)} \bar{p}_1\right)^n$, where $h(\gamma) = -\gamma \log_2 \gamma - (1 - \gamma) \log_2 (1 - \gamma)$ is the binary entropy. This bound follows because the probability to win a modified version of the $C_{BB84}^{x=1}$ in which a fraction $\gamma$ of bit errors is allowed is not greater than $\left(2^{2h(\gamma)} \bar{p}_1\right)^n$ [40]. Thus, for $\gamma < 0.015$, we have $2^{2h(\gamma)} \bar{p}_1 < 1$, hence, unconditional security follows.

**Appendix C: SCOT with modified geometry of the output regions**

We consider a SCOT scenario in which the geometry of the output regions $R_i$ is defined as follows. The bit $x_i^j$ must be output at the spacetime point $Q_i^j = (h + j \delta, -(1)^j h, 0, 0)$ for $j = 0, 1, \ldots, n - 1$, where $\delta > 0$. We say that Bob outputs $x_i$ within $R_i$ if he outputs $x_i^j$ at $Q_i^j$ for all $j = 0, 1, \ldots, n - 1$.

We give an unconditionally secure SCOT protocol for the output regions defined above. In the past light cone of $P$, $A$ prepares $r = \{r_0, r_1, \ldots, r_{n-1}\} \in \{0, 1\}^n$ and $s = \{s_0, s_1, \ldots, s_{n-1}\} \in \{0, 1\}^n$ randomly, and $n$ qubits $A_0, \ldots, A_{n-1}$ in BB84 states. The qubit $A_j$ is prepared in the state $|\psi_j^{+}\rangle$. $A$ gives $B$ the qubit $A_j$ at the spacetime point $P_j = (j \delta, 0, 0, 0)$. Using her secure classical channels, $A$ sends the bits $s_j$ and $t_j^i = r_j \oplus x_i^j$ to $A_i$, who receives them at $Q_i^j$. Agent $A_i$ gives agent $B_i$ these bits at $Q_i^j$.

Immediately after receiving $A_j$ from $A$ at $P_j$, $B$ sends it through his secure quantum channel to $B_i$. At $Q_i^j$, $B_i$ measures $A_j$ in the BB84 basis $D_{ij}$, obtaining the bit outcome $r_j$. Then, $B_i$ computes the bit $r_j \oplus t_j^i$, which equals $x_i^j$. Thus, $B_i$ outputs $x_i^j$ at $Q_i^j$ for all $j = 0, 1, \ldots, n - 1$, as required.

1. **Security against Alice**

Similarly to the SCOT protocol given in the main text, this protocol is secure against Alice, given our assumptions that Bob’s laboratories and quantum channels are secure.

2. **Security against Bob**

The security against Bob follows trivially from the security proof of the SCOT protocol given in the main text. We give an alternative security proof below.

In an arbitrary cheating strategy by Bob, at the spacetime point $P_j$, agent $B$ applies a unitary operation $U_j$ on the qubit $A_j$, received from $A$, and some ancillary system.
which is achieved by the same strategy on the respective spacetime points \(Q_0^i\) and \(Q_1^i\). After receiving the bits \(s_j\) and \(t_i^j = x_i^j \oplus r_j\) at \(Q_1^i\), \(B_i\) implements a measurement on \(B_i^i\) chosen according to the value of \(s_j\), obtaining a bit output \(r_i^j\). Finally, at the spacetime point \(Q_1^i\), \(B_i\) outputs \(y_i^j = r_i^j \oplus t_i^j\), which equals \(x_i^j\) if \(r_i^j = r_j\).

We argue that a general cheating strategy is of the form described above. First, since the spacetime point \(Q_1^i\) where \(B_i\) must output \(x_i^j\) is light separated from the spacetime point \(P_j\) where agent \(B\) receives the qubit \(A_j\) encoding \(x_i^j\), \(B_i\) must apply any quantum operations on \(A_j E_j\) at \(P_j\) and instantaneously send \(B_i^i\) to \(B_i\). This implies that \(B\) cannot wait a time \(\delta\) to receive the next qubit \(A_{j+1}\) at \(P_{j+1}\) in order to apply a joint operation on \(A_j\) and \(A_{j+1}\).

