Secure positioning and quantum non-local correlations

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

Recently, the problem of quantum position-verification has been extensively analyzed in the formal notion but all existing ceremonial single-round position-verification schemes are insecure. We call here the quantum position-verification schemes formal if verifiers initiate the scheme at time $t = t_i$ and later verify the received outcome at time $t = t_f$ while they perform no other local unitary transformations in time interval $t_i < t < t_f$. We propose here a different notion for quantum position-verification where, instead of sending challenge encoded over flying qubits at time $t = t_i$, one of the verifiers teleports the challenge to the prover while prover is required to measure encoded challenge in specified basis as well as teleport to another verifier while being on the same time slice $t = (t_f - t_i)/2$. After receiving outcomes of single qubit measurements as well as Bell state measurements from prover at time $t = t_f$, the scheme enables verifiers to trace the origin of received outcome and hence identify dishonest provers with very high probability $\rho \geq 1 - 1/2^n$ where n is the number of entangled pairs used. No-signaling principle assures that any group of dishonest provers, not at the position to be verified, cannot simulate their actions with the prover who is supposed to be at the specified position.

Key Words: Quantum information; No-signaling; Position-based quantum cryptography

1. Introduction

Position-based cryptography [1] is the art of protecting information from adversaries through cryptographic schemes based solely on positioning. That is, information-theoretic security is tried to be achieved while the only credential of communicating parties is their positions; sender and receiver have no pre-shared data. Position-based cryptography has many practical applications such as secure communication between military bases at specified positions, communication between a bank and its customers in nearby vicinity, automatic toll collection when vehicles enter at some specified locations etc. To make such applications secure against adversaries not at the specified position, it is customary to devise unconditionally secure position-verification (PV) schemes.

In classical setting, a set of distant and trusted verifiers $\{V_0, V_i; i=1,2,\ldots n\}$ ascertain that the prover P is communicating from his/her claimed position as follows: verifier V_0 sends encoded challenge while rest of the verifiers V_i send pieces of corresponding decoding key to the prover such that both challenge and key reach at Prover's site concurrently. Prover decodes the challenge and sends outcome to all verifiers simultaneously. A secure PV scheme enables the verifiers to validate position jointly if the prover operates from the claimed position and replies the certified outcome to all verifiers in time. However, if the prover P or a set of his/her dishonest agents $\{P_i; i=0,1,2,\ldots n\}$ operate form position other than the claimed one and try to convince verifiers that they are at the specified position, a secure PV scheme enables the verifiers to reject it with high probability. However, an unconditionally secure PV scheme is impossible in classical cryptography where classical data can be copied [1].

We call here the PV schemes formal if verifiers initiate the scheme at time $t = t_i$ and later verify the outcome at time $t = t_f$ while they perform no other local unitary transformations in time interval $t_i < t < t_f$. A large number of quantum position-verification (QPV) schemes [2-8] in formal notion have also been proposed but unfortunately all these schemes are proved to be insecure later. Currently it is known in the literature that if the position of the prover is his/her only credential and he/she does not have any pre-shared data with the verifiers then unconditionally secure QPV in formal notion is impossible [7-9]. That is, security of any QPV scheme constructed in formal notion can be destroyed by coalition of dishonest provers through teleporting quantum states back and forth and performing instantaneous non-local quantum computation, an idea introduced by Vaidman[10]. S. Beigi and R. Konig showed that if dishonest provers posses an exponential (in n) amount of entanglement then they can successfully attack any formal QPV scheme where n qubits are communicated [11]. Burrman *et al* have also shown that the minimum amount of entanglement needed to perform a successful attack on any formal QPV scheme must be at least linear in the number of communicated qubits [8,12].

However, some weaker models of formal QPV are possible; either if dishonest provers have bounded amount of pre-shared entanglement or the prover and the verifiers have pre-shared classical/quantum data. Single-round QPV schemes PV_{BB84} and its EPR version PV^{ε}_{BB84} [8,13] are secure only in the No-PE model; dishonest provers do not have pre-shared entanglement. QPV scheme [14] is secure where the prover and one of the verifiers have pre-shared classical bit string unknown to dishonest provers. The secret classical data is then used as a key to authenticate the communication. Key-based QPV can also be securely achieved if verifiers and the prover have pre-shared entangled states [15]. The verifiers and the prover obtain secret keys through entanglement swapping [16,17] and later use these keys for authentication of secret messages. Although schemes [14,15] are not standard for positioning alone, these schemes can be useful for providing a second layer of security, along with usual cryptographic techniques.

We propose here a different notion for quantum position-verification where actions of the prover are determined through quantum non-local correlations generated by local single qubit measurements as well as Bell state measurements (BSM) [18] performed by both verifiers and the prover at the same time slice. Instead of sending challenge encoded over flying qubits at time $t = t_i$ as performed in formal notion, one of the verifiers teleports the challenge to the prover while prover is required to measure encoded challenge in specified basis as well as teleport to another verifier while being on the same time slice $t = (t_f - t_i)/2$. After receiving measurement outcomes from prover at time $t = t_f$, the scheme enables verifiers to trace the origin of received outcome and hence identify dishonest provers with very high probability.

It allows controlling the prover's actions and bound him/her to perform single qubit measurements as well as BSM only after receiving challenge (teleported) from one of the verifiers. In this setting, no-signaling principle assures that any group of dishonest provers, not at the position to be verified, cannot simulate their actions with the prover who is supposed to be at the specified position. Proposed scheme guarantees secure positioning with standard conditions: (i) Verifiers have no pre-shared quantum/classical data with the prover, (ii) Dishonest provers have sufficient pre-shared entanglement and there is no bound on their computational powers.

