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 propose here a different notion for position-verification where distant verifiers determine the actions of the prover through quantum non-local correlations generated by local measurements at the provers' site: instead of sending challenge encoded over flying qubits, one of the verifiers teleports the challenge to the prover while prover is required to perform single qubit measurements as well as Bell state measurements and return the outcomes. It allows controlling the prover's actions and bound him/her to receive challenge from one of the verifiers, measure in known basis, teleport to another verifier, and return the measurement outcomes to all verifiers simultaneously. Here, 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. The scheme enables verifiers to trace the origin of received information and hence identify dishonest provers with very high probability $\rho \geq 1-1/2^n$, where n is the number of entangled pairs used.

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 formal notion of PV scheme, 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; Verifier V_0 sends encrypted challenge while rest of the verifiers V_i send pieces of corresponding decryption key to the prover such that both challenge and key reach at Prover's site concurrently. Prover decrypts 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 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.

An unconditionally secure PV scheme is impossible in classical cryptography where classical data can be copied [1]. 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 PV 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_{BB84}^{ε} [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 QPV where one of the verifiers, instead of sending challenge encoded over flying qubits (entangled or not), teleports the challenge to the prover while prover is required to perform single qubit measurements as well as Bell state measurements (BSM) [18] and return the outcomes. It allows controlling the prover's actions and bound him/her to receive challenge from one of the verifiers, measure in known basis, teleport to another verifier, and return the measurement outcomes to all verifiers simultaneously. 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 arbitrary amount of 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 [29-42]. 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 are on the same space-like hyper surface. 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, all previous quantum/classical PV schemes in formal notion were built upon 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

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

where $a,b \in \{0,1\}$ and $\oplus$ denotes addition with mod 2. Bob can send an arbitrary quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to Alice instantly by performing BSM on $|\psi\rangle$ 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:

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

where k and k' depend upon Bob's MSB result bb' as well as Bell state $|\beta_{ab}\rangle$ shared between Alice and Bob. For example, if they share a Bell state $|\beta_{00}\rangle$ then $k = b$ and $k' = b'$. If shared Bell state is $|\beta_{01}\rangle$ then $k = b$ and $k' = 1 \oplus b'$. If they share Bell state $|\beta_{10}\rangle$ then $k = 1 \oplus b$ and $k' = b'$ while for $|\beta_{11}\rangle$, $k = 1 \oplus b$ and $k' = 1 \oplus b'$. If Bob sends two classical bits bb' to Alice who knows the identity of entangled state $|\beta_{ab}\rangle$, she can easily recover $|\psi\rangle$ by applying suitable unitary operators. However, without knowing shared entangled state $|\beta_{ab}\rangle$ or BSM result bb' of Bob, $|\psi'\rangle$ remains totally random to Alice and we use this fact in our scheme for secure positioning.

3. Setup for position-verification

We assume that the sites of the prover and verifiers are secure from adversary; enabling them to store and hide the quantum 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 decrypted challenge to both verifiers in the second half of every QPV, so either measurement basis must be publically known or one of the verifiers needs to send information of measurement basis to P. This allows P to make copies of decrypted challenge 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 measurement basis are publically known as follows (i) single qubit systems will always be

measured in $\{\delta_0, \delta_1\}$ basis where $\delta_0 = (|0\rangle + i|1\rangle)/2$ and $\delta_1 = (|0\rangle - i|1\rangle)/2$. (ii) two-qubit systems will always be measured in Bell basis. Moreover, quantum systems sent to the prover P by verifiers V_0 and V_1 will always be denoted by Hilbert space representation H_{p_0} and H_{p_1} respectively.

4. Formal notion of position-verification

To introduce the formal notion of QPV in detail, we describe a general procedure for single-round QPV scheme and then a number of its variants. We conclude that all these formal schemes are proved to be insecure against entanglement-based attacks [7-9]. This section contains a partial review of QPV, suitable for our proposed scheme in next section.

