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 mistrustful cryptography that exploits the fascinating connection of quantum non-locality and special theory of relativity with cryptography. The underlying principle of unconditional security is two-fold quantum non-local correlations: first entanglement swapping and then teleportation. The proposed framework has following remarkable and novel features. (i) Helps in defining a new notion of oblivious transfer where both the data transferred and the transfer position remain oblivious. (ii) The confidentiality and integrity of the data transferred is guaranteed by the actions of sender and receiver in their own secure laboratories instead of sending data over noisy channels. (iii) It directly leads to unconditionally secure and deterministic two-sided two-party computation which is currently considered to be impossible. (iv) the two-party computation turns out to be asynchronous ideal coin tossing with zero bias which has not been achieved previously. (v) The same framework implies unconditionally secure bit commitment. Finally, we conjecture here that the combination of quantum non-locality and theory of relativity as discussed here is complete and sufficient to solve all the mistrustful cryptographic tasks securely.

In the last few years, researchers have shown great excitement in the area of relativistic quantum cryptography[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 setup in relativistic quantum theory that would be sufficient to solve all the mistrustful cryptographic tasks securely.

Kilian showed that classical oblivious transfer[29-32] (OT) is a basic building block for other mistrustful cryptographic protocols, for example, two-party secure computations[33]. However, since computationally hard classical protocols can be broken, various protocols for OT have also been proposed that are based on non-relativistic quantum mechanics[34] and relativistic quantum theory[22]. In existing non-relativistic quantum OT protocols, only data remains oblivious to Alice while she can be well aware of Bob's position. On the other hand, in relativistic OT protocol[22], the data can be completely determined by Alice while she remains ignorant about the position of Bob.

Moreover, in all previously proposed OT protocols, Bob 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[35,36]. These impossibility results have also been extended to relativistic quantum cryptography[37]. However, relativistic cryptography gives hope for secure implementation of nondeterministic two-sided TPSC and hence variable-bias coin tossing[38]. Moreover, asynchronous ideal coin tossing is impossible in

classical/non-relativistic quantum cryptography[39] while only synchronous ideal coin tossing is possible if impossibility of superluminal signaling is considered[40].

Furthermore, bit commitment is another very important and basic cryptographic protocol that is impossible in classical/nor-relativistic quantum cryptography[41-43] but has been proved to be possible in relativistic quantum theory[10,24,26]. These no-go theorems show the limits 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[44] solves the very basic ingredient of cryptography, QKD[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[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 define a general relativistic quantum framework for mistrustful 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 (zero bias), (iv) bit commitment, and (v) secure quantum secret sharing. In fact, the framework is sufficient to solve all the mistrustful cryptographic tasks unconditionally secure against Lo- Chau attacks[35,39].

Non-locality and relativistic mistrustful quantum cryptography

In a general framework of relativistic quantum cryptography proposed by Adrian Kent, background space time is approximately Minkowski and communicating parties are not the individuals but are agencies having distributed agents throughout the space time. The agencies are assumed to have fixed 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. 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.

For simplicity, we suppose here that Alice is an individual while Bob has three agents; R, B_1 and B_2 at the relevant points in Minkowski space-time. This assumption does not provide any advantages to Bob over Alice in the framework. Moreover, even if Alice manages agents at specific space time positions, it will not give her any advantages over Bob. We also assume Bob and his agents can communicate quantum information securely with each other. However, all the quantum/classical channels between Alice and Bob are insecure. Both parties have powers of instantaneous computation and time for information processing at their secure sites is assumed to be negligibly small. Finally, the proposed framework is purely relativistic quantum mechanical and does not require any secure classical channels; classical information can be publically announced.

All the mistrustful cryptographic tasks can be implemented with following procedure: Suppose Bob and Alice are at (0,0) and (x,t) point of Minkowski space time while Bob's agents R, B_1 and B_2 are at arbitrary space-like separated positions unknown to Alice. Alice only knows the directions where B_1 and B_2 can receive the data, they are light-like separated from Alice, but not their exact positions. Bob shares a secret entangled system $\mathcal{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ with Alice. Bob also prepares another secret entangled system $\mathcal{A'R} \in \mathcal{H}_{A'} \otimes \mathcal{H}_R$ and sends $\mathcal{H}_{A'}$ to Alice while $\mathcal{H}_R$ to R such that both Alice and R receive $\mathcal{H}_{A'}$ and $\mathcal{H}_R$ simultaneously. That is, Alice, Bob and R share a system $\mathcal{S} = \mathcal{AA'BR}$ denoted by $\mathcal{H}_S = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_R$ only known to Bob.