In quantum information science, it has been demonstrated successfully that quantum non-local correlations have wide range of applications in quantum computing [19], quantum communication [17,20], quantum cryptography [21-25], and crucial impacts on the foundation of

quantum mechanics [26-28]. Moreover, no-signaling principle along with methods of quantum mechanics has advanced quantum cryptography in multiple ways [29-43]. Our proposed QPV scheme, based on the combination of quantum non-local correlations and no-signaling principle, is different from formal notion for PV in its construction; bounding prover to receive, measure, and teleport challenge simultaneously allows constructing PV scheme where all the verifiers and the prover apply local unitary operations on the same space-like hyper surface from where prover is required to return outcome. In this setting, verifiers can trace the origin of received measurement outcome, to be sent at speed of light, and hence differentiate between the position of prover and dishonest provers. On the other hand, in all quantum/classical PV schemes in formal notion, all verifiers as well as the prover applies local unitary operations on the same null-like hyper surfaces; verifiers send challenge and key to the prover who then replies outcome while being on the intersection of null-like hyper surface connecting him/her with the verifiers and hence insecure [31].

2. Teleportation

Teleportation is the most important step in our proposed scheme for secure positioning. In general teleportation works as follows [17]: Suppose Alice and Bob share a maximally entangled state in Bell basis

$$\left|\beta_{ab}\right\rangle = \frac{\left|0\right\rangle\left|b\right\rangle + (-1)^{a}\left|1\right\rangle\left|1\oplus b\right\rangle}{\sqrt{2}} \tag{1}$$

where $a,b \in \{0,1\}$ and $\oplus$ denotes addition with mod 2. Bob can send an arbitrary quantum state $\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$ to Alice by performing BSM on $\left|\psi\right\rangle$ and his half of entangled pair. If Bob gets classical 2-bit string bb', Alice's entangled half instantly becomes one of the four possibilities:

$$\left|\psi'\right\rangle = \sigma_z^k \sigma_x^{k'} \left|\psi\right\rangle \tag{2}$$

where k and k' depend upon Bob's MSB result bb' as well as Bell state $\left|\beta_{ab}\right\rangle$ shared between Alice and Bob. For example, if $\left|\beta_{ab}\right\rangle = \left|\beta_{00}\right\rangle$ then $k = b$ and $k' = b'$, if $\left|\beta_{ab}\right\rangle = \left|\beta_{01}\right\rangle$ then $k = b$ and $k' = 1 \oplus b'$, if $\left|\beta_{ab}\right\rangle = \left|\beta_{10}\right\rangle$ then $k = 1 \oplus b$ and $k' = b'$, and for $\left|\beta_{ab}\right\rangle = \left|\beta_{11}\right\rangle$, $k = 1 \oplus b$ and $k' = 1 \oplus b'$. If Bob sends two classical bits bb' to Alice who knows the identity of entangled state $\left|\beta_{ab}\right\rangle$, she can easily recover $\left|\psi\right\rangle$ by applying suitable unitary $U = \sigma_z^k \sigma_x^{k'}$.

However, without knowing either shared entangled state $\left|\beta_{ab}\right\rangle$ or BSM result bb' of Bob, $\left|\psi'\right\rangle$ remains totally random to Alice. Moreover, soon after performing and getting BSM result bb', Bob knows that how the Alice's entangled half would have been transformed. That is, identity of state $\left|\psi'\right\rangle = \sigma_z^k \sigma_x^{k'} \left|\psi\right\rangle$ purely depends upon Bob's BSM result bb' and entangled state $\left|\beta_{ab}\right\rangle$, hence, remains known to Bob without any communication from Alice to Bob. Finally, BSM performed by Bob teleports the state $\left|\psi\right\rangle$ to Alice instantaneously, except for a possible transformation by $U = \sigma_z^k \sigma_x^{k'}$ which can only be corrected after receiving classical communication from Bob. All possible initially shared entangled states between Alice and Bob, Bob's BSM result, and corresponding transformations $U = \sigma_z^k \sigma_x^{k'}$ are summarized in table 1. In the rest of the paper, we use the word teleportation for BSM only irrespective of whether classical communication channel between Alice and Bob exists or not.

$\lvert\beta_{ab}\rangle$	bb'				$U=\sigma_z^k\sigma_x^{k'}$			
$\lvert\beta_{00}\rangle$	00	01	10	11	I	σ_x	σ_z	$\sigma_z\sigma_x$
$\lvert\beta_{01}\rangle$	00	01	10	11	σ_x	I	$\sigma_z\sigma_x$	σ_z
$\lvert\beta_{10}\rangle$	00	01	10	11	σ_z	$\sigma_z\sigma_x$	I	σ_x
$\lvert\beta_{11}\rangle$	00	01	10	11	$\sigma_z\sigma_x$	σ_z	σ_x	I

Table 1: Teleportation: If sender Bob and receiver Alice share entangled state $\lvert\beta_{ab}\rangle$, BSM performed by Bob on quantum state $\lvert\psi\rangle$ and his entangled half teleports the state $\lvert\psi\rangle$ to Alice instantly except for a possible transformation by $U=\sigma_z^k\sigma_x^{k'}$ on $\lvert\psi\rangle$ where k and k' depend upon Bob's BSM result bb' as well as initially shared Bell state $\lvert\beta_{ab}\rangle$.