In the formal notion of QPV scheme, 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 both challenge encoded over quantum system and corresponding decryption classical information to the prover. That is, Verifier V_0 (say) sends encrypted challenge while rest of the verifiers V_i send pieces of corresponding decryption information to the prover P such that both quantum and classical information reach at the site of P concurrently. The prover P decrypts the quantum challenge and sends outcome k to all the verifiers simultaneously. Formal notion of QPV with two verifiers V_0 and V_1 is shown in figure 1.

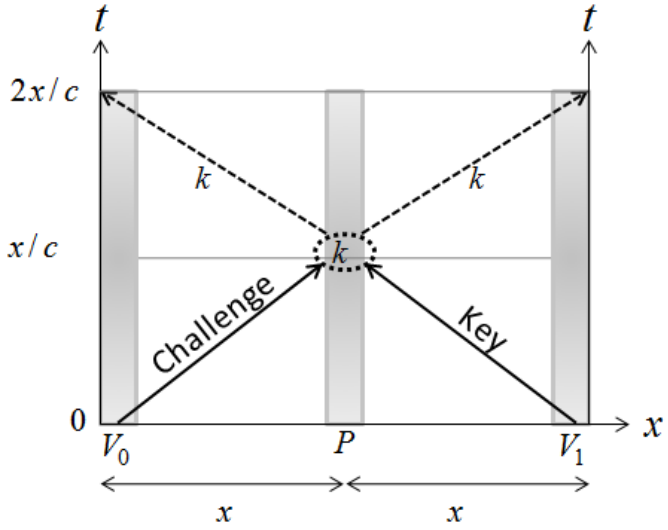

Figure 1: Formal position verification: Verifier V_0 sends challenge to the prover P while verifier V_1 sends decrypting key such that both challenge and key reach at P's site concurrently. Prover decrypts the challenge and sends outcome to both verifiers simultaneously.

4.1 QPV-I: Suppose verifiers V_0 and V_1 priorly agree on secret classical information $\mathcal{V}_0$ and $\mathcal{V}_1$ and challenge $|\psi\rangle \in \{\delta_0, \delta_1\}$ unknown to the prover P. The classical information $\mathcal{V}_0$ and $\mathcal{V}_1$ correspond to unitary operators U_{v_0} and U_{v_1} respectively such that $U_{v_0} U_{v_1} = I$. The operators U_{v_0} and U_{v_1} can be rotation operators $R_{v_0}(\theta_0)$ and $R_{v_1}(\theta_1)$ respectively such that $\theta_1 = -\theta_0$ with publically known value for θ. Here θ_0 denotes clockwise while that of θ_1 counterclockwise rotation about x-axis on Bloch 2-sphere.

1). At time t=0, verifier V_0 sends encoded challenge $U_{v_0}|\psi\rangle \in H_{p_0}$ while V_1 sends classical information $\mathcal{V}_1$ encoded over single qubit state $|v_1\rangle \in H_{p_1}$ to P.

2). At time t=*x*/c, P receives $\mathcal{V}_1$ by measuring $|v_1\rangle$, applies corresponding unitary operation U_{v_1} on $U_{v_0}|\psi\rangle$, measures $|\psi\rangle$, and returns the outcome to both V_0 and V_1. Remember, P performs all single qubit measurements in $\{\delta_0, \delta_1\}$ basis.

3). At time t=2*x*/c, verifiers V_0 and V_1 authenticate the position of P if he/she returns valid outcome within allocated time otherwise abort.

