Quantum non-locality, causality and mistrustful cryptography

Muhammad Nadeem
Department of Basic Sciences,
School of Electrical Engineering and Computer Science
National University of Sciences and Technology (NUST)
H-12 Islamabad, Pakistan
muhammad.nadeem@seecs.edu.pk

Here we propose a general relativistic quantum framework for cryptography that exploits the fascinating connection of quantum non-locality and special theory of relativity with cryptography. The underlying principle of unconditional security is causality and two-fold quantum non-local correlations: first entanglement swapping and then teleportation over causally independent entangled systems. We show that the proposed framework has following remarkable and novel features in mistrustful cryptography: (i) It helps in defining a new notion of oblivious transfer where both the data transferred and the transfer position remains oblivious. (ii) The authenticity and integrity of the data transferred is guaranteed by the fundamental principles of quantum theory instead of computational complexity. (iii) It directly leads to unconditionally secure and deterministic two-sided two-party computation which is currently considered to be impossible. (iv) the proposed framework turns out to be asynchronous ideal coin tossing with zero bias which has not been achieved previously. (v) The same framework also implies unconditionally secure bit commitment. Finally, the combination of quantum non-locality and theory of relativity as discussed here can easily be generalized to multiparty setting that could be used to solve other mistrustful cryptographic tasks such as secret sharing and key agreement securely.

In the last few years, researchers have shown great excitement in the area of relativistic quantum cryptography\textsuperscript{1-9,10-28} where causal structure of Minkowski space time or impossibility of superluminal signaling gives power to relativistic quantum cryptography in defining tasks that are not possible in non-relativistic setting, especially in mistrustful cryptography. These interesting developments give further hope for defining a more general framework in relativistic quantum theory that would be sufficient to solve all the cryptographic tasks securely.

Kilian showed that classical oblivious transfer\textsuperscript{29-32} (OT) is a basic building block for many mistrustful cryptographic protocols, for example, two-party secure computations\textsuperscript{33}. However, since computationally hard classical protocols can be broken, various protocols for OT based on non-relativistic\textsuperscript{34} and relativistic quantum theory\textsuperscript{22} have also been proposed. In existing non-relativistic quantum OT protocols, only data remains oblivious while sender/receiver can be well aware of transfer position. On the other hand, in relativistic OT protocol\textsuperscript{22}, the data can be completely determined by sender/receiver while they remain oblivious about the transfer position.

Moreover, in all previously proposed OT protocols, receiver cannot be certain that the data he received has not been altered during the protocol. Hence, currently it is known that 1-out-of-2 oblivious transfer and deterministic two-sided two-party secure computations (TPSC) are impossible in classical/non-relativistic quantum cryptography\textsuperscript{35,36}. These impossibility results have also been extended to relativistic quantum cryptography\textsuperscript{37}. However, relativistic quantum
cryptography gives hope for secure implementation of nondeterministic two-sided TPSC and hence variable-bias coin tossing\textsuperscript{38}. Moreover, asynchronous ideal coin tossing is impossible in classical/non-relativistic quantum cryptography\textsuperscript{39} while only synchronous ideal coin tossing is possible if impossibility of superluminal signaling is considered\textsuperscript{40}.

Furthermore, bit commitment is another very important and basic cryptographic protocol that is impossible in classical/non-relativistic quantum cryptography\textsuperscript{41-43} but has been proved to be possible in relativistic quantum theory\textsuperscript{10,24,26}. These no-go theorems show the limitations of classical/non-relativistic quantum cryptography while possibility results show that relativity adds its weight, and hence gives more power, towards quantum cryptography to evade such no-go theorems.

At this point, we would like to discuss an important quantum mechanical concept, non-locality, which has an interesting connection with cryptography and cryptanalysis. Non-local Einstein-Podolsky-Rosen (EPR) type correlations\textsuperscript{44} solves the very basic ingredient of cryptography, QKD\textsuperscript{45}, that gives unconditionally secure means for secret communications between distant parties. On the other hand, in mistrustful cryptography, a dishonest party can exploit the non-locality (EPR types quantum attacks) to cheat successfully\textsuperscript{35,41-43}.

In this work, we exploit the fascinating connections of quantum non-locality and relativity with cryptography and show that the combination of relativity with non-locality favors cryptography rather than cryptanalysis. We propose a general relativistic quantum framework for cryptography and show that the proposed framework proves to be a building block for many interesting mistrustful cryptographic protocols that are considered to be impossible. For example, it directly leads to (i) a new notion of OT where both the data transferred and the transfer position remain oblivious, (ii) deterministic two-sided TPSC, (iii) asynchronous ideal coin tossing with zero bias, and (iv) unconditionally secure bit commitment.

In fact, the proposed framework could be used to solve other mistrustful cryptographic tasks with guarantee of authenticity and integrity of the data transferred along with unconditional security against Mayers and Lo-Chau (MLC) attacks\textsuperscript{35,39, 41-43} and quantum attacks based on non-local instantaneous computations\textsuperscript{46}. The proposed framework attains unconditional security through combination of causality and two-fold quantum non-local correlations: first entanglement swapping\textsuperscript{47} and then teleportation\textsuperscript{48} over causally independent entangled systems.

**Mistrustful Cryptography**

In a standard mistrustful cryptography, communicating parties do not trust each other and security is concerned against these parties only (internal eavesdropping); everything outside secure laboratories of the communicating parties is assumed to be insecure. This subject is very divers and has gained a lot of attention especially in quantum setup; however, we focus here only those cryptographic primitives which could be used as a building block for implementing many other protocols. For example, (i) OT and (hence) two-sided TPSC and ideal coin tossing and (ii) unconditionally secure bit commitment.

**Oblivious transfer:** OT was originally defined by Rabin where sender Alice sends a 1-bit message to the receiver Bob who can only receive the message with probability no more than half\textsuperscript{29}. The security of the protocol relies on the fact that Bob can find out whether or not he got the 1-bit message from Alice after the completion of protocol but Alice remains oblivious about it. In a related notion, 1-out-of-2 OT, Alice sends two 1-bit messages to Bob who can only receive one of them and remains ignorant about the other while Alice remains entirely oblivious.
to which of the two messages Bob received\textsuperscript{30,31}. It is shown later by Crépeau that both of these notions of OT are equivalent\textsuperscript{32}.