3. Setup for quantum position-verification

We assume that the sites of the prover and verifiers are secure from adversary; enabling them to store and hide the secret data and process. We also assume that the verifiers can communicate both classical and quantum information securely with each other. However, all the quantum/classical channels between verifier(s) and the prover are insecure. Moreover, there is no bound on pre-shared entanglement, storage, computing, receiving and transmitting powers of dishonest provers. They can interfere or jam communication of the prover without being detected. In short, dishonest provers have full control of environment except sites of the prover and verifiers.

All verifiers and the prover have fixed positions in Minkowski spacetime. Both quantum and classical signals can be sent between prover and verifiers at the speed of light while the time for information processing at their sites is negligible. For simplicity, we consider only two verifiers V_0 and V_1 at distant reference stations collinear with prover P, such that the prover is at a distance x from both reference stations.

Since prover P is required to return outcome of his local trace decreasing unitary operators to both verifiers in the second half of every QPV, so either measurement basis must be publically known or verifiers need to send information of measurement basis to P. This allows P to make copies of challenge states and send to multiple verifiers. To make the analysis simple and consistent with both formal (section 4 and 5) and proposed notions of QPV (section 6 and 7), we assume that (i) single qubit systems will be measured in either $\delta_0\in\{+,-\}$ or $\delta_1\in\{+i,-i\}$ basis prescribed by verifier $f(v_0,v_1)\to\{0,1\}$ where $\lvert\pm\rangle=\left(\lvert0\rangle\pm\lvert1\rangle\right)/2$ and $\lvert\pm i\rangle=\left(\lvert0\rangle\pm i\lvert1\rangle\right)/2$, (ii) two-qubit systems will be measured in Bell basis, and (iii) quantum systems sent to the prover P by verifiers V_0 and V_1 will be denoted by Hilbert space representation H_{p_0} and H_{p_1} respectively.

4. Formal notion of position-verification

In the formal notion of PV in classical setting, a set of distant verifiers $\{V_0,V_i;\ i=1,2,\ldots n\}$ ascertain that the prover P is communicating from his/her claimed position by sending encoded challenge and corresponding decoding information to the prover. That is, verifier V_0 (say) sends encoded challenge while rest of the verifiers V_i send pieces of corresponding decoding information to the prover P such that both challenge and all the components of key reach at the

site of P concurrently. The prover P decodes the challenge and sends outcome k to all the verifiers simultaneously. Formal notion of PV with two verifiers V_0 and V_1 is shown in figure 1.

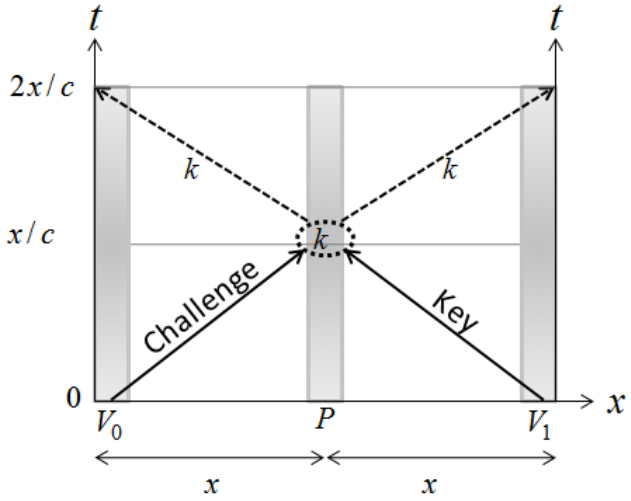

Figure 1: Formal position verification in classical setting: Verifier V_0 sends challenge to the prover P while verifier V_1 sends decoding key such that both challenge and key reach at P's site concurrently. Prover decodes the challenge and sends outcome k to both verifiers simultaneously.

The general structure of formal notion for QPV scheme in 1+1 dimensional Minkowski spacetime can be described as follows: verifiers V_0 and V_1 agree on secret classical information $\mathcal{V}_0$ and $\mathcal{V}_1$ which correspond to unitary transformations U_{v_0} and U_{v_1} respectively. They also agree upon quantum system $H_{p_0p_1} = H_{p_0} \otimes H_{p_1}$ which can be a product system, entangled system, or component of some larger quantum system $H = H_{p_0} \otimes H_{p_1} \otimes H_{v_0} \otimes H_{v_1}$. Verifiers V_0 and V_1 initiate the scheme at time $t = 0$ by sending components $U_{v_0}(H_{p_0})$ and $U_{v_1}(H_{p_1})$ to the prover respectively. The prover then applies unitary transformations $U^{\dagger} = U^{\dagger}_{v_0} \otimes U^{\dagger}_{v_1}$ on $H'_{p_0p_1} = (U_{v_0} \otimes U_{v_1})H_{p_0p_1}$ at time $t = x/c$ and replies the outcome to both verifiers. At time $t = 2x/c$, verifiers validate the exact position of P if he replies correct information $U^{\dagger}(H'_{p_0p_1})$, consistent with $\mathcal{V}_0$ and $\mathcal{V}_1$ and hence larger quantum system H, within allocated time.

In this formal notion, verifiers initiate the scheme at time $t = 0$ and later verify the outcome at time $t = 2x/c$ while they perform no other local unitary transformations in time interval $0 < t < 2x/c$. It allows dishonest provers, not at the position to be verified, to receive information from verifiers, manipulate, and later simulate their outcomes with that of prover at the specified position. Hence, general structure for formal QPV and a number of its variants are all proved to be insecure against entanglement-based attacks [7-9]. Such a formal notion for QPV schemes with two verifiers V_0 and V_1 is shown in figure 2(a).