Alice then performs Bell state measurement[46] (BSM) by applying local Bell operator ($\beta_a \otimes I$) on $(\mathcal{H}_A \otimes \mathcal{H}_{A'}) \otimes (\mathcal{H}_B \otimes \mathcal{H}_R)$. She keeps her measurement result $u_a u_{a'} \in \{00,01,10,11\}$ secret. As a result, Bob's and R's systems get entangled[47]; $\mathcal{BR} \in \mathcal{H}_{\mathcal{B}} \otimes \mathcal{H}_{\mathcal{R}}$. Now Bob prepares a quantum state $|\varphi\rangle$, applies transformations $U^{u_b} U^{u_{b'}}$ corresponding to data $u_b u_{b'}$ he wants to send and teleports[48] the quantum state to R by applying local Bell operator $\beta_a \otimes I$ on $(|\varphi\rangle \otimes \mathcal{H}_{\mathcal{B}}) \otimes \mathcal{H}_{\mathcal{R}}$. The non-locally correlated system $\mathcal{R}$ remains totally random to R. Instantly R measures his system $\mathcal{R}$ and sends the outcome to Alice. Alice prepares the same quantum system corresponding to received classical information from R, applies further unitary transformations $U^{u_a} U^{u_{a'}}$ (or $U^{u_a} U^{1 \oplus u_{a'}}$) and sends to either B_1 or B_2. The local transformations $U^{u_a} U^{u_{a'}}$ (or $U^{u_a} U^{1 \oplus u_{a'}}$) applied by Alice determine the data (commitment) she is sending to Bob. Simultaneously, she announces her BSM result $u_a u_{a'}$. Bob validates the actions of Alice if she replies within time and her announcement is consistent with non-local quantum correlations between BSM results of Alice, Bob and shared quantum system $\mathcal{H}_S = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_R$. B_i measures the received quantum system from Alice in the pre-agreed basis and sends the outcome to Bob. Now Bob can find the information about Alice's data as comes from the specific code discussed below. Underlying principle of unconditional security in this framework is two-fold quantum non-local correlations: first entanglement swapping and then teleportation.

To make the analysis simple, we assume in the rest of the discussion that $\mathcal{H}_S = (C^2)^{\otimes 4}$; each subspace of $\mathcal{H}_S$ is 2-dimensional complex space. That is, both $\mathcal{H}_A \otimes \mathcal{H}_B = (C^2) \otimes (C^2)$ and $\mathcal{H}_{A'} \otimes \mathcal{H}_R = (C^2) \otimes (C^2)$ are 2-qubit maximally entangled systems with Bell basis

$$|u_m u_n\rangle = \frac{|0\rangle|u_n\rangle + (-1)^{u_m}|1\rangle|1 \oplus u_n\rangle}{\sqrt{2}} \tag{1}$$

where u_m and $u_n \in \{0,1\}$ and $\oplus$ denotes addition with mod 2.

Procedure-I

Let's suppose Alice and Bob agree on a code: if sender S (Alice/Bob) applies unitary transformation I, σ_x, σ_z, or $\sigma_z \sigma_x$ on a quantum system $|\phi\rangle \in \mathcal{H}_S$, he/she is actually giving input data 00, 01, 10 or 11 to the system $\mathcal{H}_S$ respectively. That is, transformation $\sigma_s \in \{I, \sigma_x\}$ correspond to classical data $u_s u_{s'} = \{00,01\}$ (or classical bit $s = u_s \oplus u_{s'} = \{0,1\}$) while those of $\sigma_s \in \{\sigma_z, \sigma_z \sigma_x\}$ correspond to classical data $u_s u_{s'} = \{10,11\}$ (or classical bit $s = u_s \oplus u_{s'} = \{1,0\}$). As a result, data will be transferred by the actions of sender and receiver in their own secure laboratories instead of sending data over noisy channels.

This procedure-I solves the problem of OT, deterministic two-sided TPSC, and asynchronous ideal coin tossing with zero bias. If sender wants to send data $u_s u_{s'}$ to the receiver,

he/she will apply Pauli transformations $\sigma_s \in \{\sigma_z^{u_s}\sigma_x^{u_{s'}}, \sigma_z^{u_s}\sigma_x^{1\oplus u_{s'}}\}$ on the shared quantum state $|\varphi\rangle \in \{+,-\}$ with receiver. We would like to highlight here that $\sigma_z^{u_s}\sigma_x^{u_{s'}}|\varphi\rangle = \sigma_z^{u_s}\sigma_x^{1\oplus u_{s'}}|\varphi\rangle$ if $|\varphi\rangle \in \{+,-\}$ where we ignore the overall phase factor. We started this procedure for OT where Alice is the sender while Bob is the receiver. The same procedure will be applicable for two-sided TPSC and asynchronous ideal coin tossing to be discussed latter.