4.2 QPV-II: QPV-I is the simplest version of PV_{BB84} [8], publically known orthogonal basis are used instead of non-orthogonal BB84 basis. It can easily be generalized to a scheme similar to that of EPR version PV_{BB84}^{ε} [8,13] as follows: Suppose verifiers V_0 and V_1 priorly agree on secret classical information $\mathcal{V}_0$ and $\mathcal{V}_1$ and a Bell state $|\beta_{ab}\rangle \in H_{v_0} \otimes H_{p_0}$ unknown to the prover P. Here $|\beta_{ab}\rangle$ and $\mathcal{V}_0$ are kept by V_0 while $\mathcal{V}_1$ is possessed by V_1. The classical information $\mathcal{V}_0$ and $\mathcal{V}_1$ correspond to unitary operators U_{v_0} and U_{v_1} respectively such that $U_{v_0}U_{v_1} = U$ where $U|0\rangle = |\delta_0\rangle$ and $U|1\rangle = |\delta_1\rangle$. If we consider U_{v_0} and U_{v_1} as rotation operators $R_{v_0}(\theta_0)$ and $R_{v_1}(\theta_1)$ respectively on Bloch 2-sphere, then $\theta_0 + \theta_1 = \pi/2$.

1). At time t=0, verifier V_0 applies $U \otimes U_{v_0}$ on $H_{v_0} \otimes H_{p_0}$ and sends $U_{v_0}(H_{p_0})$ to P. Similarly, V_1 sends classical information $\mathcal{V}_1$ encoded over single qubit state $|v_1\rangle \in H_{p_1}$ to P.

2). At time t=*x*/c, P applies unitary operation U_{v_1} on $U_{v_0}(H_{p_0})$, measures $U_{v_1}U_{v_0}(H_{p_0})$ in $\{\delta_0, \delta_1\}$basis, and returns the outcome to both V_0 and V_1.

3). At time t=2*x*/c, verifiers V_0 and V_1 authenticate the position of P if he/she returns valid outcome within allocated time otherwise abort.

4.3 QPV-III: The scheme QPV-II turns out to be a Malaney's scheme [4] now with modified construction as follows: Suppose verifiers V_0 and V_1 priorly agree on secret 2-bits $ab \in \{00,01,10,11\}$ unknown to the prover P encoded over pre-shared Bell state $|\beta_{ab}\rangle \in H_{p_0} \otimes H_{p_1}$ among them. Verifiers also agree on classical information $\mathcal{V}_0$ and $\mathcal{V}_1$ that correspond to unitary operators U_{v_0} and U_{v_1} respectively.

1). At time t=0, verifier V_0 sends $U_{v_0}(H_{p_0})$ while V_1 sends $U_{v_1}(H_{p_1})$ to P. Simultaneously, both V_0 and V_1 send classical information $\mathcal{V}_0$ and $\mathcal{V}_1$ to P respectively such that both quantum and classical information reach at P's site concurrently.

2). At time t=*x*/c, P applies unitary operators $U_{v_0}^{\dagger}$ and $U_{v_1}^{\dagger}$ on respective qubits, performs BSM on $(U_{v_0}^{\dagger} \otimes U_{v_1}^{\dagger})(U_{v_0}H_{p_0} \otimes U_{v_1}H_{p_1})$, and returns the outcome $k = a'b'$ to both V_0 and V_1 immediately.

3). At time t=2*x*/c, verifiers V_0 and V_1 authenticate the position of P if he/she returns valid outcome, $a'b' = ab$, within allocated time otherwise abort.

5. Security analysis-I: Entanglement-based quantum attacks

If the verifiers and the prover have no pre-shared data while the dishonest provers have pre-shared entanglement, QPV schemes I-III and a number of their variants [6] constructed over

formal notions are proved to be insecure against entanglement-based attacks relying on non-local instantaneous quantum computations by dishonest provers [8,9,11,12].

For example, the general structure of formal notion for QPV schemes can be summarized as follows: the prover P receives a quantum system $U_{v_0}(H_{p_0})$ from the verifier V_0 and a system $U_{v_1}(H_{p_1})$ from V_1. Here H_{p_0} and H_{p_1} can be components of some larger quantum system $H = H_{p_0} \otimes H_{p_1} \otimes H_{v_0} \otimes H_{v_1}$. The prover then applies some unitary transformations $U^{\dagger} = U_{v_0}^{\dagger} \otimes U_{v_1}^{\dagger}$ on $H_{p_0 p_1} = U_{v_0}(H_{p_0}) \otimes U_{v_1}(H_{p_1})$ depending upon the classical information $\mathcal{V}_0$ and $\mathcal{V}_1$ obtained from V_0 and V_1 respectively and replies the outcome to both V_0 and V_1. In this notion, the verifiers validate the exact position of the prover P if he replies correct information $U^{\dagger}(H_{p_0 p_1})$, consistent with $\mathcal{V}_0$ and $\mathcal{V}_1$ and hence larger quantum system H , within allocated time. Such a general notion for formal QPV schemes with two verifiers V_0 and V_1 is shown in figure 2(a).