**Two-sided two-party secure computation:** Two-sided TPSC enables two distant parties Alice and Bob to compute a function $f(a,b)$ where $a$ and $b$ are inputs from Alice and Bob respectively. The protocol is said to be secure if it fulfills following security requirements: (i) both Alice and Bob learn output of $f(a,b)$ deterministically. (ii) Alice learns nothing about Bob’s input $b$ and (iii) Bob learns nothing about Alice’s input $a$. The no-go theorems for secure two-party computations are based on possibilities that one party, say Bob, can also compute $f(a,b')$ where $b' \in \{b_1, b_2, \ldots\}$. That is, Bob can cheat by computing the value of the function $f$ for all of his inputs $b'$ and hence violate the security requirement of single input from each party. Lo\textsuperscript{35} has shown that Bob can do this by applying unitary transformations on his own quantum system $\mathcal{H}_B$.

That is, the system $\mathcal{H}_B$ kept by Bob must be an eigenstate of the measurement operator that he uses for computing $f(a,b)$. Being an eigenstate, $\mathcal{H}_B$ remains undisturbed by Bob’s measurement that makes computation of $f(a,b')$ feasible.

**Ideal quantum coin tossing:** Coin tossing\textsuperscript{49} is another fundamental primitive function in communication that allows distant mistrustful parties Alice and Bob to agree on a random data. Coin tossing is said to be ideal if it follows: (i). It results in three possible outcomes $\gamma$: $\gamma_+ = +$, $\gamma_- = -$ or $\gamma_{\pm} = \text{invalid}$. (ii). Outcome $\gamma_+$ and $\gamma_-$ occurs with equal probability $P_+ = P_- = 1/2$ and both parties have equal cheating probabilities, $P_{+}^{A} = P_{-}^{B} = P_{\gamma}$, which means that the coin tossing is fair. (iii). If both parties are honest, the outcome $\gamma_{\pm} = \text{invalid}$ never occurs; $P_{\pm} = 0$. (iv). If any one of the parties is dishonest, the outcome invalid occurs with probability $P_{\pm} = 1$.

**Bit commitment:** A bit commitment is also an important cryptographic scheme between two mistrustful parties, committer (Alice) and receiver (Bob), where Alice commits herself to a specific bit $a$ in the commitment phase. In this phase or during the scheme, Bob should not be able to extract the bit value. In the revealing phase, however, it must be possible for Bob to know the genuine bit value $a$ with absolute guarantee when Alice reveals the committed bit and Alice should not be able to change her mind about the value of the bit $a$.

**Proposed framework for relativistic quantum cryptography**

In a relativistic quantum cryptographic setup proposed by Adrian Kent, background space time is approximately Minkowski and communicating parties Alice and Bob are not the individuals but are agencies having distributed agents throughout the space time. The agencies are assumed to possess secure sites in a given inertial frame and can communicate with each other by sending quantum/classical signals at near light speed $c=1$. Moreover, the agencies have unlimited powers of information processing and efficient technology (quantum computers) and are restricted from cheating by principals of quantum theory only. Alice and Bob can communicate with their respective agents securely; however, all the quantum/classical channels between Alice and Bob are insecure. Both agencies have powers of instantaneous computation and time for information processing at their secure sites is assumed to be negligibly small. If one of the agencies sends a quantum/classical signal from point $(x,0)$, then after some fixed time $t > 0$, the light-like separated agents from the sender in some given inertial frame can receive the signal on a special sphere of radius $t$ and centered at $x$.

In the proposed framework for relativistic quantum cryptography we assume that Alice has two agents $A_1$ and $A_2$ while Bob has three agents $B'$, $B_1$ and $B_2$ respectively. Suppose Alice possesses secure site at $(x_a, t_a)$, space-like separated from Bob and his agent $B'$ at positions
(x_b, t_b) and (x_b', t_b') respectively such that t_a = t_b = t_b' = t, x_b < x_a < x_b' and x_a = (x_b' - x_b)/2. However, Bob’s agents B_1 and B_2 are at arbitrary positions (x_b, t_b) and (x_a, t_a) in the causal future of Alice respectively. Alice only knows the directions where B_1 and B_2 can receive the data but not their exact positions; they are light-like separated from Alice. Similarly, Alice’s agents A_1 and A_2 are light-like separated from Bob in his causal future at positions (x_a, t_a) and (x_a', t_a').

Alice, Bob, and his agent B’ share quantum system \( H_S = H_A \otimes H_B \otimes H_{AB} \), where \( H = |\phi\rangle \) is kept by Bob while entangled systems \( H_{AB} = H_A \otimes H_B \) and \( H_{AB'} = H_A \otimes H_{B'} \) are shared with Alice by Bob and B’ respectively. Alice and Bob give input data \( u, u' \in \{00, 01, 10, 11\} \) and \( u_b, u_b' \in \{00, 01, 10, 11\} \) to the shared quantum system \( H_S \) by applying unitary transformations \( U^{u_a} U^{u_b} \) and \( U^{u_b} U^{u_b'} \) on \( H_S \) respectively as follows: Alice applies transformations \( U^{u_a} U^{u_b} \) on \( H_A \), performs Bell state measurement (BSM) on \( H_A \otimes H_A \), and publically announces her BSM result \( \alpha\alpha' \). As a result, Bob and his agent B’ get entangled; \( H_{BB'} = H_B \otimes H_{B'} \). Simultaneously, Bob applies transformations \( U^{u_b} U^{u_b'} \) on \( H = |\phi\rangle \), teleports the quantum state \( U^{u_b} U^{u_b'} |\phi\rangle \) to B’ by applying local Bell operator \( \beta_b \) on \( H \otimes H_B \), and publically announces his BSM result \( \beta\beta' \). He also sends \( U^{u_b} U^{u_b'} |\phi\rangle \) to either A_1 or A_2. Instantly B’ (measures if required and) sends his system \( H_{B'} = U^I U^{u_b} U^{u_b'} |\phi\rangle \) to Alice where \( U^I \) is teleportation encoding. Alice applies further unitary transformations \( U^{u_a} U^{u_b} \) and sends \( U^{u_a} U^{u_b} U^I U^{u_b} U^{u_b'} |\phi\rangle \) to either B_1 or B_2.

Alice and Bob validate the protocol if non-local quantum correlations between Alice’s transformation \( U^{u_a} U^{u_b} \), Bob’s transformation \( U^{u_b} U^{u_b'} \), and teleportation encoding \( U^I \) are consistent with BSM results (\( \alpha\alpha' \) and \( \beta\beta' \)) of Alice and Bob on initially shared quantum system \( H_S \). This framework is secure in general and against Alice/Bob in particular through quantum non-local correlations and causal structure of Minkowski space time.