5. Security analysis-I: Formal QPV schemes

If the verifiers and the prover have no pre-shared data while the dishonest provers have pre-shared entanglement, all formal QPV schemes are proved to be insecure [7-9] against group of dishonest provers $\{P_0, P_1\}$ at positions different from the one to be verified. Suppose P_0 is between V_0 and P at position $(x\text{-}\delta,0)$ while P_1 is between V_1 and P at position $(x\text{+}\delta,0)$

respectively where $\delta << x$ is the radius of prover's site. Moreover, suppose P_0 and P_1 also have arbitrary amount of pre-shared entanglement denoted by $H_{p_0'p_1'} = H_{p_0'} \otimes H_{p_1'}$. Dishonest provers P_0 and P_1 can obtain both quantum systems $U_{v_0}(H_{p_0})$ and $U_{v_1}(H_{p_1})$ as well as classical information $\mathcal{V}_0$ and $\mathcal{V}_1$ respectively before the prover P, at time $t = (x-\delta)/c$.

By consuming pre-shared entanglement $H_{p_0'p_1'}$, specially separated P_0 and P_1 can transform system $H_{p_0p_1}$ to $U_{p_0p_1}(H_{p_0p_1})$ instantaneously by applying set of unitaries $U_{p_0p_1} = \{U_{v_0}^{\dagger} \otimes U_{v_1}^{\dagger}, U_{p_0} \otimes U_{p_1}\}$ locally without any communication with each other. As a result, by exchanging their local unitary outcomes, they can agree upon a definite outcome of transformation $U_{p_0p_1}(H_{p_0p_1})$ at time $t = (x+\delta)/c$ and correct it such that $(T_{p_0} \otimes T_{p_1})U_{p_0p_1}(H_{p_0p_1}) \approx U^{\dagger}(H_{p_0p_1})$. Here, $T_{p_0} \otimes T_{p_1}$ depends upon local unitary outcomes of P_0 and P_1. Hence, they can reply exact information to both verifiers within time, $t = 2x/c$.

In conclusion, all formal QPV scheme are insecure as follows: dishonest provers receive information from verifiers at time $t = (x-\delta)/c$, manipulate in the time interval $(x-\delta)/c \le t \le (x+\delta)/c$, and later at time $t = (x+\delta)/c$ simulate their outcomes with that of the prover P at time $t = x/c$. The verifiers cannot differentiate whether they received outcome $U^{\dagger}(H_{p_0p_1})$ from the prover P or dishonest provers $\{P_0, P_1\}$ as shown in figure 3(a).

6. Proposed QPV scheme

Instead of sending quantum system $H_{p_0} \otimes H_{p_1}$ and classical information $\mathcal{V}_0$ and $\mathcal{V}_1$ to the prover at time $t = 0$ and then wait till time $t = 2x/c$ as they do in formal notion, methods of quantum mechanics allow verifiers to apply some unitary transformations during time interval $0 < t < 2x/c$ as well and lock the challenge. That is, verifiers V_0 and V_1 send quantum system $H_{p_0} \otimes H_{p_1}$ and classical information $\mathcal{V}_0$ and $\mathcal{V}_1$ to the prover at time $t = 0$ while prover receive this information on the intersection of null-like hyper surfaces connecting him with the verifiers. Later, at space-like hyper surface $t = x/c$, V_0 teleports the challenge $|\psi\rangle \in \{\delta_0, \delta_1\}$ to the prover who first measures H_{p_0} in either $\delta_0 \in \{+,-\}$ or $\delta_1 \in \{+i,-i\}$ basis depending upon outcome $f(v_0, v_1) \to \{0,1\}$ as well as performs BSM on $H_{p_0} \otimes H_{p_1}$ and returns the measurement outcomes to both V_0 and V_1. Explicit procedure of our proposed quantum scheme for secure positioning is shown in figure 2(b) and is described below.

1). At time $t = 0$, verifiers V_0 and V_1 secretly prepare EPR pairs $|\beta_{v_0p_0}\rangle \in H_{v_0} \otimes H_{p_0}$ and $|\beta_{v_1p_1}\rangle \in H_{v_1} \otimes H_{p_1}$ respectively and each sends second half to P. They also send classical information $\mathcal{V}_0$ and $\mathcal{V}_1$ to the prover respectively such that $\mathcal{V}_0$, $\mathcal{V}_1$ and $H_{p_0} \otimes H_{p_1}$ reach at the P's site concurrently.

2). At time $t = x/c$, V_0 teleports state $|\psi\rangle \in H_{\psi}$ where $|\psi\rangle \in \{\delta_0, \delta_1\}$ to P. As a result V_0 gets classical information $vv' \in \{00,01,10,11\}$ while the P's half becomes $|\psi'\rangle = \sigma_z^k \sigma_x^{k'} |\psi\rangle$ where values of k and k' depend on vv' and $|\beta_{v_0p_0}\rangle$ only known to V_0. At the same time t=x/c, P measures

his half H_{p_0} in either $\delta_0 \in \{+,-\}$ or $\delta_1 \in \{+i,-i\}$ basis depending upon $f(v_0, v_1) \to \{0,1\}$ and teleports outcome $|\psi'\rangle$ to V_1 over EPR channel $|\beta_{v_1 p_1}\rangle$. Entangled half in possession of V_1 becomes $|\psi''\rangle = \sigma_z^l \sigma_x^{l'} |\psi'\rangle$ where values of l and l' depend on P's BSM result $pp' \in \{00,01,10,11\}$ and identity of $|\beta_{v_1 p_1}\rangle$. Simultaneously, P sends classical 2-bit string $k = pp'$ as well as $k_{\psi'} \in \{+,-,+i,-i\}$, measurement outcome of $|\psi'\rangle$, to both V_0 and V_1.