Second, an arbitrary measurement that \(B\) might perform at \(P_j\) can be delayed until points \(Q_1^i\). In particular, \(B\) cannot obtain any information about the bits \(r_j\) with \(j' > j\) encoded in subsequent qubits \(A_{j+1}, A_{j+2}, \ldots, A_{n-1}\) by applying a measurement on \(A_j\) because the bits \(r_j\) and \(s_j\) are random, hence, the state \(|\psi_i^i\rangle\) of qubit \(A_j\) does not encode any information about bits \(r_{j'}\) or \(x_{i}^{j'}\) for \(j' \neq j\). Similarly, \(B\) cannot obtain any information about \(r_{j'}\) that is not already encoded in \(A_j\) by preparing some ancilla \(D_j\) entangled with \(A_j\) and then applying some joint measurement on \(D_j A_j\), for \(j' > j\).

Finally, the measurement implemented by \(B_i\) at \(Q_1^i\) in general depends on \(s_j\) but not on \(t_i^j = x_i^j \oplus r_j\) because the state \(|\psi_i^i\rangle\) of qubit \(A_j\) depends on \(s_j\) but not on \(t_i^j\), which is random. Similarly, in general, the goal of this measurement is to output a bit \(r_i^j\) that equals \(r_j\) with high probability because of the encoding of \(x_i^j\) via \(t_i^j = x_i^j \oplus r_j\).

Let \(q^j\) be the maximum success probability that \(B_0\) and \(B_1\) output \(x_i^j\) and \(x_i^j\) at \(Q_0^i\) and \(Q_1^i\), respectively. As discussed above, in general, Bob must treat qubit \(A_j\) independently of other qubits \(A_{j'}\). Since the protocol implies that Alice follows to encode \(x_i^j\) is the same for any \(j\), and bits \(x_i^j\) and \(x_i^{j'}\) are encoded independently for any \(j' \neq j\), we have that \(q^j = q^{j'} \equiv q\) for all \(j, j' \in \{0, 1, \ldots, n-1\}\), which is achieved by the same strategy on \(A_j E_j\) for all \(j\). We show below that

\[
q \leq \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}}\right). 
\]  

(C1)

Since the probability that \(B_i\) outputs \(x_i^j\) at \(Q_1^i\) is independent of the probability to output \(x_i^{j'}\) for \(j' \neq j\), as follows from the discussion above, we have that the maximum success probability that \(B_0\) and \(B_1\) output \(x_i^0\) and \(x_i^1\) at \(Q_0^i\) and \(Q_1^i\), respectively, for all \(j = 0, 1, \ldots, n-1\) is \(p_{\text{max}} = (q^n)\). It follows from (C1) that unconditional security, as defined by equation (1) of the main text, is satisfied.

We show (C1) by considering the case \(j = 0\). We simplify notation by setting \(A_0 = A, E_0 = E, B_0^i = B_i, P_0 = P, Q_0^i = Q_i, x_i^0 = x_i, r_0 = r, s_0 = s\) and \(r_i^j = r_j\). Let \(q^i\) be the probability that \(B_i\) outputs \(x_i\) at \(Q_i\), for \(i \in \{0, 1\}\), in a strategy achieving \(q\). It follows that \(q \leq \frac{1}{2}(q^0 + q^1)\). We show below that

\[
q_{\text{max}} = 1 + \frac{1}{\sqrt{2}}. 
\]  

(C2)

where \(q_{\text{max}} \equiv \max\{q^0 + q^1\}\), and where the maximum is taken over all possible strategies by Bob, as described above. Thus, (C1) follows. We note that \(q_{\text{max}}\) is achieved if Bob applies \(1 \rightarrow 2\) optimal symmetric cloning [41] of the BB84 states to qubit \(A\) and sends a clone to \(B_i\), who then measures it in the BB84 basis \(D_i\) on which \(A\) was prepared and outputs the outcome as \(r_i\), for \(i \in \{0, 1\}\). Alternatively, \(q_{\text{max}}\) is achieved if \(B\) measures \(A\) in the Breidbart basis \(\{|\omega_0\rangle, |\omega_1\rangle\}\), where \(|\omega_0\rangle = \cos \left(\frac{x}{2}\right) |0\rangle + \sin \left(\frac{x}{2}\right) |1\rangle\) and \(|\omega_1\rangle = -\sin \left(\frac{x}{2}\right) |0\rangle + \cos \left(\frac{x}{2}\right) |1\rangle\) and sends the outcome to agents \(B_i\), who outputs it as \(r_i\).