Here \( H, H_{AB}, \) and \( H_{AB'} \) can be any higher dimensional quantum systems where Alice and Bob can execute any set of suitable unitary transformations \( U^{u_a} U^{u_b} \) and \( U^{u_b} U^{u_b'} \) respectively. However, to make the analysis simple, we assume in the rest of the discussion that \( H = |\phi\rangle = |\pm\rangle \) where \( |\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2} \) while both \( H_A \otimes H_B = (C^2) \otimes (C^2) \) and \( H_A \otimes H_{B'} = (C^2) \otimes (C^2) \) are 2-qubit maximally entangled systems with Bell basis

\[
|u_m u_n\rangle = \frac{|0\rangle|u_m\rangle + (-1)^{u_n}|1\rangle|u_n\rangle}{\sqrt{2}}
\]

where \( u_m \) and \( u_n \in \{0, 1\} \) and \( \oplus \) denotes addition with mod 2. The unitary transformations used by Alice and Bob will be \( U^{u_a} U^{u_b} = \sigma_{z}^{u_a} \sigma_{x}^{u_b} \) and \( U^{u_b} U^{u_b'} = \sigma_{z}^{u_b} \sigma_{x}^{u_b'} \) respectively where they agree on a code: if sender S (Alice/Bob) applies unitary transformation \( I, \sigma_x, \sigma_z, \) or \( \sigma_z \sigma_x \) on the quantum state \( |\phi\rangle \in H_S \), he/she is actually giving input data 00, 01, 10 or 11 to the system \( H_S \) respectively. Since \( \sigma_{z}^{u_a} \sigma_{x}^{u_b'} |\phi\rangle = \sigma_{z}^{u_a} \sigma_{x}^{u_b'} |\phi\rangle = |\phi\rangle \), where we ignore the overall phase factor, we restate the code as follows: to send data \( u, u', \in \{00, 01\} \) or \( u, u', \in \{10, 11\} \), sender S (Alice/Bob) applies corresponding Pauli transformations \( \sigma_{z}^{u_a} \sigma_{x}^{u'}, \sigma_{z}^{u'} \sigma_{x}^{u_a} \) on the
quantum state $\left| \phi \right\rangle \in \mathcal{H}_S$. With two dimensional quantum registers, explicit procedure for our proposed framework is described below:

1. At $t=0$, Bob and his agent $B'$ prepare EPR pairs $\left| u_a u_b \right\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and $\left| u'_a u'_b \right\rangle \in \mathcal{H}_A' \otimes \mathcal{H}_B'$ respectively and each sends first qubit to Alice.

2. At $t=x_a - x_b$, Alice applies Pauli transformation $\sigma_a \in \{\sigma^x, \sigma^y, \sigma^z\}$ on $\left| u_a \right\rangle$, performs BSM on qubits $\left| u_a \right\rangle$ and $\left| u'_a \right\rangle$ and publically announces her BSM result $\alpha \alpha'$.

3. At the same time $t=x_a - x_b$, Bob prepares a qubit $\pm = \left| \phi \right\rangle$, applies Pauli transformation $\sigma_b \in \{\sigma^x, \sigma^y, \sigma^z\}$ and teleports the state $\sigma_b \left| \phi \right\rangle$ to $B'$ over EPR channel $\left| u_b u'_b \right\rangle \in \mathcal{H}_B \otimes \mathcal{H}_B'$ established between them due to BSM of Alice. As a result, $\mathcal{H}_B'$ becomes one of the corresponding four possible states $\left| \psi \right\rangle = \sigma_j \sigma_b \left| \phi \right\rangle$ where teleportation encoding $\sigma_j \in \{I, \sigma_x, \sigma_y, \sigma_z\}$ is unknown to everyone. Simultaneously, Bob publically announces his BSM $\beta \beta'$, sends $\sigma_b \left| \phi \right\rangle$ to either $A_1$ or $A_2$ while $B'$ measures and sends $\left| \psi \right\rangle$ to Alice.

4. At $t=2(x_a - x_b)$, Alice measures $\left| \psi \right\rangle$, applies unitary transformations corresponding to her input data $\sigma_a \in \{\sigma^x, \sigma^y, \sigma^z\}$ on $\left| \psi \right\rangle$ and immediately sends the outcome of two-sided computation $\left| \psi' \right\rangle = \sigma_a \left| \psi \right\rangle = \sigma_a \sigma_b \sigma_b \left| \phi \right\rangle$ to either $B_1$ or $B_2$.

5. $B_i$ receives the state $\left| \psi' \right\rangle$ from Alice, measures in $\{+, -\}$ basis and gets joint measurement outcome $\psi'$.

**Figure 1:** Relativistic quantum framework for cryptography in 1+1 Minkowski space time. Entangled systems $\mathcal{H}_{AB}$ and $\mathcal{H}_{A'B'}$ are represented by red particles while particle in green at Bob’s site represents $\mathcal{H} = \left| \phi \right\rangle$. At time $t=x_a - x_b$, swapped entangled system $\mathcal{H}_{BB'}$ is represented by blue color where dotted arrow shows teleportation from Bob to $B'$. For two-sided computations and bit commitment, Alice’s agents $A$ and $A'$ ensure that Bob and $B'$ are at announced space-like separated positions $x_b$ and $x'_b$ respectively.
For two-sided computations (TPSC & coin tossing) and bit commitment, the proposed framework strictly requires that Bob and his agent B’ should have operated from their designated space-like separated positions \((x_b, t_b)\) and \((x'_b, t'_b)\). Alice can insure this by assigning two more agents \(A\) and \(A'\) at disjoint sites nearby \((x_a, t_a)\) and \((x'_a, t'_a)\) respectively. Instead of sending \(H_a\) and \(H_a'\) directly to Alice, Bob and B’ will share these quantum systems with \(A\) and \(A'\) respectively who then pass these systems to Alice securely.

Applications of proposed relativistic framework in mistrustful cryptography

In this section, we show that the proposed framework solves the problem of OT, deterministic two-sided TPSC, asynchronous ideal coin tossing with zero bias and unconditionally secure bit commitment.

To implement OT, deterministic two-sided TPSC, and asynchronous ideal coin tossing with zero bias, let’s suppose shared quantum system \(H_S\) is known to both Alice and Bob (priorly decided somewhere in causal past) and they use the code as follows: unitary transformation \(\{00, 01\} \in \{0, 1\} \otimes \{\sigma_x, \sigma_y, \sigma_z\}\) while those of \(\{10, 11\} \in \{0, 1\} \otimes \{\sigma_x, \sigma_y, \sigma_z\}\) correspond to classical 2-bit string \(u, u' \in \{0, 1\}\), Alice commits herself to the bit value \(a = 0\) if \(u = 0\) and \(a = 1\) if \(u = 1\). In the revealing phase, Alice sends \(\{\psi\} = \sigma_a|\psi\rangle = \sigma_a \sigma_b |\varphi\rangle\) where her commitment is encoded in unitary transformation \(\sigma_a\).