3). At time $t = 2x/c$, verifier V_1 verifies whether $|\psi'\rangle$ and $|\psi''\rangle$ are consistent with BSM result $k = pp'$ of P or not. Similarly V_0 validates whether $|\psi\rangle$ and $|\psi'\rangle$ are consistent with his BSM result vv' or not. If both V_0 and V_1 receive verified information from P, they exchange their measurement outcomes somewhere in their causal future and verify the position of P if P has replied authenticated outcome within allocated time; at $t = 2x/c$.

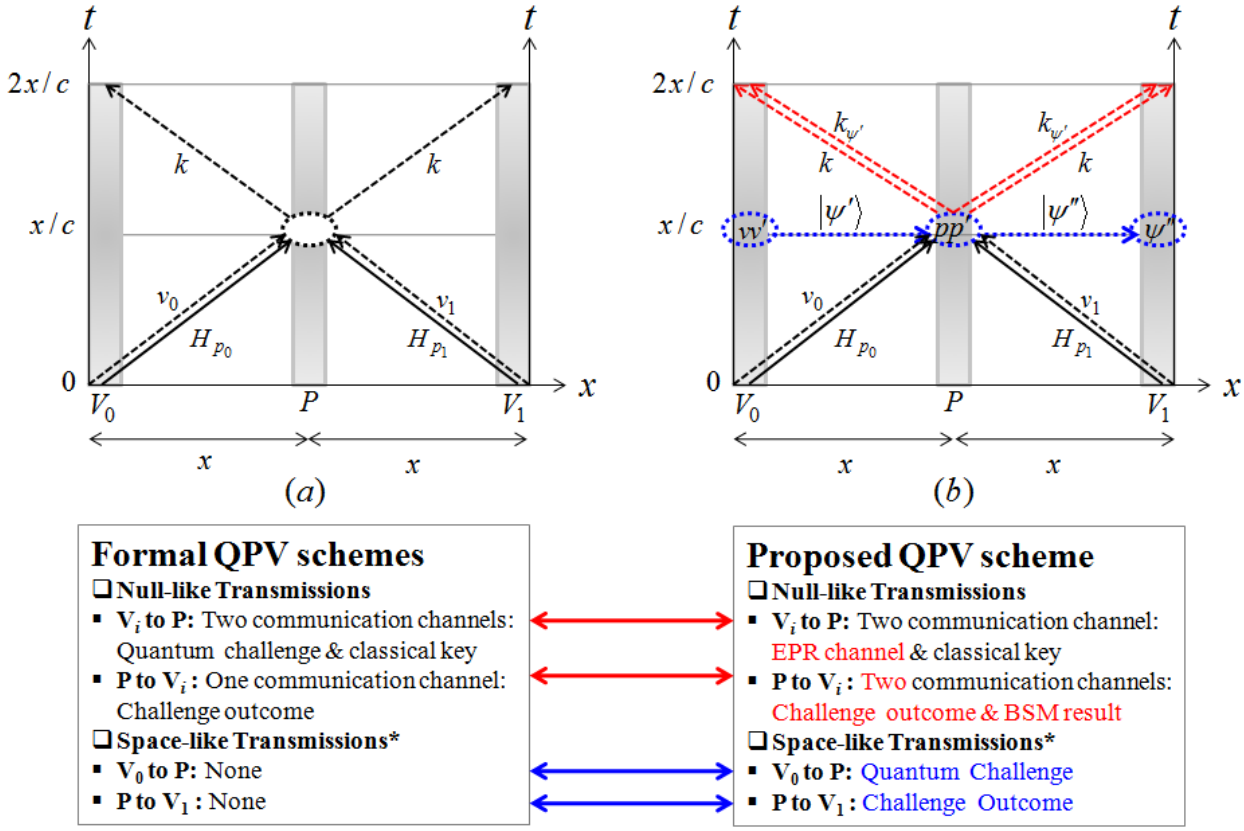

Figure 2: Comparison of formal and proposed QPV schemes: Solid arrows represent quantum states, dotted arrows show teleportation without classical communication while dashed arrows represent classical communication. **(a)** Formal notion of QPV schemes where verifiers initiate the scheme at time $t = 0$ and later verify the outcome at time $t = 2x/c$ while they perform no other local unitary transformations in time interval $0 < t < 2x/c$. **(b)** Proposed QPV scheme where verifiers initiate the scheme at time $t = 0$, V_0 performs BSM while V_1 performs single qubit measurement at the same time $t = x/c$, and later verify the outcome at time $t = 2x/c$.

*By space-like transmission, we mean here BSM which transforms space-like separated entangled half instantaneously.

7. Security analysis-II: Proposed QPV scheme

Here we show that our proposed scheme is secure against entanglement-based attacks discussed in section 5. Our security argument is very simple: verifiers start the scheme at time $t = 0$ by preparing quantum system $H = H_{p_0} \otimes H_{p_1} \otimes H_{\psi} \otimes H_{v_0} \otimes H_{v_1}$, send component system $H_{p_0} \otimes H_{p_1}$ as well as classical information $\mathcal{V}_0$ and $\mathcal{V}_1$ to prover P over null-like hyper surfaces, and later control P's spacetime position by teleporting the challenge $|\psi\rangle \in \{\delta_0, \delta_1\}$ at space-like hyper surface $t = x/c$. Before spacetime position at time slice $t = 2x/c$ (occupied by prover P), dishonest provers cannot manipulate the challenge $|\psi\rangle \in H_{\psi}$ since (i) quantum system $H_{p_0} \otimes H_{p_1}$ does not contains any information about the challenge $|\psi\rangle \in \{\delta_0, \delta_1\}$ and (ii) classical information $\mathcal{V}_0$ and $\mathcal{V}_1$ is not accessible at a single point hence definite outcome of function $f(v_0, v_1) \to \{0,1\}$ cannot be found anywhere in the causal past of prover P.