Such formal QPV schemes are not secure against group of dishonest provers $\{P_0, P_1\}$ at positions different from the one to be verified figure 3(a). Suppose P_0 is between V_0 and P at position (x-δ,0) while P_1 is between V_1 and P at position (x+δ,0) respectively. Here δ<< 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-δ)/c. By consuming pre-shared entanglement $H_{p_0' p_1'}$, specially separated P_0 and P_1 can transform system $H_{p_0 p_1}$ to $U^{\dagger}(H_{p_0 p_1})$ instantaneously by applying $U_{v_0}^{\dagger}$ and $U_{v_1}^{\dagger}$ locally without any communication. As a result, by exchanging their measurement outcomes, they can agree upon a definite outcome of transformation $U^{\dagger}(H_{p_0 p_1})$ at time t=(x+δ)/c. Hence, they can reply exact information to both verifiers within time, t=2x/c. The verifiers cannot differentiate whether they received outcome from the prover P or dishonest provers $\{P_0, P_1\}$.

6. Proposed QPV scheme based on non-local quantum correlations

Instead of sending both quantum system $H_{p_0} \otimes H_{p_1}$ and classical information $\mathcal{V}_0$ and $\mathcal{V}_1$ to the prover simultaneously, verifiers V_0 and V_1 send only quantum systems H_{p_0} and H_{p_1} respectively on null-like hyper surfaces connecting them with the prover. 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 known $\{\delta_0, \delta_1\}$ basis 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 described below.

1). At time t=0, verifiers V_0 and V_1 secretly prepare EPR pairs $|\beta_{v_0 p_0}\rangle \in H_{v_0} \otimes H_{p_0}$ and $|\beta_{v_1 p_1}\rangle \in H_{v_1} \otimes H_{p_1}$ respectively and each sends second half to P.

2). At time t=x/c, V_0 teleports state $|\psi\rangle \in \{\delta_0, \delta_1\}$ 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 $|\beta_{v_0 p_0}\rangle$ only known to V_0. At the same time t=x/c, P measures his half in $\{\delta_0, \delta_1\}$ basis 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 bit $k = p \oplus p'$ and quantum state $|\psi'\rangle$ 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 $k = p \oplus p'$ 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.