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[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[30,31]. It is shown later by Crépeau that both of these notions of OT are equivalent[32].

Our proposed procedure-I helps in defining a new notion of OT where receiver Bob remains oblivious about both the data transferred and the transfer position; he may know both the transferred messages but remains oblivious about the genuine one. On the other hand, the sender Alice cannot learn the transfer position even after the protocol is completed. Moreover, Bob accepts the data only if he is certain that data has come from Alice, by measuring time lapse and testifying non-local quantum correlations established through local operations. Finally, in our secure OT protocol, Alice cannot change the data she started with otherwise Bob rejects the protocol – that is something not possible in all the previously proposed OT protocols. Explicit procedure-I for OT is described below:

(1). Bob secretly prepares an EPR pair $|u_a u_b\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and sends first qubit to Alice.

(2). Bob prepares another EPR pair $|u_{a'} u_r\rangle \in \mathcal{H}_{A'} \otimes \mathcal{H}_R$ and sends fist qubit to Alice while second qubit to his agent R such that both Alice and R receive qubits $|u_{a'}\rangle$ and $|u_r\rangle$ simultaneously.

(3). After time t=*x*/c, Alice receives $|u_{a'}\rangle$ and performs BSM on qubits $|u_a\rangle$ and $|u_{a'}\rangle$ in his possession and gets two classical bits, say $u_a u_{a'} \in \{00,01,10,11\}$. This measurement projects the qubits $|u_b\rangle$ and $|u_r\rangle$ into one of the four possible Bell states $|u_b u_r\rangle \in \mathcal{H}_B \otimes \mathcal{H}_R$ instantly, unknown to both Alice and Bob.

(4). At the same time t, Bob prepares a qubit $|\varphi\rangle \in \{+,-\}$ in the agreed Hadamard basis, applies Pauli transformation $\sigma_b \in \{\sigma_z^{u_b}\sigma_x^{u_{b'}}, \sigma_z^{u_b}\sigma_x^{1\oplus u_{b'}}\}$ corresponding to data $u_b u_{b'}$ he wants to send and teleports the state $\sigma_b|\varphi\rangle$ to R. As a result, R's half of the shared Bell's state becomes one of the corresponding four possible states $|\psi\rangle = \sigma_i\sigma_b|\varphi\rangle$ where $\sigma_i \in \{I, \sigma_x, \sigma_z, \sigma_z\sigma_x\}$ unknown to everyone. R measures his system and sends outcome ψ to Alice. In fact, Bob (R) has transferred the data $u_b u_{b'}$ encoded in σ_b to Alice where she remains oblivious about the data even after receiving ψ. We would like to mention here that as for as oblivious transfer is concerned, from Alice to Bob, there would be no requirement of transformation σ_b from Bob's side; it serves purely the purpose of TPSC, coin tossing and quantum secret sharing to be discussed later.

(5). Instantly, Alice prepares corresponding quantum state $|\psi\rangle$, applies unitary transformations corresponding to her input data $\sigma_a \in \{\sigma_z^{u_a}\sigma_x^{u_{a'}}, \sigma_z^{u_a}\sigma_x^{1\oplus u_{a'}}\}$ on $|\psi\rangle$ and immediately sends the state

$$|\psi'\rangle = \sigma_a|\psi\rangle = \sigma_a\sigma_i\sigma_b|\varphi\rangle \quad (2)$$

to either B_1 or B_2 over insecure quantum channel between them. Here, Alice's choice of sending state $|\psi'\rangle$ to B_1 or B_2 is totally random. Simultaneously she publically announces values of $u_a u_{a'}$.

(6). Suppose Bob and one of his agent B_i receive the information from Alice at times t_b and t_{b_i} respectively. If values $u_a u_{a'}$ are consistent with swapped entangled state $|u_b u_r\rangle$ and corresponding σ_i and Alice replied within allocated time, Bob verifies that Alice is fair otherwise aborts the protocol. Here, for each value of $u_a u_{a'}$, there will be unique Bell state $|u_b u_r\rangle$ and hence unique σ_i as shown in table 1 and table 2.

(7) B_i measures the received state $|\psi'\rangle$ in $\{+,-\}$ basis, and sends the result and time t_{b_i} to Bob. Bob can check that whether Alice's transformation is consistent with her announcement or not. If $u_a u_{a'} \in \{00,01\}$ she should have applied $\sigma_a \in \{I, \sigma_x\}$ on $|\psi\rangle$ while $\sigma_a \in \{\sigma_z, \sigma_z\sigma_x\}$ in case of $u_a u_{a'} \in \{10,11\}$. As a result, Bob can find that either $u_a u_{a'} \in \{00,01\}$ (or $u_a u_{a'} \in \{10,11\}$) but remains ignorant about the specific classical data/bit $u_a u_{a'} / a = u_a \oplus u_{a'}$ Alice has sent.