Oblivious Transfer: Our proposed framework helps in defining a new notion of OT where receiver \(R\) (Alice/Bob) remains oblivious about both the data transferred and the transfer position; he/she may know both the transferred messages \(\sigma_x |\varphi\rangle = \sigma_a \sigma_b |\varphi\rangle\) but remains oblivious about the genuine one. On the other hand, the sender \(S\) (Alice/Bob) cannot learn the transfer position even after the protocol is completed. Moreover, \(R\) accepts the data \(\sigma_s\) only if he is certain that data has come from legitimate sender \(S\), by measuring time lapse and testifying non-local quantum correlations established through local operations. Finally, in our secure OT protocol, \(S\) cannot change the data he/she started with otherwise \(R\) rejects the protocol – that is something not possible in all the previously proposed OT protocols.

Two-sided two-party secure computation: Our proposed framework also results in secure and deterministic two-sided TPSC of function \(f(\sigma_a, \sigma_b, |\varphi\rangle)\) where \(\sigma_a\) and \(\sigma_b\) are unitary transformations on quantum system \(H_S = H_A \otimes H_B \otimes H_{AB}\) applied by Alice and Bob respectively. According the code, when Alice and Bob apply these transformations on \(|\varphi\rangle\), they actually provide input \(u, u' \rightarrow \sigma_a\) and \(u, u' \rightarrow \sigma_b\) to the shared quantum system \(H_S\) respectively. At the end of the computation, both parties know the same definite outcome

\[
f(\sigma_a, \sigma_b, |\varphi\rangle) = \sigma_a \sigma_b |\varphi\rangle
\]
where teleportation encoding $\sigma_i$ is non-locally correlated with local operations of Alice and Bob on the shared quantum system $\mathcal{H}_S$. Bob’s input $u_b,u_b'$ remains totally random to Alice while Bob also remains oblivious about Alice’s input $u_a,u_a'$. Finally both Alice and Bob get same unbiased outcome of function $f(\sigma_a,\sigma_b;|\varphi\rangle)$ deterministically. As we show in security analysis, neither Alice nor Bob can cheat by altering their inputs to the shared quantum system $\mathcal{H}_S$ and (hence) cannot cheat to get outcome of function $f(\sigma_a,\sigma_b;|\varphi\rangle)$ as they want.

**Ideal quantum coin tossing:** Proposed framework is in fact an asynchronous ideal quantum coin tossing where both parties have equal resources and the protocol offers zero bias. That is, it fulfils all the security requirements of ideal coin tossing: $P_+ = P_- = 1/2$, zero cheating probabilities for Alice and Bob ($P_d^A = P_d^B = 0$), $P_z = 0$ if both parties are honest and $P_z = 1$ if any one of the parties tries cheating. Although both parties give input simultaneously at time $t = x_a - x_b$, however, proposed framework is asynchronous in the sense that Bob and Alice reveal their inputs at different times; $t = x_a - x_b$ and $t = 2(x_a - x_b)$ respectively.

**Bit commitment:** As for as bit commitment is concerned, Bob need not to send $\sigma_b|\varphi\rangle$ to A. We show in the security analysis that (i) Committer Alice cannot alter her commitment $\sigma_a$ (or $u_a,u_a'$ or $a$ ) after announcement of her BSM result $aa'$. (ii) Receiver Bob remains unable to know Alice’s committed bit $a$ during the protocol. (iii) Framework allows Bob to know the definite Alice’s commitment $\sigma_a \in \{1,\sigma_z\}$ ($u_a,u_a' \in \{00,01\}$ or $a = 0$) or $\sigma_a \in \{\sigma_x,\sigma_z,\sigma_x\}$ ($u_a,u_a' \in \{10,11\}$ or $a = 1$) at the end of protocol. (iv) Two-fold quantum non-local correlations guarantee Bob to reject the protocol if Alice tries to alter her commitment in the revealing phase.

Proposed framework can be modified for computational basis with transformations $\sigma_z \in \{\sigma_z,\sigma_x,\sigma_x^{10},\sigma_x^{01}\}$ on the state $|\varphi\rangle$. These operations by sender guarantee that receiver can get only either $\sigma_z \in \{1,\sigma_z\}$ or $\sigma_z \in \{\sigma_x,\sigma_z,\sigma_x\}$ but not the exact Pauli operator. That is, receiver can successfully guess either sender has sent data $u_a,u_a' \in \{00,10\}$ or $u_a,u_a' \in \{01,11\}$ but not the definite 2-bit string $u_a,u_a'$.

**Security analysis**

In this section, we show that the power of two-fold quantum non-local correlations and special theory of relativity bounds both parties to remain fair and act according to the agreed codes: use genuine transformations, priorly agreed basis, and respond within allocated times. The underlying principle of unconditional security in the proposed framework is causality and two-fold quantum non-local correlations: first entanglement swapping and then teleportation over causally independent entangled systems. That is, for each $\sigma_a$ and every value of Alice’s BSM result $aa'$, there will be unique swapped Bell state $|u_b,u_b'\rangle$ and hence unique teleportation encoding $\sigma$ corresponding to BSM result of Bob $\beta\beta'$ as shown in table 1 & 2.

From $\sigma_b|\varphi\rangle$, $|\psi\rangle = \sigma_a|\sigma_b|\varphi\rangle$, and measuring time lapse, Alice can verify that whether Bob’s actions are consistent with his BSM result $\beta\beta'$ and corresponding teleportation operator $\sigma_i$ or not. On the other hand, if Alice’s input $\sigma_a$ is consistent with Alice’s BSM result $aa'$, swapped entangled state $|u_b,u_b'\rangle$ (hence corresponding teleportation operator $\sigma_i$) and Alice replied within allocated time, Bob verifies that Alice is fair otherwise aborts the protocol.
In our proposed framework, security against mistrustful Alice and Bob lies in following requirements: (i) Alice (Bob) should not be able to know the definite Bob’s input $\sigma_b$ (Alice’s input $\sigma_a$) even at the end of protocol. (ii) Before or during the protocol, Alice (Bob) should not know the position of $A_i$ ($B_i$) where Bob (Alice) will send the data until her (his) agents receive the data. Similarly, Alice (Bob) should not know the position of $B_i$ ($A_i$) even at the end of protocol. (iii) Proposed framework should not allow Alice (Bob) to alter her (his) input $\sigma_a$ ($\sigma_b$) during the protocol and hence should allow Alice (Bob) to get joint measurement outcome $|\psi'\rangle = |\sigma_{a},\sigma_{b}\rangle |\varphi\rangle$ of her (his) choice. (iv) Proposed framework should be resistant to Mayers and Lo-Chau attacks\textsuperscript{41-43} where Alice can delay her input and try to influence measurement outcome $|\psi'\rangle = |\sigma_{a},\sigma_{b}\rangle |\varphi\rangle$ by getting information about Bob’s input $\sigma_b$. (v) Proposed framework should evade entanglement-based quantum attacks through non-local instantaneous computations. In other words, Alice responding from other than her announced position must be detected while Bob and $B'$ must not be able to know Alice’s input $\sigma_a$ during the protocol; before time $t=2(x_a-x_b)$ where Alice reveals her oblivious input.