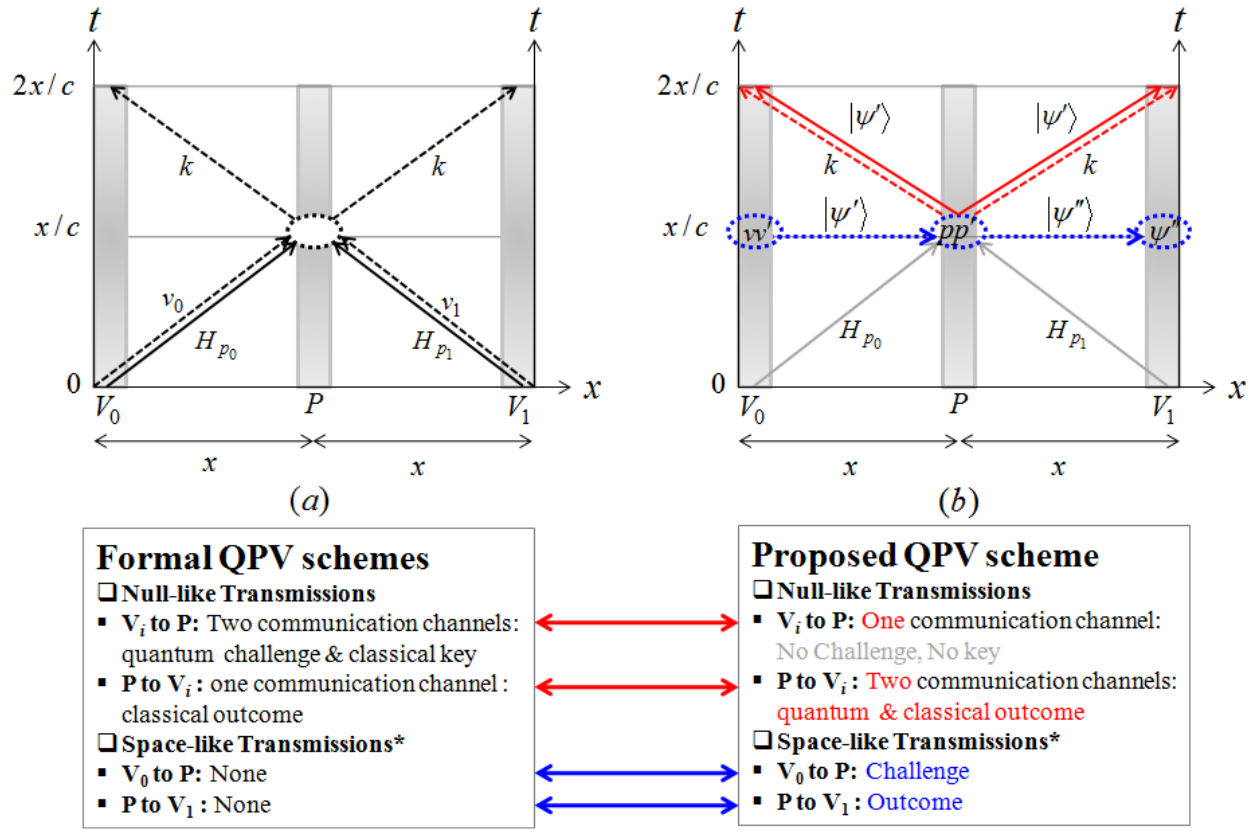

Figure 2: Comparison of formal and proposed QPV schemes: Solid arrows represent quantum states, dotted arrows show teleportation while dashed arrows represent classical communication. **(a)** Formal notion of QPV schemes where verifiers send both quantum challenge as well as classical decryption information to the prover who replies back to verifiers with classical information. **(b)** Proposed QPV scheme where verifiers send entangled halves carrying no information and later, at time t=x/c, V_0 teleports challenge to the prover while prover teleports again to V_1 and replies measurement outcome to both V_0 and V_1.

In the proposed scheme, classical communication from the prover to verifiers is reduced to single bit only; $k = p \oplus p' \in \{0,1\}$, because $|\psi\rangle \in \{\delta_0, \delta_1\}$ and hence $|\psi'\rangle \in \{\delta_0, \delta_1\}$. In this setting, Pauli encodings $\sigma_z^l \sigma_x^{l'} \in \{I, \sigma_z \sigma_x\}$ give same outcome $|\psi''\rangle = \sigma_z^l \sigma_x^{l'} |\psi'\rangle$ at V_1 site up to overall phase factor. Similarly, $\sigma_z^l \sigma_x^{l'} \in \{\sigma_x, \sigma_z\}$ give same outcome $|\psi''\rangle$. For example, if $|\beta_{v_1 p_1}\rangle \in \{|\beta_{00}\rangle, |\beta_{11}\rangle\}$, then P's BSM result $pp' \in \{00,11\}$ will result in $\sigma_z^l \sigma_x^{l'} \in \{I, \sigma_z \sigma_x\}$ while that of $pp' \in \{10,01\}$ will generate $\sigma_z^l \sigma_x^{l'} \in \{\sigma_x, \sigma_z\}$. Similarly, if $|\beta_{v_1 p_1}\rangle \in \{|\beta_{10}\rangle, |\beta_{01}\rangle\}$, then P's BSM result $pp' \in \{00,11\}$ will result in $\sigma_z^l \sigma_x^{l'} \in \{\sigma_x, \sigma_z\}$ while that of $pp' \in \{10,01\}$ will generate $\sigma_z^l \sigma_x^{l'} \in \{I, \sigma_z \sigma_x\}$. Hence, instead of sending classical 2-bit string pp' to verifiers, prover can simply announce $k = p \oplus p' \in \{0,1\}$.