Suppose dishonest prover P_0 is between V_0 and P at position $(x\text{-}\delta,0)$ while P_1 is between V_1 and P at position $(x+\delta,0)$ respectively. Now P_0 can intercept H_{p_0} and get entangled with the verifier V_0 by sharing quantum system $H_{v_0p_0} = H_{v_0} \otimes H_{p_0}$ while P_1 intercepts and shares entangled system $H_{v_1p_1} = H_{v_1} \otimes H_{p_1}$ with verifier V_1 at $t = (x-\delta)/c$. As prover P requires, dishonest provers have to reply both $k_{\psi'} \in \{+,-,+i,-i\}$ as well as classical 2-bit string $k = pp'$ simultaneously. In other words, dishonest provers have to receive teleported state $|\psi'\rangle$ from V_0, measure in either $\delta_0 \in \{+,-\}$ or $\delta_1 \in \{+i,-i\}$ basis depending upon outcome $f(v_0, v_1) \to \{0,1\}$ and teleport same state $|\psi'\rangle$ to V_1. That is, since verifier V_0 knows the definite state $|\psi'\rangle = \sigma_z^k \sigma_x^{k'} |\psi\rangle$ from initially prepared EPR pair $|\beta_{v_0p_0}\rangle$ and his BSM result vv', hence dishonest provers need to agree upon correlated state $|\psi'\rangle = \sigma_z^k \sigma_x^{k'} |\psi\rangle$ and $k = pp'$.

Since verifier V_0 teleports quantum state $|\psi\rangle$ over EPR pair $|\beta_{v_0p_0}\rangle$ not before time $t = x/c$, hence specially separated dishonest provers P_0 and P_1 are restricted from performing non-local instantaneous computations during time interval $(x-\delta)/c \le t < x/c$; any attempt of measurement on $H_{p_0p_1} = H_{p_0} \otimes H_{p_1}$ without knowing both $\mathcal{V}_0$ and $\mathcal{V}_1$ will collapse the larger system $H = H_{p_0} \otimes H_{p_1} \otimes H_{\psi} \otimes H_{v_0} \otimes H_{v_1}$ in an arbitrary state. For example, if dishonest provers attempt non-local instantaneous computations in time interval $(x-\delta)/c \le t < x/c$ and get state $|\varphi'\rangle$ after measureing H_{p_0}, they cannot agree upon definite unitary transformation U such that $U|\varphi'\rangle = |\psi\rangle$. As a result, they cannot get definite information $k_{\psi'} \in \{+,-,+i,-i\}$ and classical 2-bit string $k = pp'$ simulated with local outcome of verifiers.

However, P_0 and P_1 can perform non-local instantaneous computations through multiple rounds of teleportation [10] at time $t = x/c$ and can agree on $|\psi'\rangle = \sigma_z^k \sigma_x^{k'} |\psi\rangle$ and required classical 2-bit string $k = pp'$ only at time $t = (x+2\delta)/c$. As a result, they can send required information to both V_0 and V_1 but not before time $t = (2x+\delta)/c$. In conclusion, if the verifiers run proposed scheme with $H_{v_0} = (C^2)^{\otimes n}$, $H_{v_1} = (C^2)^{\otimes n}$ and $H_p = H_{p_0} \otimes H_{p_1} = (C^2)^{\otimes n} \otimes (C^2)^{\otimes n}$, it

enables them to identify dishonest provers with very high probability; $\rho \geq 1-1/2^n$. Proposed QPV scheme in the presence of dishonest provers P_0 and P_1 is shown in figure 3(b).

We assumed that P is equidistant between V_0 and V_1 to make our analysis simple. However, this condition doesn't make any compromise on the security analysis of proposed scheme or any limitations on its practical feasibility. The most crucial step in our construction is step 2, where verifiers send (receive) quantum information to (from) prover while being on the same space-like hyper surface $t = x/c$. If this could be arranged, then in step 3 it doesn't matter whether verifiers receive information replied by the prover at same time $t = 2x/c$ or not. Both verifiers can count round trip time on their own clocks and verify or abort the positioning by exchanging their data. If P is not equidistant between V_0 and V_1, then V_0 and V_1 have to send their respective entangled halves H_{p_0} and H_{p_1} such that both quantum systems reach at the prover's site concurrently. As a result, both verifiers and the prover need to share quantum system $H = H_{p_0} \otimes H_{p_1} \otimes H_{\psi} \otimes H_{v_0} \otimes H_{v_1}$ at the same space-like hyper surface which is necessary for unconditionally secure positioning.

