Practical and unconditionally secure spacetime-constrained oblivious transfer

Damián Pitalúa-García\(^1\) and Iordanis Kerenidis\(^2\)

\(^1\)IRIF, Université Paris Diderot, Paris, France
\(^2\)IRIF, CNRS, Université Paris Diderot, Paris, France

Spacetime-constrained oblivious transfer (SCOT) extends the fundamental primitive of oblivious transfer to Minkowski space. SCOT and location oblivious data transfer (LODT) are the only known cryptographic tasks with classical inputs and outputs for which unconditional security needs both quantum theory and relativity. We give an unconditionally secure SCOT protocol that, contrasting previous SCOT and LODT protocols, is practical to implement with current technology, where distant agents need only communicate classical information, while quantum communication occurs at a single location. We also show that our SCOT protocol can be used to implement unconditionally secure quantum relativistic bit commitment.

I. INTRODUCTION

The two main theories in physics are quantum theory and relativity. Relativistic quantum cryptography \(^1\) \(\text{[1–3]}\) investigates the security of cryptographic protocols based on the physical principles of these theories. On the one hand, the causality of Minkowski spacetime — and of the approximately-Minkowski spacetime near the Earth surface — implies that physical systems and information cannot travel faster than light. On the other hand, quantum information cannot be cloned \(^4\) \(\text{[4, 5]}\), non-orthogonal quantum states cannot be perfectly distinguished, quantum entanglement is monogamous \(^6\), and there are quantum correlations that violate Bell inequalities \(^7\).

Some cryptographic primitives can be implemented with unconditional security based only on the principles of quantum theory, for example, quantum key distribution \(^8\) \(\text{[8–10]}\), private randomness expansion \(^11\) \(\text{[11–13]}\), and weak coin tossing with arbitrarily small bias \(^14\) \(\text{[14]}\). However, other important cryptographic tasks are impossible to implement with unconditional security based only on quantum theory, like bit commitment \(^15\) \(\text{[15, 16]}\), strong coin tossing with arbitrarily small bias \(^17\) \(\text{[17–19]}\), oblivious transfer \(^20\) \(\text{[20–22]}\), and more general two-party classical computation \(^21\) \(\text{[22, 23]}\) — although there are quantum protocols with strictly better security than classical protocols for bit commitment \(^24\), strong coin tossing \(^25\) and oblivious transfer \(^26\). Nevertheless, Kent showed that considering the causality of Minkowski spacetime allows us to obtain unconditionally secure protocols for strong coin tossing \(^2\) and bit commitment \(^1\) \(\text{[1]}\), even if quantum theory is not considered.

It is interesting to ask whether there are cryptographic primitives whose unconditional security requires both quantum theory and relativity. While unconditionally secure protocols for oblivious transfer remain impossible to implement even with relativistic quantum protocols \(\text{[22, 28]}\), unconditionally secure protocols for its variants location-oblivious data transfer (LODT) \(^20\) and spacetime-constrained oblivious transfer (SCOT) \(^30\) exist in relativistic quantum settings. However, unconditionally secure LODT and SCOT are impossible when based only on quantum theory, or in relativity. Only the combined properties of quantum information and Minkowski causality can allow for unconditionally secure LODT and SCOT protocols \(\text{[20, 30]}\). As far as we know, LODT and SCOT are the only known cryptographic tasks with classical inputs and outputs whose unconditional security necessitates both quantum theory and relativity.

LODT and SCOT are relativistic extensions of oblivious transfer. The primitive of one-out-of-two oblivious transfer \(^31\) is informally defined as follows. Alice has two bits \(x_0, x_1\) and Bob has a bit \(b\). At the end of the protocol, Bob must learn \(x_b\) but not \(x_{\overline{b}}\), and Alice must not learn \(b\). While somewhat abstract, oblivious transfer is related to private information retrieval and is a universal primitive, meaning that any secure computation between Alice and Bob can be reduced to this simple primitive \(^32\). In LODT \(^20\), Alice transfers a message to Bob at a random spacetime location that neither Alice nor Bob can determine in advance, and the location where Bob receives the message remains unknown to Alice. In SCOT \(^30\), Alice has two input messages \(x_0, x_1\) and Bob has an input bit \(b\), Bob obtains \(x_b\) in \(R_b\), but he cannot obtain \(x_{\overline{b}}\) in \(R_{\overline{b}}\), where \(R_0\) and \(R_1\) are fixed spacelike separated spacetime regions.

We motivate SCOT by the following scenario. Alice wants to give access to Bob to one of two computers: \(C_0\) or \(C_1\). The computer \(C_i\) can only be accessed by Bob if he inputs the password \(x_i\) in the spacetime region \(R_i\), for \(i \in \{0, 1\}\). Each computer reveals a different database to Bob, or allows Bob to perform a different computational process. Bob does not want to reveal which computer he wants to access and Alice needs to make sure that Bob does not get access to both computers. SCOT guarantees that Bob can access one of the computers, without Alice knowing which one. Moreover, Alice is certain that, for a time interval, Bob cannot access the second com-

---

\(^{5}\) [D.Pitalua-Garcia@studentdamtp.cam.ac.uk]

\(^{6}\) [Present address: Centre for Quantum Information and Foundations, DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WA, U.K.]
puter too. Thus, by changing the access passwords before this time interval expires, the protocol guarantees that Bob can only access one of the computers. As mentioned above, oblivious transfer is a very strong cryptographic primitive \cite{22}. SCOT is a strong cryptographic primitive too, as we show below that it implements unconditionally secure relativistic bit commitment.

Although there are unconditionally secure protocols for LODT \cite{23} and SCOT \cite{30}, these are not practical to implement with current technology. On the one hand, the LODT protocol of Ref. \cite{23} requires preparation of two qudits in a maximally entangled state and their secure transmission over long distances. On the other hand, the SCOT protocol of Ref. \cite{30} requires preparation of Bennett-Brassard 1984 (BB84) \cite{8} qubits and their secure transmission over long distances as long as hundreds of kilometers if the time length of the regions \( R_i \) is of only a few milliseconds – and, if Bob does not have quantum memories to store the received qubits, the preparation and transmission of a large number of BB84 states within a very short time – not greater than the time length of the regions \( R_i \).

In this paper we introduce an unconditionally secure SCOT protocol that is practical to implement with current technology: it requires preparation, transmission and measurement of BB84 qubits at a single location, and secure transmission of classical information over long distances, but it does not require quantum memories or long-distance quantum communication. Furthermore, the quantum communication in our protocol can take an arbitrarily long time, while still giving Bob the freedom to chose his input \( b \) only slightly in the past of \( R_0 \) and \( R_1 \). This is the first practical and unconditionally secure protocol of a cryptographic task whose unconditional security necessitates both quantum theory and relativity. Our SCOT protocol can also be used to implement unconditionally secure relativistic quantum bit commitment.