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=2*x*/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 $H = H_{p_0} \otimes H_{p_1} \otimes H_{v_0} \otimes H_{v_1}$ at the same space-like hyper surface which is necessary for unconditionally secure positioning.

7. Security analysis-II: Proposed QPV scheme

Here we show that our proposed scheme is secure against entanglement-based attacks discussed in section 5: verifiers neither send qubit-wise encrypted quantum systems as a challenge nor classical information for decrypting that challenge. Instead, verifiers determine the actions of the prover through non-local correlations generated by local measurements from a specific position. The verifiers starts the scheme at time t=0 by preparing quantum system $H = H_{v_0 p_0} \otimes H_{v_1 p_1}$ where $H_{v_0 p_0} = H_{v_0} \otimes H_{p_0}$ is a maximally entangled system to be shared between V_0 and P while while $H_{v_1 p_1} = H_{v_1} \otimes H_{p_1}$ is the entangled system to be shared between V_1 and P share at time t=*x*/c. Verifiers control the spacetime position where they want to reveal the challenge through teleportation. Before that spacetime position (occupied by prover P), dishonest provers cannot extract required information from quantum systems H_{p_0} and H_{p_1} in the causal past of prover P since these quantum systems do not contain information which is required to resend verifiers.

Suppose dishonest prover P_0 is between V_0 and P at position (x-δ,0) while P_1 is between V_1 and P at position (x+δ,0) respectively. Now P_0 can intercept H_{p_0} and get entangled with the verifier V_0 in a state $H_{v_0 p_0}$ while P_1 shares entangled state $H_{v_1 p_1}$ with verifier V_1 at t=(x-δ)/c.

In our proposed scheme, prover P (or dishonest provers) has to reply with both quantum state $|\psi'\rangle$ and classical bit $k = p \oplus p'$ simultaneously. In other words, P (or dishonest provers)

has to receive teleported state $|\psi'\rangle$ from V_0 and then teleport same state $|\psi'\rangle$ to V_1. Since verifier V_0 knows the definite state $|\psi'\rangle = \sigma_z^k \sigma_x^{k'} |\psi\rangle$ from initially prepared EPR pair $|\beta_{v_0 p_0}\rangle$ and his BSM result vv', hence verifiers V_0 and V_1 can verify whether the announced state $|\psi'\rangle$ and $k = p \oplus p'$ from prover P (or dishonest provers) is consistent with $|\psi\rangle$ and $|\psi''\rangle = \sigma_z^l \sigma_x^{l'} |\psi'\rangle$ or not.

Moreover, since verifier V_0 teleports quantum state $|\psi\rangle$ over EPR pair $|\beta_{v_0 p_0}\rangle$ 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 $\{(x-\delta)/c, x/c\}$; any measurement on $H_{p_0 p_1} = H_{p_0} \otimes H_{p_1}$ will collapse the larger system $H = H_{v_0 p_0} \otimes H_{v_1 p_1}$. Hence, even if P_0 and P_1 have infinite amount of pre-shared entanglement and perform non-local instantaneous computations through multiple rounds of teleportation [10] at time t=x/c, P_0 and P_1 can agree on $|\psi'\rangle = \sigma_z^k \sigma_x^{k'} |\psi\rangle$ and required classical bit $k = p \oplus p'$ (BSM) only at time t=(x+2δ)/c. As a result, they can send required information to both V_0 and V_1 not before time t=(2x+δ)/c. Proposed QPV scheme in the presence of dishonest provers P_0 and P_1 is shown in figure 3(b). 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; $\rho \geq 1 - 1/2^n$.