We show (C2). After \(B\) applies the unitary operation \(U\), the system \(AE = B_0 B_1\) is transformed into

\[
|\Psi^i\rangle_{B_0 B_1} = U |\psi_i^i\rangle_A |\chi\rangle_E. 
\]  

(C3)

In general, we can consider that the measurement applied by \(B_i\) on \(B_i\) is a projective measurement \(M_{i,s} = \{\Pi_{s,k}^i\}_{k=0}^1\). This is because an arbitrary measurement can be implemented by introducing an ancilla, included in \(B_i\) at \(P\), and then performing a projective measurement on the whole system. Thus, we have

\[
q_0 + q_1 = \frac{1}{4} \sum_{r=0}^1 \sum_{s=0}^1 \left(\langle \Psi^i_0 | \Pi_{s,0}^i \Pi_{r,0}^i | \Psi^i_0 \rangle + \langle \Psi^i_1 | \Pi_{s,1}^i \Pi_{r,0}^i | \Psi^i_0 \rangle + \langle \Psi^i_0 | \Pi_{s,0}^i \Pi_{r,1}^i | \Psi^i_1 \rangle \right), 
\]  

(C4)

where the projector \(\Pi_{s,k}^i\) acts on system \(B_i\) and \(I\) is the identity operator acting on the other system. We write \(4(q_0 + q_1) = \mu_0 + \mu_1\), where

\[
\mu_0 = \langle \Psi^i_0 | \Pi_{0,0}^i \Pi_{0,0}^i | \Psi^i_0 \rangle + \langle \Psi^i_0 | \Pi_{1,0}^i \Pi_{0,0}^i | \Psi^i_0 \rangle + \langle \Psi^i_0 | I \Pi_{1,0}^i \Pi_{1,0}^i | \Psi^i_0 \rangle + \langle \Psi^i_1 | I \Pi_{1,0}^i \Pi_{1,0}^i | \Psi^i_1 \rangle, 
\]  

(C5)

\[
\mu_1 = \langle \Psi^i_0 | I \Pi_{0,0}^i | \Psi^i_0 \rangle + \langle \Psi^i_0 | I \Pi_{1,1}^i | \Psi^i_0 \rangle + \langle \Psi^i_0 | \Pi_{0,0}^i \Pi_{1,0}^i | \Psi^i_1 \rangle + \langle \Psi^i_1 | \Pi_{0,0}^i \Pi_{1,1}^i | \Psi^i_1 \rangle. 
\]  

(C6)

We note from the symmetry of the terms \(\mu_i\) that the maximum value of \(\mu_0, \mu_{\text{max}}\), equals the maximum value of \(\mu_1\). Thus, \(q_0 + q_1 \leq \mu_{\text{max}}/2\). We show below that

\[
\mu_{\text{max}} = 2 + \sqrt{2}. 
\]  

(C7)

Since, as mentioned above, the value \(q_0 + q_1 = 1 + \frac{1}{\sqrt{2}}\) is achieved by an optimal cloning strategy, or by measuring in the Breidbart basis, equation (C2) follows.

We show (C7). We recall the definitions given in the main text:

\[
|\psi^i_k\rangle = |k\rangle, \quad |\psi^i_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^k |1\rangle). 
\]  

(C8)
for \( k \in \{0, 1\} \), and where \( \langle 0|1 \rangle = 0 \). From (C9) and (C8), we have

\[
\langle \Psi_0^0|\Psi_1^0 \rangle = 0, \quad |\Psi_2^0 \rangle = \frac{1}{\sqrt{2}} \left( (|\Psi_0^0 \rangle + (-1)^r|\Psi_1^0 \rangle) \right). \tag{C9}
\]

Using the second equality of (C9) and the relations \((\Pi_{r,s}^r)^\dagger = \Pi_{r,s}^r\) and \(\Pi_{r,s}^1 = I_{B_s} - \Pi_{r,s}^0\) in (C5), we reduce the expression of \(\mu_0\) to

\[
\mu_0 = 2 + \langle \Psi_0^0 | \Pi_{0,0}^0 \otimes I | \Psi_0^0 \rangle + \langle \Psi_1^0 | \Pi_{0,0}^0 \otimes I | \Psi_1^0 \rangle + 2\text{Re}(\langle \Psi_0^0 | I \otimes \Pi_{1,1}^1 | \Psi_1^0 \rangle). \tag{C10}
\]