This paper is organized as follows. In Sec. II we describe the setting of relativistic quantum cryptography that applies to our protocol, we define the task of SCOT, and we provide some mathematical notation. We present our SCOT protocol in Sec. III. We show in Sec. IV that our protocol is unconditionally secure. Some extensions of our protocol are discussed in Sec. V in particular to deal with losses and errors. We discuss in Sec. VI how our SCOT protocol can be used to implement unconditionally secure quantum relativistic bit commitment. We conclude in Sec. VII.

II. PRELIMINARIES

A. The setting

The general model of relativistic quantum cryptography was introduced by Kent \cite{1,13}. Here, we detail the specific setting of our protocol. Alice and Bob live in Minkowski – or approximately Minkowski – spacetime. Alice (Bob) consists of three different agents, denoted by \( A, A_0, A_1, (B, B_0, B_1) \), each controlling a secure laboratory adjacent to the space location \( L, L_0, L_1 \), having finite spatial extension with set of three-dimensional coordinates \( \Delta L^A, \Delta L^B_0, \Delta L^B_1 \), respectively. Alice and Bob agree on a particular reference frame \( F \) with spacetime coordinates \((t, x, y, z)\), where the first entry is temporal, and where we set units in which the speed of light through vacuum is unity. Here we consider \( L = (0,0,0) \) and \( L_i = (-(−1)^ih,0,0) \), with the maximum length extension of any laboratory being much smaller than \( h \), for \( i \in \{0,1\} \).

We assume the processing of classical and quantum information within each laboratory to be secure and without errors, and the transmission of classical or quantum systems between laboratories being free of errors and losses. The communication between Alice’s (Bob’s) agents is done through authenticated and secure classical channels, which can be implemented with previously shared secret keys. There are classical channels between Alice’s and Bob’s adjacent agents, i.e. between the pairs \((A,B),(A_0,B_0)\) and \((A_1,B_1)\). There is a single quantum channel between \( A \) and \( B \). Note that the only quantum communication is between agents at the same location, an important difference with the setting in Ref. \cite{30}.

B. Definition of SCOT

As mentioned above, SCOT \cite{30} is a relativistic variant of one-out-of-two oblivious transfer \cite{31}, defined as follows. Alice and Bob agree on two spacelike separated spacetime regions \( R_0 \) and \( R_1 \). Bob’s agent \( B \) inputs \( b \in \{0,1\} \) in the intersection of the causal pasts of all the spacetime points of \( R_0 \) and \( R_1 \). For \( i \in \{0,1\} \), Alice’s agent \( A_i \) inputs \( x_i \in \{0,1\}^n \) in the causal past of a spacetime point \( Q_i \) of \( R_i \) – previously agreed by Alice and Bob. The goal of the SCOT protocol is that \( B_0 \) obtains \( x_0 \) in \( R_0 \). A SCOT protocol is secure against Alice if she cannot learn \( b \) anywhere in spacetime; it is secure against Bob if the probability that \( B_0 \) obtains \( x_0 \) in \( R_0 \) and \( B_1 \) obtains \( x_1 \) in \( R_1 \) goes to zero as a function of some security parameter, which here we take to be the parameter \( n \) \cite{31}.

Here we consider \( R_i = \{ (t,1) | h \leq t \leq h + \Delta h, l \in \Delta L_i^B \} \) and \( Q_i = (h, -(−1)^ih,0,0) \), for \( i \in \{0,1\}, \) where \( h > 0 \) and \( \Delta h > 0 \). We note that \( R_i \) includes the spacetime point \( Q_i \), for \( i \in \{0,1\} \). By definition of SCOT, \( R_0 \) and \( R_1 \) must be spacelike separated; hence, \( \Delta h \) must be smaller than the shortest time that light takes to travel between \( \Delta L_0^B \) and \( \Delta L_1^B \), requiring \( \Delta h < 2h \). \( B \) generates \( b \) within his laboratory in the past light cone of the spacetime point \( P = (0,0,0,0) \). For \( i \in \{0,1\} \), \( A_i \) inputs \( x_i \) within her laboratory in the past light cone of \( Q_i \).
C. Notation

We define \( [n] = \{1, 2, \ldots, n\} \). We denote the jth bit entry of a string \( a \in \{0, 1\}^n \) by \( a^j \), for \( j \in [n] \). When applied to bits (bit strings) \( \oplus \) denotes (bitwise) sum modulo 2. We denote the complement of a bit \( a \) by \( \bar{a} = a \oplus 1 \), and of a bit \( a^j \) by \( \bar{a}^j \). \( D_0 = \{0\}, \{1\} \) and \( D_1 = \{0, 1\} \) denote the computational and Hadamard bases, respectively, where \( |\bar{a}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^a|1\rangle) \), for \( a \in \{0, 1\} \).

III. A PRACTICAL AND UNCONDITIONALLY SECURE SCOT PROTOCOL

We present an unconditionally secure SCOT protocol, consisting of two main stages. Stage I includes quantum communication between the laboratories adjacent to location \( L \) and can be completed within any finite time in the past light cone of \( P \). Stage II includes fast classical processing and communication between Alice’s and Bob’s agents at the locations \( L, L_0 \) and \( L_1 \), as well as classical communication between Alice’s (Bob’s) agents at the locations \( L \) and \( L_i \) for \( i \in \{0, 1\} \). Steps 1–6 take place in the past of \( P \). Our protocol is illustrated in Fig.

A. Stage I

1. \( A \) generates the strings \( r_0, r_1, s \in \{0, 1\}^n \) randomly and securely and sends copies to \( A_i \), who receives them in the past light cone of \( Q_i \), for \( i \in \{0, 1\} \).

2. \( A \) prepares a set of \( 2n \) qubits \( \{A_i^j\}_{j \in \{0, 1\}} \) in BB84 states \( |\Phi^+\rangle \). For \( j \in [n] \), the qubit pair \( A^j_i = A_0^j A_1^j \) is prepared in the state

\[
|\psi^{\oplus}_{r_0 r_1}\rangle_{A_0^j A_1^j} = |r_0^j\rangle_{A_0^j} \otimes |r_1^j\rangle_{A_1^j}.
\]

We note that \( s^j \in \{0, 1\} \) indicates which qubit in the pair \( A^j \) is prepared in the basis \( D_0 \) and which one in \( D_1 \). The qubits prepared in the basis \( D_i \) encode the string \( r_i \), for \( i \in \{0, 1\} \). For \( i \in \{0, 1\} \) and \( j \in [n] \), \( A \) sends the qubits \( A_i^j \) with their labels \( i, j \) to \( B \).