(i) Data remains oblivious: As for as Bob’s data is concerned, Alice cannot find the exact value of $\sigma_b$ deterministically during or after the protocol – by measuring $\sigma_b|\varphi\rangle$, Alice can find that either $u_bu'_b\in\{00,11\}$ or $u_bu'_b\in\{10,11\}$ corresponding to Bob’s operations $\sigma_b\in\{I,\sigma_x\}$ or $\sigma_b\in\{\sigma_z,\sigma_z\sigma_x\}$ but remains ignorant about the specific classical 2-bit string $u_bu'_b$ (or bit $b=\oplus u_b\oplus u'_b$) Bob has sent.

Similarly, Bob cannot differentiate between Alice’s transformations $\sigma^u_x\sigma^v_z$ or $\sigma^u_x\sigma^v_z\sigma^w_z10u_w$ on $|\psi\rangle$ since $\sigma^w_z\sigma^v_z10u_w|\psi\rangle = \sigma^w_z\sigma^v_z\sigma^u_x10u_w|\psi\rangle$ where $|\psi\rangle = |\pm\rangle$. That is, if Bob gets $\psi' = \psi$ then he will be sure that Alice has applied $\sigma_a\in\{I,\sigma_x\}$ on $|\psi\rangle$ while $\sigma_a\in\{\sigma_z,\sigma_z\sigma_x\}$ in case of $\psi'\neq\psi$. As a result, Bob can find (or bit $a=\oplus u_b\oplus u'_b$) Alice has sent.

Similarly, Bob cannot differentiate between $\sigma^u_x\sigma^v_z|\psi\rangle = \sigma^w_z\sigma^v_z10u_w|\psi\rangle$ if $|\psi\rangle\in\{00,11\}$, can Bob find exact operation by Alice on $|\psi\rangle$ by choosing different basis; computational one rather than agreed Hadamard basis? Interestingly, answer is NO. If B’ deviates from agreed basis and sends $|\psi\rangle\in\{00,11\}$ to Alice, Alice will measure in Hadamard basis and get either $\psi = +$ or $\psi = -$ with equal probability unknown to Bob. As a result, Bob will not be able to know whether Alice has applied transformations $\sigma_a\in\{I,\sigma_x\}$ or $\sigma_a\in\{\sigma_z,\sigma_z\sigma_x\}$ on $|\psi\rangle$. By doing this, Bob will not get any advantages but rather he will allow Alice to cheat; since he cannot conclude now whether Alice’s actions are consistent with non-local correlations or not.

(ii) Transfer positions remain oblivious: Before or during the protocol, Alice (Bob) cannot predict the position where Bob (Alice) will send the data. The choice of transfer position is totally random and Alice (Bob) can only know the transfer position $A_i$ ($B_i$) receives the data from Bob (Alice). Similarly, Alice (Bob) remains ignorant about transfer position $B_i$ ($A_i$) even after the protocol is complete - $B_i$ ($A_i$) do not communicate with Alice (Bob) during the protocol. Hence Alice (Bob) cannot compute time lapse or distance of the receiver $B_i$ ($A_i$).
(iii) Zero biasness: As we have stated earlier, underlying principle for unconditional security is quantum non-locality and causality; actions of space-like separated agents are causally independent and hence they cannot simulate their actions at some fixed time. Inputs $\sigma_a$ and $\sigma_b$ from Alice and Bob and their announced BSM results $\alpha \alpha'$ and $\beta \beta'$, result in unique swapped Bell state $|u_a u_b\rangle$ and hence unique teleportation encoding $\sigma_i$. At the end of protocol, both parties know quantum states $\sigma_b|\phi\rangle$ and $|\psi\rangle = \sigma_i \sigma_b|\phi\rangle$. Hence both parties can validate or abort the protocol by looking whether the inputs $\sigma_a$ and $\sigma_b$ are consistent with non-local correlations among BSM results $\alpha \alpha'$ and $\beta \beta'$ and corresponding teleportation operator $\sigma_i$ or not.

Let’s consider a simplest possible situation where $|u_a u_b\rangle = 00$, $|u_a u_b\rangle = 00$, $\sigma_a = I$ (and $\sigma_b = \sigma_x$), and Alice announces BSM result $\alpha \alpha' = 00$ then $|u_a u_b\rangle = 00(|u_a u_b\rangle = 01)$. Now if BSM result of Bob is $\beta \beta' = 11$ while teleporting $\sigma_i|\phi\rangle$ to B’, then $\sigma_i = \sigma_z \sigma_x$ (and $\beta_i = \sigma_x$). In the revealing phase, if Alice acts fairly and replies $|\psi\rangle = I \sigma_a \sigma_b |\phi\rangle$ ($|\psi\rangle = \sigma_a \sigma_b |\phi\rangle$), Bob will verify that Alice’s input $\sigma_a \in \{I, \sigma_z\}$ is consistent with teleportation encoding $\sigma_i = \sigma_a \sigma_z$ (and $\beta_i = \sigma_z$) by comparing $\sigma_b|\phi\rangle$ and $|\psi\rangle = \sigma_b |\phi\rangle$. However, if Alice tries to cheat by using different values of $\sigma_a = \sigma_z$ (and $\sigma_a = \sigma_z \sigma_x$) and sends $|\psi\rangle = \sigma_z \sigma_a |\phi\rangle$ ($|\psi\rangle = \sigma_z \sigma_a \sigma_b |\phi\rangle$). Bob will extract $|u_a u_b\rangle = 10$ ($|u_a u_b\rangle = 11$) and hence different teleportation encoding $\sigma_i = \sigma_z$ (and $\sigma_i = I$). As a result, Bob will abort the protocol by forcing Alice’s input $\sigma_a \in \{\sigma_x \sigma_z, \sigma_z \sigma_x\}$ inconsistent with the actual teleportation encoding $\sigma_i = \sigma_z \sigma_x$ (and $\beta_i = \sigma_z$). In conclusion Alice should not be able to change $\sigma_a$ from $\sigma_a \in \{I, \sigma_z\}$ to $\sigma_a \in \{\sigma_x \sigma_z, \sigma_z \sigma_x\}$ or $u_a u_b'$ from $u_a u_b \in \{00, 01\}$ to $u_a u_b' \in \{10, 11\}$ after performing BSM on $H_1 \otimes H_1$ and she cannot do this in our proposed procedure.