I would like to mention here that modification of our protocol for computational basis $\{0,1\}$ is straightforward where both parties agree that Alice will apply unitary transformations $\sigma_a \in \{\sigma_z^{u_a}\sigma_x^{u_{a'}}, \sigma_z^{1\oplus u_a}\sigma_x^{u_{a'}}\}$ on the state $|\psi\rangle$ where $\sigma_z^{u_a}\sigma_x^{u_{a'}}|\psi\rangle = \sigma_z^{1\oplus u_a}\sigma_x^{u_{a'}}|\psi\rangle$ if $|\psi\rangle \in \{0,1\}$ where we ignore the overall phase factor. These operations by Alice guarantee that Bob can get only following information: either $\sigma_a \in \{I, \sigma_z\}$ or $\sigma_a \in \{\sigma_x, \sigma_z\sigma_x\}$ but not the exact Pauli operator. That is, Bob can successfully guess either Alice has sent qubit $u_a u_{a'} \in \{00,10\}$ or $u_a u_{a'} \in \{01,11\}$ but not the definite data.

Security analysis

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.

Security against Alice

In our OT protocol, cheating Alice means she could try to get following information during or after the protocol: (I) try to know the specific data σ_b Bob has transferred (II) want to know the position of B_i with certainty or (III) try to alter her BSM result $u_a u_{a'}$ (from $u_a u_{a'} \in \{00,01\}$ to $u_a u_{a'} \in \{10,11\}$) after getting ψ from R and convince Bob for joint measurement outcome $|\psi'\rangle = \sigma_a\sigma_i\sigma_b|\varphi\rangle$ of her choice. As for as Bob's data is concerned, Alice cannot find the exact value even after the protocol is complete – the system $\mathcal{H}_S = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_R$ BSM results of Bob and $|\varphi\rangle$ is completely unknown to her. On the other hand, she also remains ignorant about transfer position since the proposed protocol does not allow her to compute time lapse and hence distance of the receiver; both B_1 and B_2 do not communicate with Alice during the protocol.

Can Alice choose Mayers and Lo-Chau attacks[41-43] or other strategies and try to cheat by altering values of $u_a u_{a'}$ after she has made BSM on qubits $|u_a\rangle$ and $|u_{a'}\rangle$? Answer is NO; Bob

will detect cheating Alice with probability P=1. She can try following strategies: (i) If she receives result ψ from Bob's agent R, then prepares different state, and hence applies/announce different values of $u_a u_{a'}$, this procedure guarantees Bob to detect her cheating since Bob's agent R knows ψ. (ii) If she delays and do not apply BSM on qubits $|u_a\rangle$ and $|u_{a'}\rangle$, she will receive teleported state $|\psi\rangle = \sigma_i \sigma_b |\varphi\rangle$ from Bob and single bit u_r from R. Both of these results are useless for Alice to cheat, cannot get any information about $|\sigma_b\rangle$ or $|\sigma_i\rangle$ and hence non-local correlations. (iii) Instead of sending a single qubit in the state $|\psi\rangle \in \{+,-\}$, suppose Alice prepares an entangled quantum system $|\psi\rangle$ where

$$|\psi\rangle = \sum_i \lambda_i |\alpha_i\rangle |\beta_i\rangle \tag{3}$$

and sends system $|\beta_i\rangle$ to Bob. Even then, she cannot cheat by enfocing Bob to get valid non-local correlations by applying unitary transformations on $|\alpha_i\rangle$.

As we have stated earlier, underlying principle of unconditional security in the proposed framework is two-fold quantum non-local correlations: first entanglement swapping and then teleportation. That is, for each value of $u_a u_{a'}$, there will be unique Bell state $|u_b u_r\rangle$ and hence unique σ_i. Let's consider a simplest possible situation from first row of table 1 and first, fifth and ninth column of table 2. Suppose $|u_a u_b\rangle = 00$, $|u_{a'} u_r\rangle = 00$ and $u_a u_{a'} = 00$ then $|u_b u_r\rangle = 00$. Now if BSM result of Bob is $u_b u_{b'} = 11$ while teleporting $\sigma_b |\varphi\rangle$ to R, then $\sigma_i = \sigma_z \sigma_x$. If Alice tries to cheat by announcing different values of $u_a u_{a'} = 01,10,11$ then Bob will extract $|u_b u_r\rangle = 01,10,11$ and hence different $\sigma_i = \sigma_z, \sigma_x, I$.