3. Before receiving the qubits from \( A \), \( B \) randomly chooses a bit \( c \). For \( i \in \{0, 1\} \) and \( j \in [n] \), \( B \) measures the qubits \( A_i^j \) in the basis \( D_c \), obtaining the bit outcomes \( d_i^j \), defining \( d_i = (d_1^i, d_2^i, \ldots, d_n^i) \). For \( i \in \{0, 1\} \), \( B \) sends \( c, d_0 \) and \( d_1 \) to \( B_i \), with reception in the past of \( Q_i \).

B. Stage II

4. \( B \) generates his bit input \( b \) and sends the bit \( b' = c \oplus b \) to \( A \).

5. For \( i \in \{0, 1\} \), \( B \) sends \( b \) to \( B_i \), who receives it in the past of \( Q_i \).

6. For \( i \in \{0, 1\} \), \( A \) sends \( b' \) to \( A_i \), who receives it in the past of \( Q_i \).

7. For \( i \in \{0, 1\} \), \( A_i \) generates \( x_i \) within her laboratory in the past of \( Q_i \), and gives \( t_i = r_i \oplus b' \otimes x_i \) and \( s \) to \( B_i \) at \( Q_i \).

8. Within the region \( R_0 \), \( B_b \) uses \( s, d_0, d_1 \), and \( c \) to obtain \( (d_1^i, \ldots, d_n^i) \), which equals \( r_c \). Then, \( B_b \) outputs \( y_b = r_c \oplus t_b \), which equals \( x_c \).

C. Comments and variations

We note that \( B \) has the freedom to choose \( b \) after all the received qubits have been measured. This is useful in situations where the quantum communication takes a long time (e.g., several hours), while Bob wants to decide which message to obtain within a short time (e.g., a fraction of a second) in the past of \( R_0 \) and \( R_1 \). Furthermore, Alice has the freedom to generate her inputs in real time; i.e., \( A \) can generate \( x_i \) slightly in the past of \( Q_i \), for \( i \in \{0, 1\} \).

Different variations of the above protocol can be considered. For example, in one variation \( B \) does not send \( b \) to his agents and \( B_i \) acts assuming that \( b = i \), for \( i \in \{0, 1\} \). In another variation, \( A \) generates \( x_0 \) and \( x_1 \) in the past of \( P \) and sends \( x_i \) to \( A_i \), who receives it in the past of \( Q_i \), for \( i \in \{0, 1\} \).

IV. SECURITY ANALYSIS

A. Security against Alice

The only communication from Bob to Alice consists in the bit \( b' = c \oplus b \). Since \( c \) is random and Bob’s laboratories and classical channels are secure, Alice cannot obtain any information about \( b \). Thus, our protocol is perfectly secure against Alice.

B. Security against Bob

Security against Bob follows from Minkowski causality and the monogamy of entanglement. In a general cheating strategy by Bob, agent \( B \) introduces an ancilla \( E \) of arbitrary finite dimension in some fixed pure state \( |\chi\rangle \), and applies a unitary operation \( U \) on \( A E \) to obtain

\[
|\Psi_{r_0 r_1}^{s}\rangle_{B_0 B_1 B'} = U_{A E} |\Psi_{r_0 r_1}^{s}\rangle_A |\chi\rangle_E,
\]

where \( A = A_0^1 A_1^1 \cdots A_0^n A_1^n \), \( A E = B_0 B_1 B' \), the systems \( B_0, B_1, B' \) have arbitrary finite dimensions, and where

\[
|\Psi_{r_0 r_1}^{s}\rangle_A = \bigotimes_{j=1}^{n} |\psi_{r_0 j r_1}^{s^j}\rangle_{A_0^j A_1^j}.
\]
is the state that $B$ receives from $A$. Then, $B$ applies a projective measurement $\{R^b\}_{b' \in \{0,1\}}$ on $B'$ and sends the outcome $b'$ to $A$. For $i \in \{0,1\}$, $B$ sends $b'$ and $B_i$ to $B_i$. $B_i$, after receiving $s$ from $A_i$ at $Q_i$, applies a projective measurement $M_{iab'} = \{\Pi_{iab'}^n\}_{b' \in \{0,1\}}$ on $B_i$ and obtains the outcome $e_i$. Given that $t_i = r_{i\oplus b'} \oplus \xi_i$, the goal of the measurement $M_{iab'}$ is to obtain a string $e_i$ that equals $r_{i\oplus b'}$ with high probability, so that $B_i$ outputs $e_i \oplus t_i$, which equals $\xi_i$ with high probability. Thus, Bob’s cheating probability is $p_n = P(e_0 = r_{b'}, e_1 = r_{b'})$, which is given by

$$p_n = \frac{1}{2^n} \sum_{r_0, r_1, s, b'} \langle \Phi^+_{r_0r_1} | \Pi_{iab'}^n \otimes \Pi_{iab'}^n \otimes R^{b'} | \Phi^+_{r_0r_1} \rangle.$$  \hspace{1cm} (4)

Since the regions $R_0$ and $R_1$ at which Bob’s agents $B_0$ and $B_1$ must produce their outputs are spacelike separated, it follows from Minkowski causality that, as given by Ref. \[1\], $B_0$ and $B_1$ must obtain their outputs from measurements on disjoint systems $B_0$ and $B_1$, which could have only interacted in the intersection of the past light cones of at least one point in $R_0$ and one point in $R_1$, i.e, in the past light cone of $P'$ (see Fig. 1). Then, from the monogamy of entanglement, the measurement outcomes obtained by $B_0$ and $B_1$ cannot both be very correlated to Alice’s inputs $r_0$ and $r_1$, which implies an upper bound on $p_n$. We show below that for any cheating strategy by Bob we have

$$p_n \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n.$$  \hspace{1cm} (5)

Thus, $p_n \to 0$ exponentially with $n$, meaning that our protocol is unconditionally secure.

It remains as an open question whether the security bound (5) is tight. We describe in section IV C the best cheating strategy by Bob that we have found, which achieves $p_n = \left(\frac{4}{9}\right)^n$.