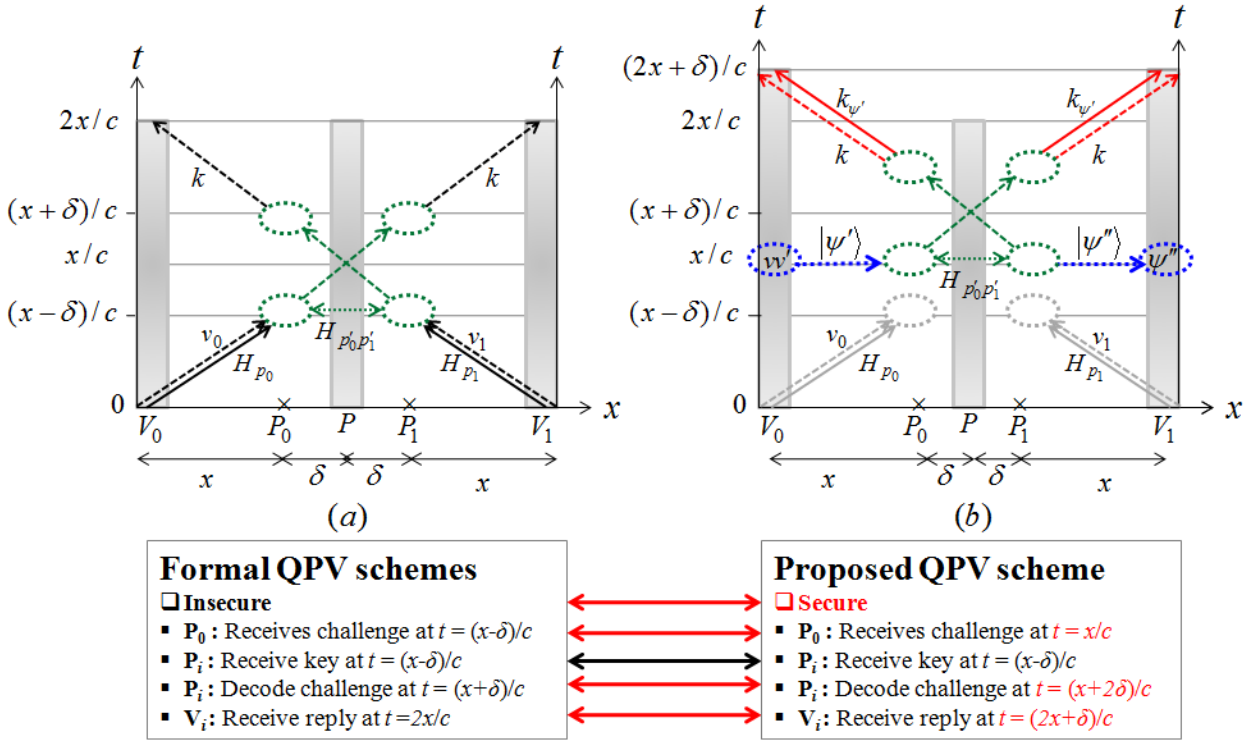

Figure 3: Comparison of formal and proposed QPV schemes in the presence of dishonest provers P_0 and P_1: Solid arrows represent qubits; dotted arrows show teleportation without classical communication while dashed arrows show classical information. **(a)** Formal notion of QPV and its insecurity against entanglement-based quantum attacks. **(b)** Proposed QPV scheme for secure positioning where dishonest provers P_0 and P_1 cannot simulate their actions with that of prover at specified position.

8. Discussion

We propose here a different notion for quantum position-verification where actions of the prover are determined through quantum non-local correlations generated by local single qubit measurements as well as Bell state measurements performed by both verifiers and the prover at

the same time slice from where prover is required to return outcome of the scheme. Instead of sending challenge encoded over flying qubits as performed in formal notion, one of the verifiers teleports the challenge to the prover while prover is required to measure encoded challenge in specified basis as well as teleport to another verifier and return outcome while being on the same time slice. The causality principle insures that the proposed quantum position-verification scheme is secure against entanglement-based attacks even if eavesdroppers have infinite amount of pre-shared entanglement and power of non-local quantum measurements in negligible time.

In quantum information science, it has been demonstrated successfully that quantum non-local correlations have wide range of applications in quantum computing, quantum communication, quantum cryptography, and crucial impacts on the foundation of quantum mechanics. In this connection, the combination of quantum non-local correlations with no-signaling principle as discussed here promises fascinating advancement in getting unconditional security from dishonest users. For example, the receiver can trust the information he receives only if the scheme verifies position of the sender and validates sender's actions in a single round. This bounds sender to reveal valid information within allocated time and guarantees him/her that the receiver on the other hand will not be able to get information unless sender reveals.

The proposed scheme for secure-positioning can be efficiently and reliably implemented using existing quantum technologies. Since the quantum memory for reliable storage of entangled quantum systems is not available yet, we use more practical setup where the prover and verifiers can measure quantum information in prescribed basis, store outcomes and create multiple copies. It would lead to a number of applications where communicating parties need to store information and then reveal after arbitrarily long time such as bit commitment and digital signatures. Proposed scheme for positioning would also be an important tool for modern technologies such as driverless quantum vehicles; an interesting application of positioning introduced by R. Malaney recently.

In conclusion, the basic difference between previously proposed position-verification schemes based on formal notion and our proposed scheme based on quantum non-local correlations is the construction of schemes in Minkowski spacetime; resources of quantum mechanics such as entanglement and teleportation allow verifiers to apply local unitary transformations at suitable spacetime location to control the actions of the prover. Hopefully, this notion of secure positioning would help in broaden the scope of formulating quantum tasks among mistrustful communicating parties in Minkowski spacetime. In the much broader perspective, this notion for secure positioning would be useful to understand relativistic quantum theory on the basis of quantum information science. For example, proposed setup allows receivers to trace the origin of received information sent from somewhere in their causal past at speed of light.

9. References

[1] Chandran, N., Goyal, V., Moriarty, R., Ostrovsky, R.: Position based cryptography. In proceedings of Advances in Cryptology — CRYPTO 2009, pages 391–407 Santa Barbara, CA, USA (Lect. Notes Comput. Sci. Vol. **5677**, Springer) (Aug. 16-20, 2009).

[2] Kent, A., Munro, W., Spiller, T.,Beausoleil, R.: Tagging systems, US20067075438 (2006).