Note here, that if Alice gets $u_a u_{a'} = 00$ and announces $u_a u_{a'} = 01$, it will not be considered as successful cheating since for the case considered above, $|\psi\rangle = \sigma_z \sigma_x \sigma_b |\varphi\rangle = \sigma_z \sigma_b |\varphi\rangle$. Similarly, if Alice gets $u_a u_{a'} = 10$ and announces $u_a u_{a'} = 11$, it will generate $|\psi\rangle = \sigma_x \sigma_b |\varphi\rangle = I \sigma_x \sigma_b |\varphi\rangle$. As a result both Alice and Bob will get same outcome $|\psi'\rangle$. In conclusion Alice should not be able to change $u_a u_{a'}$ from $u_a u_{a'} \in \{00,01\}$ to $u_a u_{a'} \in \{10,11\}$) after getting ψ from R and she cannot do this in our proposed procedure.

$\|u_a u_b\rangle \|u_{a'} u_r\rangle$				$(u_a u_{a'}) \|u_b u_r\rangle$			
$\|00\rangle \|00\rangle$	$\|01\rangle \|01\rangle$	$\|10\rangle \|10\rangle$	$\|11\rangle \|11\rangle$	$(00) \|00\rangle$	$(01) \|01\rangle$	$(10) \|10\rangle$	$(11) \|11\rangle$
$\|00\rangle \|01\rangle$	$\|01\rangle \|00\rangle$	$\|10\rangle \|11\rangle$	$\|11\rangle \|10\rangle$	$(00) \|01\rangle$	$(01) \|00\rangle$	$(10) \|11\rangle$	$(11) \|10\rangle$
$\|00\rangle \|10\rangle$	$\|01\rangle \|11\rangle$	$\|10\rangle \|00\rangle$	$\|11\rangle \|01\rangle$	$(00) \|10\rangle$	$(01) \|11\rangle$	$(10) \|00\rangle$	$(11) \|01\rangle$
$\|00\rangle \|11\rangle$	$\|01\rangle \|10\rangle$	$\|10\rangle \|01\rangle$	$\|11\rangle \|00\rangle$	$(00) \|11\rangle$	$(01) \|10\rangle$	$(10) \|01\rangle$	$(11) \|00\rangle$

Table 1: Entanglement swapping**:** Bell state shared between Alice and Bob is $|u_a u_b\rangle$ and between Alice and R is $|u_{a'} u_r\rangle$. This table shows all possible initial states of entangled particles $|u_a u_b\rangle |u_{a'} u_r\rangle$ and corresponding outcomes of Alice's BSM $(u_a u_{a'}) |u_b u_r\rangle$. For example, if $|u_a u_b\rangle |u_{a'} u_r\rangle = |00\rangle |11\rangle$ then swapped entangled pair $|u_b u_r\rangle$ would be in one of the four possible Bell sates: $|11\rangle$, $|10\rangle$, $|01\rangle$ and $|00\rangle$ corresponding to BSM result of Alice $u_a u_{a'}$ as 00, 01, 10, and 11 respectively.

$\lvert u_b u_r \rangle$	Bob BSM				R			
	$u_b u_{b'}$				$\lvert\psi\rangle = \sigma_i \sigma_b \lvert\varphi\rangle$			
$\lvert 00 \rangle$	00	01	10	11	$\sigma_b \lvert\varphi\rangle$	$\sigma_x \sigma_b \lvert\varphi\rangle$	$\sigma_z \sigma_b \lvert\varphi\rangle$	$\sigma_z \sigma_x \sigma_b \lvert\varphi\rangle$
$\lvert 01 \rangle$	00	01	10	11	$\sigma_x \sigma_b \lvert\varphi\rangle$	$\sigma_b \lvert\varphi\rangle$	$\sigma_z \sigma_x \sigma_b \lvert\varphi\rangle$	$\sigma_z \sigma_b \lvert\varphi\rangle$
$\lvert 10 \rangle$	00	01	10	11	$\sigma_z \sigma_b \lvert\varphi\rangle$	$\sigma_z \sigma_x \sigma_b \lvert\varphi\rangle$	$\sigma_b \lvert\varphi\rangle$	$\sigma_x \sigma_b \lvert\varphi\rangle$
$\lvert 11 \rangle$	00	01	10	11	$\sigma_z \sigma_x \sigma_b \lvert\varphi\rangle$	$\sigma_z \sigma_b \lvert\varphi\rangle$	$\sigma_x \sigma_b \lvert\varphi\rangle$	$\sigma_b \lvert\varphi\rangle$

Table 2: Teleportation: This table shows all possible Bell states $\lvert u_b u_r \rangle$ swapped between Bob and R due to BSM of Alice, Bob's BSM results on his/her part of the entangled pair and state $\sigma_b \lvert\varphi\rangle$ and corresponding possibilities of state $\lvert\psi\rangle$ on the R's side. For example, if Bob and R have share entangled state as $\lvert 01 \rangle$ and BSM result of Bob is 10 then R will have state $\lvert\psi\rangle = \sigma_z \sigma_x \sigma_b \lvert\varphi\rangle$ on his side.