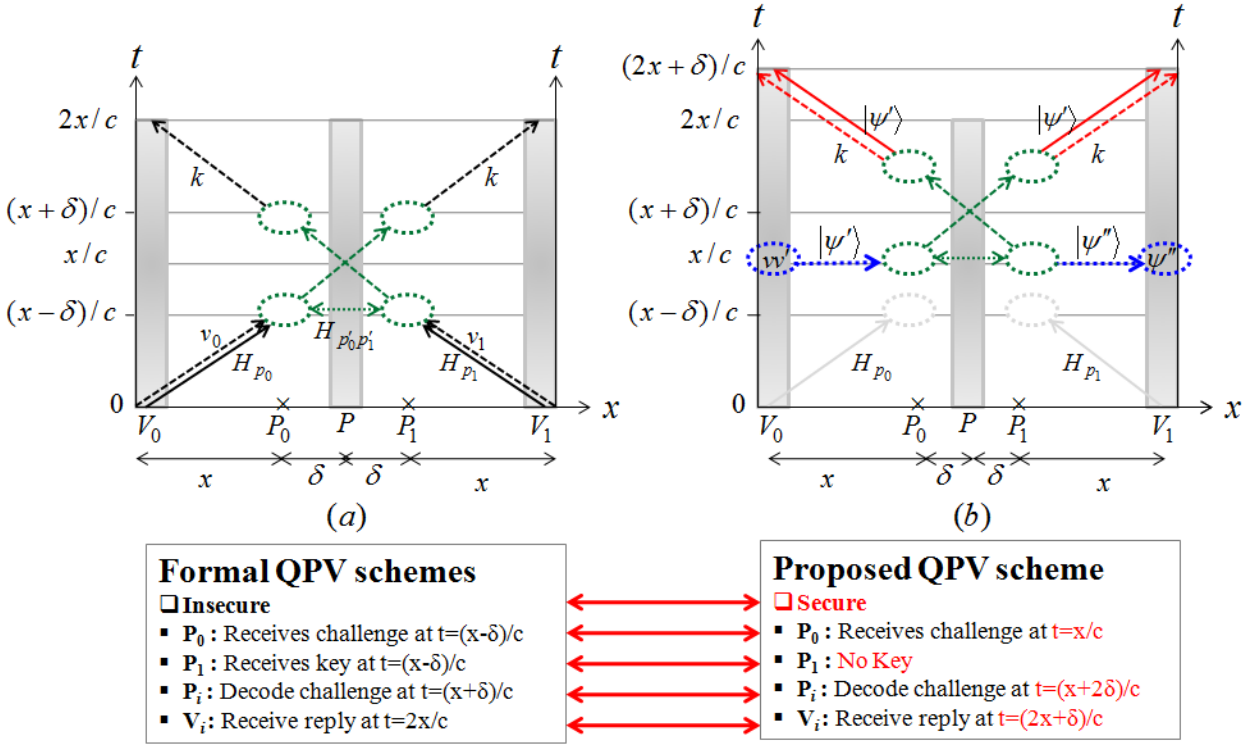

Figure 3: Comparison of formal and proposed QPV schemes in the presence of dishonest provers P_0 and P_1: Solid arrows represent qubits; dotted arrow shows teleportation while dashed arrows show classical information. **(a)** Formal notion of QPV and its insecurity against entanglement-based quantum attacks. **(b)** Proposed QPV scheme for secure positioning where dishonest provers P_0 and P_1 cannot simulate their actions with the prover at specified position.

8. Discussion

We proposed here a different notion for secure positioning where distant verifiers do not send a secret key to the prover along with challenge, as used to do in insecure formal notion, but the actions of the prover are determined through non-local correlations obtained by local measurements at the provers' site. 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 publically known 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 [29,30]. 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 [43].

In conclusion, the basic difference between previous 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 [31]. Hopefully, this notion of secure positioning would help in broaden the scope of formulating quantum tasks 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).