We express \(|\Psi_j^0\rangle\) in terms of states \(|\alpha_{jkl}\rangle\) living in the subspaces on which the projectors \(\Pi_{0,0}^0\) and \(\Pi_{1,1}^1\) act, for \(j, k, l \in \{0, 1\}\). We have

\[
|\Psi_j^0\rangle = \sum_{k=0}^1 \sum_{l=0}^1 a_{jkl}|\alpha_{jkl}\rangle, \tag{C11}
\]

where we impose the normalization conditions \(\langle \alpha_{jkl} | \alpha_{jkl} \rangle = 1\) and

\[
\sum_{k=0}^1 \sum_{l=0}^1 |a_{jkl}|^2 = 1, \tag{C12}
\]

and where the following relation holds:

\[
(\Pi_{0,0}^0 \otimes \Pi_{1,1}^1)|\alpha_{jkl}\rangle = |\alpha_{jkl}\rangle. \tag{C13}
\]

Using the properties of projectors, \(\Pi_{r,s}^r \Pi_{r',s}^{r'} = \delta_{r,r'} \Pi_{r,s}^r\) and \((\Pi_{r,s}^r)^\dagger = \Pi_{r,s}^{r'}\), we obtain from (C10), (C11) and (C13) that

\[
\mu_0 = 2 + 2\text{Re}(a_{000}^*a_{100}\langle \alpha_{000} | \alpha_{100} \rangle + a_{010}^*a_{110}\langle \alpha_{010} | \alpha_{110} \rangle) + |a_{000}|^2 + |a_{010}|^2 - |a_{100}|^2 - |a_{110}|^2. \tag{C14}
\]

From (C11), (C13) and the fact that \(\Pi_{r,s}^r\) are projectors, the orthogonality constraint in (C9) reads

\[
\langle \Psi_0^0 | \Psi_1^0 \rangle = \sum_{k=0}^1 \sum_{l=0}^1 a_{0kl}^*a_{1kl}\langle \alpha_{0kl} | \alpha_{1kl} \rangle = 0. \tag{C15}
\]

Using the expression (C13), subject to constraints (C12), (C15) and \(|\langle \alpha_{0kl} | \alpha_{1kl} \rangle| \leq 1\), we obtained numerically that the maximum of \(\mu_0\) is given by (C7), as claimed.

We give below the mathematical expression input to the Mathematica program.

The complex variables \(a_{jkl}\) and \(\langle \alpha_{0kl} | \alpha_{1kl} \rangle\) are defined in terms of real variables \(c_{jkl}, d_{jkl}, g_{kl}\) and \(h_{kl}\) for \(j, k, l \in \{0, 1\}\), as follows:

\[
a_{jkl} = c_{jkl} + id_{jkl}, \tag{C16}
\]

\[
\langle \alpha_{0kl} | \alpha_{1kl} \rangle = g_{kl} + ih_{kl}. \tag{C17}
\]

The constraints given by equations (C12) and (C15) respectively read

\[
\sum_{k=0}^1 \sum_{l=0}^1 \left[ (c_{jkl})^2 + (d_{jkl})^2 \right] = 1, \tag{C18}
\]

and

\[
0 = g_{00}(c_{000}c_{100} + d_{000}d_{100}) - h_{00}(c_{000}d_{100} - c_{100}d_{000}) + g_{01}(c_{001}c_{110} + d_{001}d_{110}) - h_{01}(c_{001}d_{110} + c_{110}d_{001}) + g_{11}(c_{011}c_{111} + d_{011}d_{111}) - h_{11}(c_{011}d_{111} + c_{111}d_{011}),
\]

\[
o = g_{00}(c_{000}d_{100} - c_{100}d_{000}) + h_{00}(c_{000}c_{100} + d_{000}d_{100}) + g_{01}(c_{001}d_{110} + c_{101}d_{001}) + h_{01}(c_{001}c_{110} + d_{001}d_{110}) + g_{11}(c_{011}d_{111} - c_{110}d_{011}) + h_{11}(c_{011}c_{111} + d_{011}d_{111}). \tag{C19}
\]