Finally, Alice cannot cheat successfully by hiding her position or delaying in sending $\lvert\psi'\rangle$. If Alice performs BSM from position P (distance *x* away from Bob) and later tries to cheat by responding to B_i from different position P', it would not help her at all. She will have to respond within allowed time and within this time lapse she cannot get any useful information about non-local correlations generated or position of B_i. In conclusion, non-local quantum correlations and relativistic quantum cryptography forces Alice to remain fair and perform agreed actions within time.

Security against Bob

In our proposed framework, security against Bob lies in following two requirements: (I) although it is necessary for Bob to know exact values of Alice's BSM $u_a u_{a'}$ but he must not be able to know the definite unitary transformation $\sigma_a \in \{\sigma_z^{u_a} \sigma_x^{u_{a'}}, \sigma_z^{u_a} \sigma_x^{1 \oplus u_{a'}}\}$ Alice has applied. (II) Before or during the protocol, Bob should not know the position where Alice will send the data.

Since Bob knows EPR pairs $\lvert u_a u_b \rangle$ and $\lvert u_{a'} u_r \rangle$, he can find exact values of Alice's BSM $u_a u_{a'}$ during the protocol by measuring swapped entangled pair $\lvert u_b u_r \rangle$. Bob's agents then can send an arbitrary quantum state and Alice's will reply back without knowing her BSM result has already been revealed. Moreover, even if Alice is fair and announce exact values of her BSM $u_a u_{a'}$, Bob cannot differentiate between Alice's transformations $\sigma_z^{u_a} \sigma_x^{u_{a'}}$ or $\sigma_z^{u_a} \sigma_x^{1 \oplus u_{a'}}$ on $\lvert\psi\rangle$ since $\sigma_z^{u_a} \sigma_x^{u_{a'}} \lvert\psi\rangle = \sigma_z^{u_a} \sigma_x^{1 \oplus u_{a'}} \lvert\psi\rangle$.

Furthermore, before or during the protocol, Bob cannot predict in advance about the position where Alice will send the data. The choice of transfer position is totally random and Bob can only know the transfer position once any one of B_1 or B_2 (who are space-like separated) receives the data from Alice. Hence the proposed OT protocol is completely secure from Bob; he will not learn the transfer position until the protocol is completed and will remain oblivious about the data Alice has sent.

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 fulfils 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 impossibility or 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[35] has shown that Bob can do this by applying unitary transformations on his own quantum system $\mathcal{H}_{\mathcal{B}}$. That is, the system $\mathcal{H}_{\mathcal{B}}$ kept by Bob must be an eigenstate of the measurement operator that he uses for computing $f(a,b)$. Being an eigenstate, $\mathcal{H}_{\mathcal{B}}$ remains undisturbed by Bob's measurement that makes computation of $f(a,b')$ feasible.

However, our proposed procedure-I discussed for OT can easily evade such attacks and results in secure and deterministic two-sided TPSC of function $f(\sigma_a,\sigma_b;|\varphi\rangle)$ where σ_a and σ_b are unitary transformations on quantum system $\mathcal{H}_S = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_R$ applied by Alice and Bob respectively. According the code, when Alice and Bob apply these transformations on $|\varphi\rangle$, they actually provide input $u_a u_{a'} \rightarrow \sigma_a$ and $u_b u_{b'} \rightarrow \sigma_b$ to the shared quantum system $\mathcal{H}_S$ respectively. At the end of the computation, both parties know the same definite outcome

$$f(\sigma_a,\sigma_b;|\varphi\rangle) = \sigma_a\sigma_i\sigma_b|\varphi\rangle \qquad (4)$$

where σ_i comes from the shared quantum system $\mathcal{H}_S$.