Since $H_2$ is also known to Alice, she can find swapped entangled state $|u_a u_b\rangle$ corresponding to her input $\sigma_a$ and BSM result $\alpha \alpha'$. Hence she can validate or abort Bob’s action by comparing $\sigma_b |\phi\rangle$ (and $\beta \beta'$) and $|\psi\rangle = \sigma_b |\phi\rangle$ received from Bob and B’ respectively. Hence proposed framework guarantees that neither Alice nor Bob can influence measurement outcome of joint computation by altering their inputs during the protocol.

(iv) Secure against MLC attacks: Alice can choose Mayers and Lo-Chau attacks and try to cheat as follow: Suppose she do not apply BSM on $H_1 \otimes H_1$, receives teleported state $|\psi\rangle = \sigma_b |\phi\rangle$ from Bob over EPR channel $|u_a u_b\rangle$ and teleports another arbitrary state $|\phi\rangle$ to B’ over EPR channel $|u_a u_b\rangle$ at $t = (x_a - x_b)$. She can know definite outcome of B’ measurement instantly but cannot find $\sigma_b$ from $|\psi\rangle = \sigma_b |\phi\rangle$ until she gets $\beta \beta'$ at $t = 2(x_a - x_b)$. Now in order to simulate her arbitrarily announced BSM result $\alpha \alpha'$ at $t = (x_a - x_b)$ with non-local correlations between $\sigma_b |\phi\rangle$ and $|\psi\rangle$, she has to apply specific $\sigma_a$ on $|\psi\rangle$ at $t = 2(x_a - x_b)$. Here Alice delayed input $\sigma_a$ can be either $\sigma_a \in \{I, \sigma_z\}$ or $\sigma_a \in \{\sigma_x, \sigma_z\}$ but she cannot give input of her choice at $t = 2(x_a - x_b)$ to get outcome she wants. In short, two-fold non-local quantum correlations and causality forces Alice to remain fair and perform agreed actions within time.

Similarly, Bob and B’ cannot cheat through MLC attacks. Instead of sending a single qubit in the state $|\psi\rangle = |\pm\rangle$ at time $t = (x_a - x_b)$, suppose B’ prepares an entangled quantum system $|\psi\rangle$ where
\[ |\psi\rangle = \sum_i \lambda_i |\alpha_i\rangle |\beta_i\rangle \] (3)

and sends system \(|\alpha_i\rangle\) to Alice. Since he is causally disconnected from Bob, he cannot cheat by enforcing Alice to get valid non-local correlations by applying unitary transformations on \(|\beta_i\rangle\).

(v) Secure against attacks based on non-local computations: Alice’s input \(\sigma_a\) can only be found before she reveals if someone has, Alice’s BSM result \(aa'\), Bob’s BSM result \(bb'\) and both quantum states \(|\phi\rangle\) and \(|\psi\rangle = \sigma_a |\phi\rangle\). Let’s consider an example where \(|u_a u_b\rangle = 00\), \(|u_{a'} u_{b'}\rangle = 00\) and Bob and B’ agree upon input \(\sigma_b\) somewhere in causal past. Instantly at time \(t = (x_a - x_b)\) when Bob teleports, eave (say B’) can found \(\sigma_b\) from \(\sigma_b |\phi\rangle\) and \(|\psi\rangle = \sigma_b |\phi\rangle\). Suppose eave finds \(\sigma = \{\sigma_z, \sigma_x \sigma_x\}\) then he can extract, from table 2, that swapped entangled state would be \(|u_{a'} u_{b'}\rangle = 0001\) (\(|u_{a'} u_{b'}\rangle = 0110\)) only if he knows that BSM result of Bob is \(bb' = 1011\) (\(bb' = 0001\)). Now if eave extracts \(|u_{a'} u_{b'}\rangle = 0001\) say, table 1 shows that he can find Alice’s input \(\sigma_a = \{I, \sigma_x\}\) (\(\sigma_a = \{\sigma_x, \sigma_x \sigma_x\}\)) only if he knows her BSM result \(aa' = 0001\) (\(aa' = 1011\)). Hence, if any piece of information from eave’s set \(E = \{\sigma_a |\phi\rangle, \sigma_b |\phi\rangle, aa', bb'\}\) is missing, Alice’s input \(\sigma_a\) cannot be extracted.

Suppose Bob and his agent B’ have an arbitrary amount of pre-shared entanglement and have unlimited power of non-local instantaneous computations. Even then they cannot find the complete set \(E\) before time \(t = 3(x_a - x_b)\). That is, they can only exchange classical information required to get outcome of non-local computations (Pauli encoding from \(\sigma_a |\phi\rangle\) and \(|\psi\rangle = \sigma_a |\phi\rangle\) here) at time \(t = 3(x_a - x_b)\). Hence maximum commitment time is \(2(x_a - x_b)\) where Alice commits at \(t = (x_a - x_b)\), reveals at \(t = 2(x_a - x_b)\), and Bob finds Alice’s commitment at \(t = 3(x_a - x_b)\) either fairly from \(|\psi\rangle = \sigma_a |\phi\rangle\) and \(|\psi\rangle = \sigma_a |\phi\rangle\) or trying to extract from eave’s set \(E\). However, minimum commitment time would be \((x_a - x_b)\) if Bob assigns another agent at disjoint site nearby \((x_a, t_a)\) who can receive complete set \(E\) at time \(t = 2(x_a - x_b)\).