1. Proof of bound (5)

The main technical part of this paper is the proof of bound (5). Our proof is a variation of the proof of a bound for the monogamy-of-entanglement game given in Ref. \[33\]. First, we note that it is equivalent in our protocol if agent $A$ prepares in the past of $P$ the state

$$|\Phi\rangle_{CA} = \bigotimes_{j=1}^{n} (|\Phi^+\rangle_{C_i^jA_i^j} \otimes |\Phi^+\rangle_{C_i^jA_i^j}),$$  \hspace{1cm} (6)

where $C = C^1C^2 \cdots C^n$, $C^j = C_i^jC_{i+1}^j$ and $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$. Then, in the past of $P$, $A$ sends $A$ to $B$ and measures $C^j$ in the basis $\{|\psi^+_{r_0j}\rangle\}_{r_0 \in \{0,1\}}$ for $j \in [n]$. With probability $\frac{1}{2^n}$, $A$ measures $C^j$ in the state $|\psi^+_{r_0j}\rangle_{C_i^jA_i^j}$ and the pair of qubits $A^j$ received by $B$ collapse into the state $|\psi^+_{r_0j}\rangle_{A_i^jA_i^j}$. Bob’s unitary operation $U$ in his cheating strategy commutes with Alice’s
measurements. Thus, we can consider that the global system $CB_0B_1B'$, before Alice’s and Bob’s measurement is implemented, is in the state

$$|\Psi\rangle_{CB_0B_1B'} = (1_C \otimes U_{B_0B_1B'})|\Phi\rangle_{C,A}|\chi_E, \quad (7)$$

where we recall that $B_0B_1B' = AE$, $E$ is an ancilla, and $B_0, B_1$ and $B'$ have arbitrary finite Hilbert space dimensions. Then, $A$ measures $C$ in the orthonormal basis $\{|\Psi_{r_0r_1}\rangle\}_{r_0,r_1\in\{0,1\}}$ according to her random value of $s \in \{0,1\}^n$. With probability $\frac{1}{2^n}$, $A$ measures $|\Psi_{r_0r_1}\rangle_C$ and $B_0B_1B'$ projects into the state $|\Phi^r_{r_0r_1}\rangle_{B_0B_1B'}$. Then, $B$ applies the projective measurement $\{R^b_i\}_{b_i\in\{0,1\}}$ on $B'$ and obtains the bit outcome $b_i$, which he sends to $A$. $A$ sends $b'$ and $B_i$ to $B_1$, for $i \in \{0,1\}$. After receiving $s$, agent $B$ applies the projective measurement $\mathcal{M}_{ab}$ on $B_1$ at $Q_1$. Thus, Bob’s cheating probability $p_n$ given by $41$ equals

$$p_n = \frac{1}{2^n} \sum_s \text{Tr}(T_s\Psi), \quad (8)$$

where $\Psi = (|\Psi\rangle\langle\Psi|)_{CB_0B_1B'}$, and

$$T_s = \frac{1}{2^n} \sum_{b'=0}^1 (D^b_s)_{CB_0B_1} \otimes (R^b_i)_{B'}, \quad (9)$$

with

$$D^b_s = \sum_{r_0,r_1} (|\Psi^s_{r_0r_1}\rangle\langle\Psi^s_{r_0r_1}|)_C \otimes (\Pi^r_{0b})_{B_0} \otimes (\Pi^{r_1b_1'})_{B_1},$$

for $b' \in \{0,1\}$.

We derive bound $3$ with the help of two lemmas of Ref. 33. Before stating these lemmas we provide some useful notation. We denote by $H$ the Hilbert space of the global system $CB_0B_1B'$, which as said before is arbitrary but finite dimensional. We denote by $\mathcal{L}(H)$ and by $\mathcal{P}(H)$ the sets of linear operators and of positive semidefinite operators on $H$, respectively. For $A, B \in \mathcal{L}(H)$, the expression $A \geq B$ means that $A - B \in \mathcal{P}(H)$. For $A \in \mathcal{L}(H)$, $||A||$ denotes the Schatten $\infty$-norm of $A$, which gives the largest singular value of $A$, and which coincides with its largest eigenvalue if $A \in \mathcal{P}(H)$.

**Lemma 1.** (Ref. 33) Let $A, B, L \in \mathcal{L}(H)$ such that $A'L \geq B'L$. Then, it holds that $||AL|| \geq ||BL||$.

**Lemma 2.** (Ref. 33) Let $D_1, D_2, \ldots, D_N \in \mathcal{P}(H)$, and let $\{s_k\}_{k \in [N]}$ be a set of $N$ mutually orthogonal permutations of $[N]$. Then

$$\left| \sum_{i \in [N]} D_i \right| \leq \sum_{k \in [N]} \max_{i \in [N]} \|D_{s_k(i)}\|^{\frac{1}{2}}.$$  

It follows from Lemma 1 that for $A, A', B, B' \in \mathcal{P}(H)$ satisfying $A' \geq A$ and $B' \geq B$, it holds that $\|\sqrt{A'}\sqrt{B'}\| \geq \|\sqrt{A}\sqrt{B}\|$ 33. Thus, if $A, A', B, B'$ are projectors on $H$ satisfying $A' \geq A$ and $B' \geq B$ then $\|A'B'\| \geq \|AB\|$. We use this property below.

To use Lemma 2 we consider the set of permutations of $s$ given by $s \rightarrow s_k = s \oplus k$, for $k \in \{0,1\}^n$. This is a set of $2^n$ mutually orthogonal permutations, that is, $s_k \neq s_k'$ if $k \neq k'$ for all $s \in \{0,1\}^n$.

We have

$$p_n = \frac{1}{2^n} \text{Tr}\left( \sum_s T_s\Psi \right)$$

$$= \frac{1}{2^n} \sum_s \left\| \sum_{b'=0}^1 D^b_s \otimes R^b_i \right\|$$

$$\leq \frac{1}{2^n} \sum_s \max_{b'} \left\| \sum_{k \in [N]} D^b_{s_k} \right\|$$

$$\leq \frac{1}{2^n} \max_{b'} \sum_{k \in [N]} \|D^b_{s_k}\|$$

$$\leq \frac{1}{2^n} \max_{b'} \sum_{k \in [N]} \|F^b_s G^b_{s_k}\|,$$

where in the first line we used the linearity of the trace, in the second line we used the definition of the Schatten $\infty$-norm, in the third line we used 33, in the fourth line we used that $\{R^b_i, R^b_i\}$ is a projective measurement, and in the last line we used Lemma 2 and the fact that $D^b_s$ and $D^b_{s_k}$ are projectors.

We define the projectors

$$F^b_s = \sum_{r_0,r_1} (|\Psi^s_{r_0r_1}\rangle\langle\Psi^s_{r_0r_1}|)_C \otimes (\Pi^r_{0b})_{B_0} \otimes 1_{B_1},$$

$$G^b_{s_k} = \sum_{r_0,r_1} (|\Psi^s_{r_0r_1}\rangle\langle\Psi^s_{r_0r_1}|)_C \otimes 1_{B_0} \otimes (\Pi^{r_1b_1'})_{B_1},$$

for $b' \in \{0,1\}$ and $s, k \in \{0,1\}^n$. We see that they satisfy $D^b_s \leq F^b_s$ and $D^b_{s_k} \leq G^b_{s_k}$. Thus, we have from Lemma 1 that

$$\|D^b_s\| \leq \|F^b_s\| G^b_{s_k},$$

$$\|D^b_{s_k}\| \leq \|F^b_s\| G^b_{s_k},$$

where the equality follows from the property $\|A\|^2 = ||AA'|| = ||A||^2$ for any $A \in \mathcal{L}(H)$ 33 and from the fact that $F^b_s$ and $G^b_{s_k}$ are projectors. We show in Appendix A that