Bob's input $u_b u_{b'}$ remains totally random to Alice even after measurement of $\sigma_i\sigma_b|\varphi\rangle$. Similarly, Bob remains oblivious about Alice's input $u_a u_{a'}$. Finally both Alice and Bob get same outcome of function $f(\sigma_a,\sigma_b;|\varphi\rangle)$ deterministically. As we have shown earlier, neither Alice nor Bob can cheat by altering quantum system $|\psi\rangle = \sigma_i\sigma_b|\varphi\rangle$, both parties know the result ψ and Alice's transformation σ_a on $|\psi\rangle = \sigma_i\sigma_b|\varphi\rangle$ generates the final outcome $f(\sigma_a,\sigma_b;|\varphi\rangle) = \sigma_a\sigma_i\sigma_b|\varphi\rangle$.

Ideal quantum coin tossing

Coin tossing[49] is another fundamental primitive function in communication that allows distant mistrustful parties to agree on a random data. Coin tossing is said to be ideal if it follows:

1). Ideal coin tossing results in three possible outcomes γ: $\gamma_+ = +$, $\gamma_- = -$ or $\gamma_\pm$ = invalid.

2). Outcome γ_+ and γ_- occurs with equal probability $P_+ = P_- = 1/2$ and both parties A and B have equal cheating probabilities, $P_\gamma^A = P_\gamma^B = P_\gamma$, which means that the coin tossing is fair.

3). If both parties are honest, the outcome $\gamma_\pm$ = invalid never occurs; $P_\pm = 0$.

4). If any one of the parties is dishonest, the outcome invalid occurs with probability $P_\pm = 1$.

Proposed procedure-I is in fact an asynchronous ideal quantum coin tossing where both parties have equal resource 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 ($P_\gamma^A = P_\gamma^B = 0$), $P_\pm = 0$ if both parties are honest and $P_\pm = 1$ if any one of the parties tries cheating.

Procedure-II

This procedure solves the cryptographic task of secure bit commitment with following code: In the commitment phase, Alice applies same unitary transformation σ on both EPR pairs $|u_a u_b\rangle$ and $|u_{a'} u_r\rangle$ and then performs BSM and gets two bits $u_a u_{a'}$. By doing this, she commit herself to

the bit value $a=0$ if $u_a=0$ and $a=1$ if $u_a=1$. That is, if $u_a u_{a'} \in \{00,01\}$, she is committed to bit $a=0$ and if $u_a u_{a'} \in \{10,11\}$, she is committed to bit $a=1$. In the revealing phase, she announces both her commitment (BSM) and unitary transformations σ she applied before BSM.

Bit commitment

A bit commitment is a cryptographic scheme between two mistrustful parties, committer (Alice) and a receiver (Bob), where Alice commit her to a specific bit b 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 b 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 b. Explicit procedure-II for bit commitment is described below:

(1). Bob secretly prepares an EPR pair $|u_a u_b\rangle$ and sends first qubit to Alice.

(2). Bob prepares another EPR pair $|u_{a'} u_r\rangle$ and sends fist qubit to Alice while second qubit to his agent R such that both Alice and R receive qubits $|u_{a'}\rangle$ and $|u_r\rangle$ simultaneously.

(3). After time t=*x*/c, Alice receives $|u_{a'}\rangle$, applies secret Pauli transformation σ on both qubits $|u_a\rangle$ and $|u_{a'}\rangle$ and performs BSM and gets two classical bits, say $u_a u_{a'} \in \{00,01,10,11\}$, her commitment. This measurement projects the qubits $|u_b\rangle$ and $|u_r\rangle$ into one of the four possible Bell states $|u_b u_r\rangle$ instantly, unknown to both Alice and Bob.

(4). At the same time t, Bob prepares a qubit $|\varphi\rangle \in \{+,-\}$ in the agreed Hadamard basis and teleports the state $|\varphi\rangle$ to R. If BSM result of Bob is $u_b u_{b'}$ while teleporting the state, then R's half of the shared Bell's state becomes one of the corresponding four possible states $|\psi\rangle = \sigma_i |\varphi\rangle$. R measures his system and sends outcome ψ to Bob.

(5). In the revealing phase, Alice announces identity of σ and values of $u_a u_{a'}$ and hence her commitment a.

(6). If values $u_a u_{a'}$ are consistent with swapped entangled state $|u_b u_r\rangle$ and corresponding σ_i, Bob verifies that Alice's commitment is genuine otherwise detects cheating Alice.