Similarly, Alice cannot cheat successfully by allowing her agents to perform non-local instantaneous computations (entanglement-based attacks) on her behalf. Suppose Alice assigns two more agents at \(x_b < x < x_a\) and \(x_a < x' < x_{b'}\), respectively. Since Bob teleports \(\sigma_b |\phi\rangle\) only at \(t = (x_a - x_b)\), Alice’s agents cannot get information about Bob’s input \(\sigma_b\) before Alice.

| \(u_{a'} u_{b'}\) | \(u_{a'} u_{b'}\) | \(\{aa'\} u_{a'} u_{b'}\) |
|----------------|----------------|----------------|
| 00 | 00 | 00 |
| 01 | 01 | 01 |
| 10 | 10 | 11 |
| 11 | 11 | 11 |
| 00 | 00 | 01 |
| 01 | 01 | 01 |
| 10 | 10 | 11 |
| 11 | 11 | 11 |
| 00 | 01 | 01 |
| 01 | 01 | 01 |
| 10 | 10 | 11 |
| 11 | 11 | 11 |
| 00 | 11 | 01 |
| 01 | 10 | 01 |
| 11 | 00 | 00 |

Table 1: Entanglement swapping: This table shows all possible initial states of entangled particles \(|u_{a'} u_{b'}\rangle\) and corresponding outcomes of Alice’s BSM \(|aa'\rangle u_{a'} u_{b'}\rangle\). For example, if \(|u_{a'} u_{b'}\rangle = 00\rangle 11\rangle\), then swapped entangled pair \(|u_{a'} u_{b'}\rangle\) between Bob and B’ will be in one of the four possible Bell states: \(11\rangle\), \(10\rangle\), \(01\rangle\) and \(00\rangle\) corresponding to BSM result of Alice \(aa'\) as 00, 01, 10, and 11 respectively.
Table 2: Teleportation: This table shows all possible Bell states $|u_i u_{i'}\rangle$ swapped between Bob and B' due to BSM of Alice, Bob’s BSM results $\beta \beta'$ on his part of the entangled pair and state $\sigma_i |\psi\rangle$ and corresponding possibilities of state $|\psi\rangle$ on the B' side. For example, if Bob and B' have share entangled state as $|01\rangle$ and BSM result of Bob is $10 = \beta' \beta'$ then B' will have state $|\psi\rangle = \sigma_z \sigma_x \sigma_i |\phi\rangle$ on his side.

In conclusion, the proposed framework is secure for the purpose of OT, two-sided TPSC and unbiased ideal coin tossing since Alice/Bob cannot influence the final outcome of her/his choice. Similarly, it fulfills the security requirements for bit commitment where committer Alice is not allowed to change her commitment while receiver Bob remains unable to know the commitment before it is revealed by Alice.

Discussion

We proposed a general relativistic quantum framework for cryptography based on non-local quantum correlations and theory of relativity. The framework determines the actions of both parties through causality and quantum non-locality. Quantum non-local correlations assure that communicating parties act fairly while impossibility of superluminal signaling is used for insuring timely responses.

The framework is based on interesting combination of non-locality and theory of special relativity that gives new notion of OT; the receiver can only get specific information about the data but not its exact identity. That is, receiver may know both the transferred messages but remains oblivious about the genuine one. Moreover, the transfer position remains oblivious to the sender throughout the protocol while receiver can find the exact position only when he/she receives the data. The sender is guaranteed that the receiver can gain specific information about the data that logically follows from the protocol and know the transfer position only if the protocol is completed and the receiver acts fairly. Moreover, if the receiver completes the protocol successfully, he will be certain that the transferred data has come from the legitimate sender. The authenticity and integrity of the data transferred is guaranteed, the receiver rejects the data if the sender tries to modify it after the protocol has been started.

This fascinating combination of EPR type quantum correlations with causal structure of Minkowski space time shows the power of relativistic quantum cryptography in defining tasks that are considered to be impossible in non-relativistic cryptography. For example, unconditionally secure and deterministic two-sided TPSC, asynchronous ideal coin tossing with zero bias and unconditionally secure bit commitment.

Although it is standard in mistrustful quantum cryptography that both parties have efficient quantum technologies (quantum computer), the proposed relativistic quantum framework can be reliably implemented without requiring quantum computer. Both parties can

| $|u_i u_{i'}\rangle$ | Bob’s BSM $\beta \beta'$ | B' $|\psi\rangle = \sigma_z \sigma_x \sigma_i |\phi\rangle$ |
|------------------|----------------|---------------------------------|
| $|00\rangle$     | $00$ $01$ $10$ $11$ | $\sigma_z |\phi\rangle$ $\sigma_z \sigma_x |\phi\rangle$ $\sigma_z \sigma_x \sigma_b |\phi\rangle$ $\sigma_z \sigma_b |\phi\rangle$ |
| $|01\rangle$     | $00$ $01$ $10$ $11$ | $\sigma_z \sigma_b |\phi\rangle$ $\sigma_z |\phi\rangle$ $\sigma_z \sigma_x \sigma_b |\phi\rangle$ $\sigma_z \sigma_b |\phi\rangle$ |
| $|10\rangle$     | $00$ $01$ $10$ $11$ | $\sigma_z \sigma_b |\phi\rangle$ $\sigma_z |\phi\rangle$ $\sigma_z |\phi\rangle$ $\sigma_z \sigma_b |\phi\rangle$ |
| $|11\rangle$     | $00$ $01$ $10$ $11$ | $\sigma_z \sigma_b |\phi\rangle$ $\sigma_z |\phi\rangle$ $\sigma_z |\phi\rangle$ $\sigma_z \sigma_b |\phi\rangle$ |
calculate $f(\sigma_a, \sigma_b | \phi)$ securely with existing quantum technologies; photo detectors without needing long term quantum memory. However, even having quantum computers, neither party can cheat successfully.

The proposed framework can easily be generalized for other multiparty mistrustful cryptographic tasks securely. For example, if B' is considered to be a third party instead of Bob’s agent then our proposed framework could be used to implement secure quantum secret sharing between sender Bob and receivers Alice and B'. The secret $\sigma_b$ can be divided among Alice and B' in terms of classical BSM result $a \alpha'$ and quantum state $|\psi\rangle = \sigma_a \sigma_b |\phi\rangle$ respectively.

We hope this work would open new directions in quantum information, quantum computation, quantum cryptography and their connections with special theory of relativity. On the other hand, proposed framework is purely relativistic quantum mechanical where both input and output data is associated with unitary transformations applied on quantum systems and it does not require any secure classical channels; classical information can be publically announced. Hence, it would in return prove to be helpful in developing our understanding about the true description of the world, the quantum theory.