$$\|F^b_s G^b_{s_k}\| = \left(\frac{1}{2}\right)^{w_k},$$

where $w_k$ is the Hamming weight of $k$. Thus, since for any $b' \in \{0,1\}$ and for a fixed $k$, the value of $\|F^b_s G^b_{s_k}\|$ is the same for any $s \in \{0,1\}^n$, we have from 12, 14 and 15 that

$$p_n \leq \frac{1}{2^n} \sum_k \left(\frac{1}{\sqrt{2}}\right)^{w_k}.\quad (16)$$
There are exactly \( \binom{n}{k} \) values of \( k \in \{0, 1\}^n \) with Hamming weight \( \omega \). Thus, from (15), we obtain

\[
p_n \leq \frac{1}{2} \sum_{\omega=0}^{n} \binom{n}{\omega} \left( \frac{1}{\sqrt{2}} \right)^\omega
= \left( \frac{1}{2} + \frac{1}{2\sqrt{2}} \right)^n,
\]

which is the claimed bound (15).

**C. A cheating strategy by Bob without the use of any quantum channels or quantum memories**

We present a cheating strategy by Bob that achieves \( p_n = \left( \frac{1}{2} \right)^n \). Interestingly, Bob’s agents do not need any quantum memories or quantum channels to perform this strategy.

Bob’s agent \( B \) gives the bit \( b' = 0 \) to Alice’s agent \( A \). Thus, Bob’s agent \( B_i \) must obtain the string \( r_i \) in \( R_i \), for \( i \in \{0, 1\} \). In the past of \( P \), agent \( B \) applies a projective measurement on the pair of qubits \( A^0 \) in the orthonormal basis defined by the following states:

\[
\begin{align*}
|\xi_{00}\rangle &= \frac{\sqrt{\frac{3}{2}}}{2} |\psi^0_{00}\rangle - \frac{1}{2\sqrt{3}} (-|\psi^0_{01}\rangle + |\psi^0_{10}\rangle + |\psi^0_{11}\rangle) \\
|\xi_{01}\rangle &= \frac{\sqrt{\frac{3}{2}}}{2} |\psi^0_{01}\rangle - \frac{1}{2\sqrt{3}} (|\psi^0_{00}\rangle - |\psi^0_{10}\rangle + |\psi^0_{11}\rangle) \\
|\xi_{10}\rangle &= \frac{\sqrt{\frac{3}{2}}}{2} |\psi^0_{10}\rangle - \frac{1}{2\sqrt{3}} (-|\psi^0_{00}\rangle + |\psi^0_{01}\rangle + |\psi^0_{11}\rangle) \\
|\xi_{11}\rangle &= -\frac{\sqrt{\frac{3}{2}}}{2} |\psi^0_{11}\rangle - \frac{1}{2\sqrt{3}} (|\psi^0_{00}\rangle + |\psi^0_{01}\rangle + |\psi^0_{10}\rangle). 
\end{align*}
\]

We denote the outcomes by \( |\xi_{ij}\rangle \), where \( i^j \equiv (i^0_0, i^0_1) \in \{0, 1\}^2 \), for \( j \in \{0, 1\} \). Agent \( B \) sends the outcomes \( i^j \) with their labels \( j \) to his agent \( B_j \), who receives them in the past of \( Q_j \), for \( j \in \{0, 1\} \) and \( i \in \{0, 1\} \). After receiving \( s \) at \( Q_j \) from \( A_j \), agent \( B_j \) guesses that Alice prepared the pair of qubits \( A^j \) in the state \( |\psi^0_{ij}\rangle \) if \( s_j = 0 \) or in the state \( |\psi^1_{ij}\rangle \) if \( s_j = 1 \), where \( f(00) = 01, f(01) = 11, f(10) = 10, f(11) = 10 \). Thus, \( B_j \) outputs \( e_j = (e_1^j, e_2^j, \ldots, e_n^j) \), with \( e_i^j = l_i^j \) if \( s_i = 0 \), or with \( e_i^j \) being the \( i \)-th entry of \( f(P) \) if \( s_i = 1 \). Bob’s cheating probability \( p_n = P(e_0 = r_0, e_1 = r_1) \) following this strategy is \( p_n = \left( \frac{1}{2} \right)^n \), where

\[
p = \frac{1}{8} \left( |\langle \psi^0_{00}, & |\psi^0_{01} \rangle + |\psi^0_{10} \rangle + |\psi^0_{11} \rangle |^2 |
\begin{align*}
+|\langle \psi^0_{11} \rangle \xi_{11} \rangle|^2 + |\langle \psi^0_{10} \rangle \xi_{10} \rangle|^2 \\
+|\langle \psi^1_{11} \rangle \xi_{11} \rangle|^2 + |\langle \psi^1_{10} \rangle \xi_{10} \rangle|^2 \\
+|\langle \psi^1_{11} \rangle \xi_{11} \rangle|^2 + |\langle \psi^1_{10} \rangle \xi_{10} \rangle|^2 \right). 
\end{align*}
\]

From the definition (11) for the states \( |\psi^s_{r_0 r_1} \rangle \), we can easily derive the relations

\[
\begin{align*}
|\psi^0_{00} \rangle &= \frac{1}{2} \left( |\psi^0_{00} \rangle + |\psi^0_{01} \rangle + |\psi^0_{10} \rangle + |\psi^0_{11} \rangle \right) \\
|\psi^0_{01} \rangle &= \frac{1}{2} \left( |\psi^0_{00} \rangle + |\psi^0_{01} \rangle - |\psi^0_{10} \rangle - |\psi^0_{11} \rangle \right) \\
|\psi^1_{00} \rangle &= \frac{1}{2} \left( |\psi^0_{00} \rangle - |\psi^0_{01} \rangle + |\psi^0_{10} \rangle - |\psi^0_{11} \rangle \right) \\
|\psi^1_{11} \rangle &= \frac{1}{2} \left( |\psi^0_{00} \rangle - |\psi^0_{01} \rangle - |\psi^0_{10} \rangle + |\psi^0_{11} \rangle \right). 
\end{align*}
\]

Using (18) – (20) it is straightforward to compute \( p = \frac{3}{4} \). Thus, this cheating strategy by Bob achieves a success probability \( p_n = \left( \frac{1}{2} \right)^n \), as claimed.