Let's consider the previous situation again. Suppose $|u_a u_b\rangle = 00$, $|u_{a'} u_r\rangle = 00$, Alice applies $\sigma_i = I$ and gets $u_a u_{a'} = 00$. The swapped state will be then $|u_b u_r\rangle = 00$. Now if BSM result of Bob is $u_b u_{b'} = 11$, then $\sigma_i = \sigma_z \sigma_x$. If Alice tries to cheat by announcing different values of $\sigma = \sigma_x, \sigma_z, \sigma_z \sigma_x$ and $u_a u_{a'} = 01,10,11$ then Bob will extract $|u_b u_r\rangle = 01,10,11$ and hence different $\sigma_i = \sigma_z, \sigma_x, I$. In short, if Alice alters values from $u_a u_{a'} = 00$ to $u_a u_{a'} = 10$ (or $u_a u_{a'} = 11$), Bob will extract $\sigma_i = \{\sigma_x, I\}$ and hence different ψ. Finally, can Alice cheat by applying σ on only one qubit $|u_a\rangle$ (or $|u_{a'}\rangle$) or σ on $|u_a\rangle$ and σ' on $|u_{a'}\rangle$? It can be seen from table 1 and 2 that answer is again NO.

Proposed bit commitment scheme has very interesting aspect that after making commitment, committer can wait for indefinite time before revealing it. Both committer and receiver extract non-locally correlated classical information in the commitment phase that can be stored and revealed whenever they want. They do not need of quantum memory for storing quantum data for long term bit commitment.

Procedure-III

Let's suppose that R is not an agent of Bob but he is a third party then procedure-I prove to be quantum secret sharing scheme[50] as shown below.

Quantum secret sharing

In procedure-III, EPR pair $|u_a u_b\rangle$ is known to both Alice and Bob while pair $|u_{a'} u_r\rangle$ is known to R and Bob only. Here Bob will be the sender while Alice and R will be receivers (with at least on trustful). R measures $|\psi\rangle$ and gets information of ψ while Alice have BSM result $u_a u_{a'}$. If they meet in causal future of light cone and send $\sigma_z^{u_a} \sigma_x^{u_{a'}} |\psi\rangle$ to Bob, Bob helps them to decode his secret σ_b by announcing required information about shared quantum system $\mathcal{H}_s$. Detailed quantum secret sharing protocol based on proposed framework and its generalization to N party will be discussed in our future work.

Discussion

We defined a general relativistic quantum framework for mistrustful cryptography based on non-local quantum correlations and theory of relativity. The proposed framework determines the actions of both parties through two-fold non-local quantum correlations; entanglement swapping and then teleportation. These correlations are used for secure mistrustful cryptographic protocols then. Moreover, impossibility of superluminal signaling is used for insuring timely responses.

In our relativistic procedure-I, new OT notion, the receiver remains ignorant about the transferred data; he can only get certain information about the data but not its exact identity. 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 oblivious data transferred from the sender to the receiver depends on the actions of both parties in their own secure laboratories instead of sending the actual data encrypted by secret keys over noisy channels. Moreover, the confidentiality and integrity of the data is guaranteed. The receiver rejects the data if the sender tries to modify it after the protocol has been started.

The procedure-I generated through interesting combination of non-locality and theory of special relativity gives then solution of longstanding problems in mistrustful cryptography; unconditionally secure and deterministic two-sided TPSC and asynchronous ideal coin tossing with zero bias. Interesting and fascinating combination of EPR type quantum correlations with causal structure of Minkowski space time show the power of relativistic quantum cryptography in defining tasks that are considered to be impossible in non-relativistic cryptography.

With little modification, procedure-I turns out to be procedure-II and III which came up with unconditionally secure bit commitment and quantum secret sharing respectively. Procedure-II has many interesting aspects like unconditional security and indefinite time for commitment. Both committer and receiver extract non-locally correlated classical information in the commitment phase that can be stored and revealed whenever they want. They do not need of quantum memory for storing quantum systems.

Although it is standard in mistrustful quantum cryptography that both the parties have efficient quantum technologies (quantum computer), the proposed relativistic quantum

framework can be reliably implemented without requiring quantum computer. Both parties can calculate $f(\sigma_a, \sigma_b; |\varphi\rangle)$ securely with existing quantum technologies; photo detectors without needing long term quantum memory. However, even having quantum computers, neither party can cheat successfully.

Finally, we conjecture here that the combination of quantum non-locality and theory of relativity as discussed here is complete and sufficient to solve all the mistrustful cryptographic tasks securely. 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 protocols are purely quantum mechanical where both input and output data is associated with unitary transformations applied on quantum systems. Hence, it would in return prove to be helpful in developing our understanding about the true description of the world, the quantum theory.

References

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. Aci´n, A., Gisin, N. & Masanes, L. From Bells theorem to secure quantum key distribution. *Phys. Rev. Lett.* **97**, 120405 (2006).
13. Aci´n, 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. & Aci´n, 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. Braunstein, S., Mann, A. & Revzen, M. Maximal violation of Bell inequalities for mixed states. *Phys. Rev. Lett*. **68**, 3259 (1992).
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. & Wooters, 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. Hillery, M., Buzek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829 (1999).