[3] Kent, A., Munro, W., Spiller, T.: Quantum tagging: authenticating location via quantum information and relativistic signalling constraints. Phys. Rev. A. **84**, 012326 (2011).

[4] Malaney, R.: Location-dependent communications using quantum entanglement. Phys. Rev. A. **81**, 042319 (2010).

[5] Malaney, R.: Quantum location verification in noisy channels. arXiv:1004.4689.
[6] Malaney, R.: Location verification in quantum communications. US 20120195597 A1 (2010).
[7] Lau, H., Lo, H.: Insecurity of position-based quantum-cryptography protocols against entanglement attacks. Phys. Rev. A. **83**, 012322 (2011).
[8] 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) (Aug. 14-18, 2011)
[9] Brassard, G.: The conundrum of secure positioning. Nature **479**, 307-308; DOI:10.1038/479307a (2011).
[10] Vaidman, L.: Instantaneous measurement of nonlocal variables. Phys. Rev. Lett. **90**, 010402 (2003).
[11] Beigi, S., Konig, R.: Simultaneous instantaneous non-local quantum computation with applications to position-based cryptography. New J. Phys. **13,** 093036 (2011).
[12] Buhrman, H., Fehr, S., Schaffner, C., Speelman, F.: The Garden-Hose Model. arXiv:1109.2563 (2011).
[13] Tomamichel, M., Fehr, F., Kaniewski, J., Wehner, S.: A monogamy-of-entanglement game with applications to device-independent quantum cryptography. New J. Phys. **15,** 103002 (2013).
[14] Kent, A.: Quantum tagging for tags containing secret classical data. Phys. Rev. A. **84**, 022335 (2011).
[15] Nadeem, M.: Position-based quantum cryptography over untrusted networks. Laser Phys. **24** 085202 (2014).
[16] Zukowski, M., Zeilinger, A., Horne, M., Ekert, A.: Event-ready-detectors'' Bell experiment via entanglement swapping. Phys. Rev. Lett. **71**, 4287 (1993).
[17] 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).
[18] Braunstein, S., Mann, A., Revzen, M.: Maximal violation of Bell inequalities for mixed states. Phys. Rev. Lett. **68**, 3259 (1992).
[19] Gottesman, D., Chuang, I.L.: Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. Nature **402**, 390 (1999).
[20] Bennett, C., Wiesner, S.: Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys. Rev. Lett. 69, 2881 (1992).
[21] Ekert, A.: Quantum Cryptography Based on Bell's Theorem. Phys. Rev. Lett. **67**, 661 (1991).
[22] Nadeem, M.: Quantum cryptography – an information theoretic security. arXiv: 1507.07918 (2015).
[23] Nadeem, M.: Quantum digital signature scheme. arXiv: 1507.03581 (2015).
[24] Nadeem**,** M.: Unconditionally secure commitment in position-based quantum cryptography. Sci. Rep. **4**, 6774; DOI:10.1038/srep06774 (2014).
[25] Nadeem, M., Noor Ul Ain.: Secure and authenticated quantum secret sharing. arXiv: 1506.08558 (2015).
[26] Einstein, A., Podolsky, B. & Rosen, N. Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. **47**, 777 (1935).
[27] Bell, J. On the Einstein Podolsky Rosen paradox. Physics **1**, 195 (1965).

[28] Clauser, J., Horne, M., Shimony, A., Holt, R.: Proposed Experiment to Test Local Hidden-Variable Theories. Phys. Rev. Lett. **23**, 880 (1969).
[29] Nadeem**,** M**.:** Delayed choice relativistic quantum bit commitment with arbitrarily long commitment time. arXiv:1504.03316 (2014).
[30] Nadeem, M.: Quantum non-locality, causality and mistrustful cryptography**.** arXiv:1407.7025 (2014).
[31] Nadeem, M.: The causal structure of Minkowski spacetime - possibilities and impossibilities of secure positioning. arXiv: 1505.01839 (2015).
[32] Kent, A.: Quantum tasks in Minkowski space. Class. Quant. Grav. **29**, 224013 (2012).
[33] Kent, A.: A no-summoning theorem in relativistic quantum theory. Q. Info. Proc. **12**, 1023-1032 (2013).
[34] 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).
[35] Barrett, J., Hardy, L., Kent, A.: No signalling and quantum key distribution. Phys. Rev. Lett. **95**, 010503 (2005).
[36] Colbeck, R.: Quantum and Relativistic Protocols For Secure Multi-Party Computation. arXiv:0911.3814 (2009).
[37] Masanes, L., Renner, R., Christandl, M., Winter, A., Barrett, J.: Unconditional security of key distribution from causality constraints. IEEE Transactions on Information Theory, **60**, 4973; DOI:10.1109/TIT.2014.2329417 (2014).
[38] Masanes, L.: Universally composable privacy amplification from causality constraints. Phys. Rev. Lett. **102**, 140501 (2009).
[39] Masanes, L., Pironio, S., Aci´n, A.: Secure device-independent quantum key distribution with causally independent measurement devices. Nature Commun. **2**, 238 (2011).
[40] Aci´n, A., Gisin, N., Masanes, L.: From Bells theorem to secure quantum key distribution. Phys. Rev. Lett. **97**, 120405 (2006).
[41] Aci´n, A., Massar, S., Pironio, S.: Efficient quantum key distribution secure against no-signalling eavesdroppers. New J. Phys. **8**, 126 (2006).
[42] Pironio, S. et al.: Random numbers certified by Bell's theorem. Nature **464**, 1021-1024 (2010).
[43] Malaney, R.: Quantum car. arXiv:1512.0321 (2015).