**V. EXTENSIONS OF OUR SCOT PROTOCOL**

We discuss possible extensions of the SCOT protocol of Sec. I. First, we note that in the SCOT protocol of Sec. II Bob is guaranteed that the pair of qubits \( A^0 \) encodes the bits \( x_i^0 \) and \( x_i^1 \) via the bits \( r_i^0 \) and \( r_i^1 \). In a straightforward extension of our protocol, among the \( 2n \) qubits that Alice prepares from the BB84 set (\( n \) in the computational basis and \( n \) in the Hadamard basis), she chooses randomly the positions of the qubits encoding the bits \( r_i^j \), for \( i \in \{0, 1\} \) and \( j \in \{0, 1\} \). Clearly, this modification in the protocol cannot make it easier for Bob to cheat; hence, unconditional security remains. We leave as an open question whether this extended protocol achieves strictly better security against Bob.

Secondly, the SCOT protocol of Sec. II considers the ideal situation in which there are not any errors during the protocol and that there are not any losses of the transmitted quantum systems. This protocol is straightforwardly extended to deal with these problems.

**A. Dealing with losses**

To deal with losses, \( B \) reports to \( A \) in the past of \( P \) a set \( S \subseteq \{n\} \) of labels \( j \) of two-qubit systems \( A^j = A^0_j A^1_j \) for which both \( A^0_j \) and \( A^1_j \) activate a detection. The protocol continues as the original one, but with input strings \( s^S, r_0^S, r_1^S, d_0^S, d_1^S, x_0^S, x_1^S \) instead of \( s, r_0, r_1, d_0, d_1, x_0, x_1 \), where \( a^S \in \{0, 1\}^N \) denotes the restriction of \( a \in \{0, 1\}^n \) in \( S \), and where \( N = |S| \). Security against Bob follows from bound (5) but with security parameter \( N \) instead of \( n \). Since Bob’s agent \( B \) gives Alice the bit \( b' = c \oplus b \), in order to guarantee security against Alice, \( B \) must make sure that announcing the detection events does not leak any information about the measurement choice \( c \), which implies that no information about Bob’s input \( b \) is given to Alice. For this, \( B \) must experimentally verify that the detection probabilities of the two-qubit systems \( A^j \) received from \( A \) are independent of whether they are measured in the basis \( D_0 \otimes D_0 \) or in the basis \( D_1 \otimes D_1 \).
B. Dealing with errors

In order to deal with noise in the system we extend the setting of SCOT. As before, in the past light cone of $Q_1$, Alice’s agent $A_i$ has the input $x_i \in \{0, 1\}^n$, for $i \in \{0, 1\}$. In the past light cone of $P'$, Bob’s agent $B$ has as an input $b \in \{0, 1\}$. However, now, the goal of the protocol is that Bob obtains a string $y_b \in \{0, 1\}^n$ in $R_b$ such that $y_b$ differs from $x_b$ in at most $\gamma n$ bit entries, for some $\gamma \in (0, 1)$ agreed in advance by Alice and Bob. As before, security against Alice means that she cannot learn $b$ anywhere in spacetime. Security against Bob means that Bob cannot obtain a string $y_0$ in $R_0$ and a string $y_1$ in $R_1$, such that $y_i$ differs from $x_i$ in at most $\gamma n$ bit entries for both $i = 0$ and $i = 1$. According to the motivation of SCOT outlined in the Introduction, this means that Bob cannot access both computers, one being accessed in $R_0$ and the other one being accessed in $R_1$, where the corresponding computer can be accessed if the password provided by Bob’s agent differs from the original password given by Alice’s agent in at most $\gamma n$ bit entries. It can be shown that our protocol remains unconditionally secure as long as $\gamma$ is small enough. In particular, we show below that our protocol remains secure if $\gamma < 0.015$.

Bob’s cheating probability in the extended setting, the probability that both agents $B_0$ and $B_1$ output valid passwords, is

$$p_n^\gamma = \frac{1}{2^n} \sum_{q \in Q_n^\gamma} \sum_s \text{Tr}(T_s^q \Psi), \quad (21)$$

where $\Psi = (|\Psi\rangle\langle\Psi|)_{CB_0B_1B'}$, with $|\Psi\rangle_{CB_0B_1B'}$ given by (7), and $T_s^q$ is a projector given by

$$T_s^q = \sum_{b' = 0}^1 (P_{s,b'}^q)_{CB_0B_1} \otimes (R_{b'})_{B'}, \quad (22)$$

with

$$D_{s,b'}^q = \sum_{r_0, r_1} \left( (|\Psi_{r_0,r_1}\rangle\langle\Psi_{r_0,r_1}|)_{C} \otimes (\Pi_{s,b'}^{r_0}\otimes q^r)_{B_0} \times \right.$$ \left.$$ \times (\Pi_{1,s,b'}^{r_0}\otimes q^r)_{B_1} \right); \quad (23)$$

and where $q = (q_0, q_1) \in Q_n^\gamma \equiv \{(q_0, q_1)|q_i \in \{0, 1\}^n, W(q_i) \leq \gamma n, i = 0, 1\}$, with $W(q_i)$ denoting the Hamming weight of $q_i$, for fixed $\gamma \in [0, 1]$. We show in Appendix (12) that

$$p_n^\gamma \leq |Q_n^\gamma| \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n. \quad (24)$$

For $\gamma \leq \frac{1}{2}$, we have $|Q_n^\gamma| \leq 2^{2\gamma h(\gamma)}$, which is shown in Sec. 1.4 of Ref. [34], where $h(\gamma) = -\gamma \log_2 \gamma - (1 - \gamma) \log_2 (1 - \gamma)$ is the binary entropy of $\gamma$. Thus, we have from (23) that

$$p_n^\gamma \leq 2^{2\gamma h(\gamma)} \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n. \quad (25)$$

For $\gamma < 0.015$, we have $2^{2\gamma h(\gamma)} \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n < 1$: hence, $p_n^\gamma \to 0$ exponentially with $n$, which means unconditional security for $\gamma < 0.015$.

VI. UNCONDITIONALLY SECURE BIT COMMITMENT FROM SCOT

In bit commitment, Bob commits a bit $b$ to Alice by giving her some proof of his commitment but without telling her the value of $b$, until he unveils his commitment to her. The security guarantee is twofold: Alice cannot learn $b$ before Bob unveils, and if Alice accepts Bob’s unveiled bit $b$ as valid, she is guaranteed that Bob was committed to $b$ at least from some time $t'$ in the past. Similarly to the SCOT protocol of Ref. [20], the SCOT protocol presented here can be used to implement unconditionally secure relativistic bit commitment, as follows (see Fig. 4). To commit to $b \in \{0, 1\}$, Bob runs the SCOT protocol with input $b$. To unveil the committed bit $b$, Bob’s agent $B_b$ obtains $x_b$ within $R_b$, and then sends $x_b$ immediately to Alice’s adjacent agent $A_b$. $A_b$ accepts $b$ as a valid commitment only if she receives $x_b$ from $B_b$ within the time interval $[h, h + \Delta h]$, i.e., in the boundary of $R_b$ that is adjacent to her laboratory.