The constraints \(|\langle \alpha_{0kl} | \alpha_{1kl} \rangle| \leq 1\) are given by

\[
(g_{kl})^2 + (h_{kl})^2 \leq 1. \tag{C20}
\]

The expression for \(\mu_0\) given by equation (C14) corresponds to

\[
\mu_0 = 2 + \sum_{l=0}^1 \left[ (c_{00l})^2 + (d_{00l})^2 - (c_{10l})^2 - (d_{10l})^2 \right] + 2\left( g_{00}(c_{000}c_{100} + d_{000}d_{100}) + g_{01}(c_{001}d_{100} - c_{100}d_{001}) + g_{11}(c_{011}c_{110} + d_{011}d_{110}) + h_{11}(c_{011}d_{111} - c_{110}d_{011}) \right). \tag{C21}
\]

We computed the maximum value of \(\mu_0\) given by (C21), subject to the constraints (C18) – (C20). It was found that \(\mu_0^\text{max} = 2 + \sqrt{2}\), as given by equation (C7).

[1] A. Kent, Phys. Rev. Lett. 83, 1447 (1999)
[2] A. Kent, Phys. Rev. Lett. 83, 5382 (1999)
[3] A. Kent, J. Cryptology 18, 313 (2005)
[4] A. P. Kent, W. J. Munro, T. P. Spiller, and R. G. Beausoleil, “Tagging systems,” U.S Patent No. 7,075,438 (2006).
[5] R. Colbeck and A. Kent, Phys. Rev. A 73, 032320 (2006)
[6] R. Colbeck, Phys. Rev. A 76, 062308 (2007)
[7] R. Colbeck, Quantum And Relativistic Protocols For Se-
cure Multi-Party Computation, Ph.D. thesis, University of Cambridge (2009), eprint arXiv:0911.3814.

[8] R. A. Malaney, Phys. Rev. A 81, 042319 (2010).

[9] A. Kent, W. J. Munro, and T. P. Spiller, Phys. Rev. A 84, 012326 (2011).

[10] A. Kent, Phys. Rev. A 84, 022335 (2011).

[11] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, SIAM J. Comput. 43, 150 (2014).

[12] A. Kent, Quantum Inf. Process. 12, 1023 (2013).

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

[14] A. Kent, Phys. Rev. A 84, 012328 (2011).

[15] A. Kent, Class. Quantum Grav. 29, 224013 (2012).

[16] P. Hayden and A. May, arXiv:1210.0913.

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

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

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

[20] 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).

[22] A. Kent, S. Massar, and J. Silman, Sci. Rep. 4, 3901 (2014).

[23] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner and H. Zbinden, Phys. Rev. Lett. 115, 030502 (2015).

[24] E. Adlam and A. Kent, Int. J. Quantum Inf. 13, 1550029 (2015).

[25] E. Adlam and A. Kent, Phys. Rev. A 92, 022315 (2015).

[26] K. Chakraborty, A. Chailloux, and A. Leverrier, Phys. Rev. Lett. 115, 250501 (2015).

[27] S. Fehr and M. Fillinger, “On the composition of two-prover commitments, and applications to multi-round relativistic commitments,” Cryp- tology ePrint Archive, Report 2016/113 (2016), http://eprint.iacr.org/2016/113.

[28] E. Adlam and A. Kent, Phys. Rev. A 93, 062327 (2016).

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

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

[31] H.-K. Lo and H. Chau, Physica D: Nonlinear Phenomena 120, 177 (1998) proceedings of the Fourth Workshop on Physics and Consumption.

[32] A. Y. Kitaev, “Quantum coin-flipping,” (2002), talk at QIP 2003.

[33] A. Ambainis, H. Buhrman, Y. Dodis, and H. Roehrig, “Multiparty quantum coin flipping,” (2004), arXiv:quant-ph/0304112.

[34] J. Kilian, “Founding cryptography on oblivious transfer,” In Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, STOC ’88 (ACM, New York, 1988) pp. 20–31.

[35] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wooters, Phys. Rev. Lett. 70, 1895 (1993).

[36] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, Rev. Mod. Phys. 77, 1225 (2005).