1. Kent, A., Munro, W., Spiller, T. & Beausoleil, R. Tagging systems, US20067075438 (2006).
2. Kent, A., Munro, W. & Spiller, T. Quantum tagging: authenticating location via quantum information and relativistic signalling constraints. *Phys. Rev. A.* **84**, 012326 (2011).
3. Malaney, R. Location-dependent communications using quantum entanglement. *Phys. Rev. A.* **81**, 042319 (2010).
4. Lau, H. & Lo, H. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Phys. Rev. A.* **83**, 012322 (2011).
5. Buhman, H. et al. Position-based cryptography: impossibility and constructions. In *proceedings of Advances in Cryptology — CRYPTO 2011*, pages 429–446 Santa Barbara, CA, USA (*Lect. Notes Comput. Sci.* Vol. **6841**, Springer) (2011)
6. Beigi, S. & Konig, R. Simultaneous instantaneous non-local quantum computation with applications to position-based cryptography. *New J. Phys.* **13**, 093036 (2011).
7. Kent, A. Quantum tagging for tags containing secret classical data. *Phys. Rev. A.* **84**, 022335 (2011).
8. Nadeem, M. Position-based quantum cryptography over untrusted networks. *Laser Phys.* **24** 085202 (2014).
9. Nadeem, M. Secure positioning and non-local correlations. *arXiv*:1406.3013 (2014).
10. Nadeem, M. Unconditionally secure commitment in position-based quantum cryptography. *Sci. Rep.* **4**, 6774; DOI:10.1038/srep06774 (2014).
11. Barrett, J., Hardy, L. & Kent, A. No signalling and quantum key distribution. *Phys. Rev. Lett.* **95**, 010503 (2005).
12. Acín, A., Gisin, N. & Masanes, L. From Bells theorem to secure quantum key distribution. *Phys. Rev. Lett.* **97**, 120405 (2006).
13. Acín, A., Massar, S. & Pironio, S. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New J. Phys.* **8**, 126 (2006).
14. Barrett, J., Kent, A. & Pironio, S. Maximally non-local and monogamous quantum correlations. *Phys. Rev. Lett.* **97**, 170409 (2006).
15. Colbeck, R. Quantum and Relativistic Protocols For Secure Multi-Party Computation. *arXiv*: 0911.3814.
16. Acin, A. *et al.* Device-independent security of quantum cryptography against collective
attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
17. Masanes, L., Renner, R., Christandl, M., Winter, A. & Barrett, J. Unconditional security of key distribution from causality constraints. *arXiv*: 0606049v4 (2009).
18. Masanes, L. Universally composable privacy amplification from causality constraints. *Phys. Rev. Lett.* **102**, 140501 (2009).
19. Pironio, S. *et al.* Random numbers certified by Bell’s theorem. *Nature* **464**, 1021 (2010).
20. Masanes, L., Pironio, S. & Acín, A. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Commun.* **2**, 238 (2011).
21. Silman, J. *et al.* Fully distrustful quantum bit commitment and coin flipping. *Phys. Rev. Lett.* **106**, 220501 (2011).
22. Kent, A. Location-oblivious data transfer with flying entangled qudits. *Phys. Rev. A* **84**, 012328 (2011).
23. Colbeck, R. & Kent, A. Private randomness expansion with untrusted devices. *J. Phys. A* **44**, 095305 (2011).
24. Kent, A. Unconditionally secure bit commitment with flying qudits. *New J. Phys.* **13**, 113015 (2011).
25. Kent, A. Quantum tasks in Minkowski space. *Class. Quant. Grav.* **29**, 224013 (2012).
26. Kent, A. Unconditionally secure bit commitment by transmitting measurement outcomes. *Phys. Rev. Lett.* **109**, 130501 (2012).
27. Kent, A. A no-summoning theorem in relativistic quantum theory. *Q. Info. Proc.* **12**, 1023 (2013).
28. Kent, A., Massar, S. & Silman, J. Secure and Robust Transmission and Verification of Unknown Quantum States in Minkowski Space. *Sci. Rep.* **4**, 3901; DOI:10.1038/srep03901 (2014).
29. Rabin, M. O. How to exchange secrets by oblivious transfer. Technical Memo TR-81, Aiken Computation Laboratory, Harvard University, (1981).
30. Wiesner, S. Conjugate coding. *Sigact News* **15**, 1, 78-88 (1983).
31. Even, S., Goldreich, O. & Lempel, A. A randomized protocol for signing contracts. In *proceedings of Advances in Cryptology — CRYPTO ’82*, pp. 205-210 Plenum Press, Michigan, USA, (1982).
32. Crépeau, C. Equivalence between two flavours of oblivious transfers. In *proceedings of Advances in Cryptology — CRYPTO ’87*, pp 350-354 Berlin Heidelberg (Lecture Notes in Computer Science, Vol. **293**, Springer-Verlag) (1988).
33. Kilian, J. Founding cryptography on oblivious transfer. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, Chicago*, pp. 20-31(1988).
34. Bennett, C. H., Brassard, G., Crépeau, C. & Skubiszewska, M.-H. Practical quantum oblivious transfer. In *proceedings of Advances in Cryptology — CRYPTO ’91*, pp. 351-366 Berlin Heidelberg (Lecture Notes in Computer Science, Vol. **576**, Springer-Verlag) (1992).
35. Lo, H. K. Insecurity of quantum secure computations. *Phys. Rev. A* **56**, 1154 (1997).
36. Buhrman, H., Christandl, M. & Schaffner, C. Complete insecurity of quantum protocols for classical two-party computation. *Phys. Rev. Lett.* **109**, 160501 (2012).
37. Colbeck, R. Impossibility of secure two-party classical computation. *Phys. Rev. A*, **76**, 062308 (2007)
38. Colbeck, R. & Kent, A. Variable-bias coin tossing. *Phys. Rev. A* **73**, 032320 (2006).
39. Lo, H. K. & Chau, H. F. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D*, **120**, 177-187 (1998).
40. Kent, A. Coin tossing is strictly weaker than bit commitment. *Phys. Rev. Lett.* **83**, 5382 (1999).
41. Mayers, D. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.* **78**, 3414-3417 (1997).
42. Lo, H. K. & Chau, H. F. Is quantum bit commitment really possible? *Phys. Rev. Lett.* **78**, 3410-3413 (1997).
43. Mayers, D., Kitaev, A. & Preskill, J. Superselection rules and quantum protocols. *Phys. Rev. A* **69**, 052326 (2004).
44. Einstein, A., Podolsky, B. & Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47**, 777 (1935).
45. Ekert, A. K. Quantum Cryptography Based on Bell's Theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
46. Vaidman, L. Instantaneous measurement of nonlocal variables. *Phys. Rev. Lett.* **90**, 010402 (2003).
47. Zukowski, M., Zeilinger, A., Horne, M. & Ekert, A. Event-ready-detectors’ Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71**, 4287 (1993).
48. Bennett, C., Brassard, G., Crepeau, C., Jozsa, R., Peres, A. & Wootters, W. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895 (1993).
49. Blum, M. Coin flipping by telephone A protocol for solving impossible problems. *Sigact News* **15**, 1, 23-27 (1983).
50. Braunstein, S., Mann, A. & Revzen, M. Maximal violation of Bell inequalities for mixed states. *Phys. Rev. Lett.* **68**, 3259 (1992).