It follows from the security of SCOT that this bit commitment protocol is unconditionally secure. Security against Alice follows trivially because our SCOT protocol is secure against Alice; hence, Alice does not know $b$ until Bob unveils.

Security against Bob means that if $A_b$ accepts $b$ as a valid commitment then $A_b$ is guaranteed that Bob was committed to $b$ from $t'$, the time coordinate of $P'$, which is the spacetime point with the greatest time coordinate (in the frame $F$) that lies in the intersection of the past light cones of a point in $R_0$ and a point in $R_1$. Security against Bob follows from Minkowski causality and the monogamy of entanglement, similarly as in the security analysis of our SCOT protocol. Namely, in any cheating strategy, Bob must send in the past of $P'$ a system $B$ to agent $B_i$, who measures the system using the information received from Alice’s agent $A_i$, and obtains his guess for her input $x_i$, in $R_i$, for $i \in \{0, 1\}$. The probability $p_n$, given by (24), that Bob obtains both $x_0$ in $R_0$ and $x_1$ in $R_1$ is upper bounded by (26). This means that for any cheating strategy followed by Bob, if we denote $p^i$ as the probability that Bob unveils $b = i$ successfully, for $i \in \{0, 1\}$, it holds that $p^0 + p^1 \leq 1 + p_n$. Since $p_n \to 0$ exponentially with $n$, our bit commitment protocol is unconditionally secure against Bob.

VII. CONCLUSION

We presented a practical unconditionally secure SCOT protocol, where spatially separated agents need only communicate classical information, while quantum communication is only between agents at the same location,
and which can be implemented with current technology. This is the first practical and unconditionally secure protocol of a cryptographic task whose unconditional security is possible in a quantum relativistic world, but impossible in a classical world, or in a quantum non-relativistic world [20, 31].

ACKNOWLEDGMENTS

DPG thanks Stefano Pironio for helpful conversations. This work was begun when DPG was 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. It was completed when DPG was at IRIF, Université Paris Diderot, supported by the project ERC QCC.

Appendix A: Proof of Eq. (15)

We show (15) for the case \( b' = 0 \). The proof for the case \( b' = 1 \) follows straightforwardly by interchanging \( B_0 \) and \( B_1 \). To simplify notation, in what follows we take \( \Pi^0_{ls} = \Pi^0_{lak}, \Pi^0_{ls} = \Pi^0_{lak}, F_s = F^0_s \) and \( G_{sk} = G^0_{sk} \). For fixed \( s \) and \( k \), we denote by \( s^j \) and \( s^j_k \) the \( j \)th entries of \( s \) and \( s_k \), respectively, and we define the sets \( \tau = \{ j \in [n] | s^j \neq s^j_k \} \) and \( \tau_c = \{ j \in [n] | s^j = s^j_k \} \). Let \( \omega_k \) be the Hamming weight of \( k \), hence, \( |\tau| = \omega_k \). Using the definitions (11), (12), and (13) of the main text, we express \( F_s \) and \( G_{sk} \) by

\[
F_s = \sum_{r_0,r_1} \left[ \bigotimes_{j \in \tau} \left( \left( |r_0^j\rangle\langle r_0^j| \right) C_{s^j} \otimes \left( |\hat{r}_1^j\rangle\langle \hat{r}_1^j| \right) C_{s^j} \right) \times \right. \\
\times \bigotimes_{j \in \tau_c} \left( \left( |r_0^j\rangle\langle r_0^j| \right) C_{s^j} \otimes \left( |\hat{r}_1^j\rangle\langle \hat{r}_1^j| \right) C_{s^j} \right) \times \\
\left. \bigotimes (\Pi^0_{lak})_{B_0} \otimes I_{B_1} \right],
\]

\[
G_{sk} = \sum_{r_0,r_1} \left[ \bigotimes_{j \in \tau} \left( \left( |r_0^j\rangle\langle r_0^j| \right) C_{s^j_k} \otimes \left( |\hat{r}_1^j\rangle\langle \hat{r}_1^j| \right) C_{s^j_k} \right) \times \right. \\
\times \bigotimes_{j \in \tau_c} \left( \left( |r_0^j\rangle\langle r_0^j| \right) C_{s^j_k} \otimes \left( |\hat{r}_1^j\rangle\langle \hat{r}_1^j| \right) C_{s^j_k} \right) \times \\
\left. \bigotimes I_{B_0} \otimes (\Pi^0_{lak})_{B_1} \right]. \tag{A1}
\]

Below we compute \( F_s G_{sk} F_s \). We express the left-hand operator \( F_s \) in terms of the dummy variables \( r_0 \) and \( r_1 \), and the right-hand one in terms of \( z_0 \) and \( z_1 \). The operator \( G_{sk} \) is expressed in terms of \( w_0 \) and \( w_1 \). From the definitions of \( \tau \) and \( \tau_c \), we have that \( s^j = s^j_k \) and \( \bar{s}^j = s^j \) for \( j \in \tau \), and \( s^j_k = s^j \) and \( \bar{s}^j_k = \bar{s}^j \) for \( j \in \tau_c \). Using these properties and \( \Pi^0_{ls} \Pi^0_{ls} = \delta_{r_0,z_0} \Pi^0_{ls} \), since \( \{ \Pi^0_{ls} \}_{r_0} \) is a projective measurement, we obtain

\[
F_s G_{sk} F_s = \sum_{r_0,r_1,w_0,w_1,z_0,z_1} \left[ \bigotimes_{j \in \tau} \left( \left( |r_0^j\rangle\langle r_0^j| \right) C_{s^j} \otimes \left( |\hat{r}_1^j\rangle\langle \hat{r}_1^j| \right) C_{s^j} \right) \times \right.
\]
\[
\times \left( \left( |\hat{w}_1^j\rangle\langle \hat{w}_1^j| \right) C_{s^j} \otimes \left( |\hat{w}_0^j\rangle\langle \hat{w}_0^j| \right) C_{s^j} \right) \times \\
\times \left. \bigotimes_{j \in \tau_c} \left( \left( |r_0^j\rangle\langle r_0^j| \right) C_{s^j} \otimes \left( |\hat{r}_1^j\rangle\langle \hat{r}_1^j| \right) C_{s^j} \right) \times \\
\times \bigotimes \left( \left( |\hat{r}_0^j\rangle\langle \hat{r}_0^j| \right) C_{s^j} \otimes \left( |\hat{r}_1^j\rangle \langle \hat{r}_1^j| \right) C_{s^j} \right) \times \\
\bigotimes \left( \left( |r_0^j\rangle\langle r_0^j| \right) C_{s^j} \otimes \left( |\hat{r}_1^j\rangle\langle \hat{r}_1^j| \right) C_{s^j} \right) \right]. \tag{A2}
\]

Then we use that \( \sum_{a=0}^{1} |a\rangle\langle a| = \sum_{a=0}^{1} |\hat{a}\rangle\langle \hat{a}| = 1 \) (the identity on a qubit) to obtain, after summing over \( r_1, w_0, z_1 \), that

\[
F_s G_{sk} F_s = \sum_{r_0,w_1} \left[ \bigotimes_{j \in \tau} \left( \left( |r_0^j\rangle\langle r_0^j| \right) C_{s^j} \otimes \left( |\hat{w}_1^j\rangle\langle \hat{w}_1^j| \right) C_{s^j} \right) \times \right.
\]
\[
\times \left. \bigotimes_{j \in \tau_c} \left( \left( |r_0^j\rangle\langle r_0^j| \right) C_{s^j} \otimes \left( |\hat{w}_0^j\rangle\langle \hat{w}_0^j| \right) C_{s^j} \right) \right]. \tag{A3}
\]

Since \( \langle \hat{r}_0^j | \hat{w}_1^j \rangle^2 = \frac{1}{2} \) and \( |\tau| = \omega_k \), it follows that

\[
F_s G_{sk} F_s = \left( \frac{1}{2} \right)^{\omega_k} \sum_{r_0,w_1} \left[ \bigotimes_{j \in \tau} \left( \left( |r_0^j\rangle\langle r_0^j| \right) C_{s^j} \otimes \left( |\hat{r}_0^j\rangle\langle \hat{r}_0^j| \right) C_{s^j} \right) \times \right.
\]
\[
\times \left. \bigotimes_{j \in \tau_c} \left( \left( |r_0^j\rangle\langle r_0^j| \right) C_{s^j} \otimes \left( |\hat{r}_0^j\rangle\langle \hat{r}_0^j| \right) C_{s^j} \right) \right]. \tag{A4}
\]

Using that \( \{ \Pi^0_{ls} \}_{r_0} \) and \( \{ \Pi^0_{lak} \}_{w_1} \) are projective measurements, it is straightforward to see from (A4) that \( 2^{\omega_k} F_s G_{sk} F_s \) is a projector. Thus, \( \| 2^{\omega_k} F_s G_{sk} F_s \| = 1 \), which implies (15). The bound (5) of the main text and security against Bob follow.
Appendix B: Proof of bound (24)

We show (24). We follow closely the proof of bound [5]. We have

\[
p_n^2 = \frac{1}{2^n} \sum_{q \in Q_n^*} \text{Tr} \left( \sum_s T_s \Psi \right) \leq \frac{1}{2^n} \sum_{q \in Q_n^*} \left\| \sum_s T_s \Psi \right\| = \frac{1}{2^n} \sum_{q \in Q_n^*} \left\| \sum_{b=0}^{b'=1} D_{s b}^{q b'} \otimes R_{b}^{q b'} \right\| \leq \frac{1}{2^n} \sum_{q \in Q_n^*} \max_b \left\| \sum_s D_{s b}^{q b'} \right\| \leq \frac{1}{2^n} \sum_{q \in Q_n^*} \max_b \sum_k \max_s \left\| D_{s b}^{q b'} \right\|^{2},
\]

where in the first line we used the linearity of the trace, in the second line we used the definition of the Schatten \(\infty\)-norm \(\|\|\), in the third line we used [22], in the fourth line we used that \(\{B^0, R\}^s\) is a projective measurement, and in the last line we used Lemma 2 and the fact that \(D_{s b}^{q b'}\) and \(D_{s k}^{q k'}\) are projectors.

We define the projectors

\[
F_{s b}^{q b'} = \sum_{r_0, r_1} \left( \langle \Psi_{r_0 r_1}^s | \langle \Psi_{r_0 r_1}^s | C \otimes (\Pi_{b=0}^{b'=1} \otimes q_s) B_0 \otimes I_{B_1} \right),
\]

\[
G_{s k}^{q k'} = \sum_{r_0, r_1} \left( \langle \Psi_{r_0 r_1}^s | \langle \Psi_{r_0 r_1}^s | C \otimes I_{B_0} \otimes (\Pi_{b=0}^{b'=1} \otimes q_s) \right),
\]

which satisfy \(D_{s b}^{q b'} \leq F_{s b}^{q b'}\) and \(D_{s k}^{q k'} \leq G_{s k}^{q k'}\). Thus, from Lemma 1 we have that

\[
\| D_{s b}^{q b'} \|^{2} \leq \| F_{s b}^{q b'} \|^{2} = \| F_{s b}^{q b'} \|^2 \leq \| F_{s b}^{q b'} G_{s k}^{q k'} \|^2.
\]

where the equality follows from \(\| A \|^2 = \| AA \|^2 = \| A \|^2\), satisfied for any linear operator \(A\) [33], and from the fact that \(F_{s b}^{q b'}\) and \(G_{s k}^{q k'}\) are projectors.

Following the proof of (13) in Appendix A it is straightforward to show that

\[
\| F_{s b}^{q b'} G_{s k}^{q k'} \| = \left( \frac{1}{2} \right)^{\omega_k},
\]

where \(\omega_k\) is the Hamming weight of \(k\). Thus, from (13), (33) and (34), we obtain

\[
p_n^2 \leq \frac{1}{2^n} \sum_{q \in Q_n^*} \sum_k \left( \frac{1}{\sqrt{\omega_k}} \right)^n \leq \left( Q_n^* \right)^{-\frac{n}{2}} \left( \frac{1}{\sqrt{\omega_k}} \right)^n = \left( Q_n^* \right)^{-\frac{n}{2}} \left( \frac{1}{2} + \frac{1}{2 \sqrt{2}} \right)^n,
\]

which is the claimed bound (24).
[24] A. Chailloux and I. Kerenidis, in *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, New York, 2011) pp. 354–362.

[25] A. Chailloux and I. Kerenidis, in *50th Annual IEEE Symposium on Foundations of Computer Science, 2009 FOCS ’09* (IEEE, New York, 2009) pp. 527–533.

[26] A. Chailloux, I. Kerenidis, and J. Sikora, *Quantum Information and Computation* **13**, 158 (2013), arXiv:1007.1875.

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

[28] R. Colbeck and A. Kent, *Phys. Rev. A* **73**, 032320 (2006).

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

[30] D. Pitalúa-García, *Phys. Rev. A* **93**, 062346 (2016).

[31] S. Even, O. Goldreich, and A. Lempel, *Commun. ACM* **28**, 637 (1985).

[32] J. Kilian, in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, STOC ’88* (ACM, New York, 1988) pp. 20–31.

[33] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, *New J. Phys.* **15**, 103002 (2013).

[34] J. H. van Lint, *Introduction to coding Theory* (Springer, Berlin, 1999).

[35] J. S. Bell, *Speakable and unspeakable in quantum mechanics* (Cambridge University Press, Cambridge, 1987).