Position-based quantum cryptography over untrusted networks

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

Received 17 April 2014
Accepted for publication 20 May 2014
Published 15 July 2014

Abstract
In this article, we propose quantum position verification (QPV) schemes where all the channels are untrusted except the position of the prover and distant reference stations of verifiers. We review and analyze the existing QPV schemes containing some pre-shared data between the prover and verifiers. Most of these schemes are based on non-cryptographic assumptions, i.e. quantum/classical channels between the verifiers are secure. It seems impractical in an environment fully controlled by adversaries and would lead to security compromise in practical implementations. However, our proposed formula for QPV is more robust, secure and according to the standard assumptions of cryptography. Furthermore, once the position of the prover is verified, our schemes establish secret keys in parallel and can be used for authentication and secret communication between the prover and verifiers.

Keywords: quantum cryptography, entanglement swapping

1. Introduction

The central task of position-based cryptography (PBC) is position verification. A prover proves to a set of verifiers located at certain distant reference stations that he/she is at a specific position [1]. Unconditional security in classical PBC is impossible because of cloning. The eavesdroppers can copy classical information, manipulate that information and get desired results before an honest prover. Recently, many authors tried to achieve information with theoretically secure position-based cryptography in quantum settings [2–9]. However, Buhrman et al showed that all proposed quantum position verification (QPV) schemes are insecure. They proved that position verification is impossible if the position of the prover is his/her only credential and he/she does not have any advantage over eavesdroppers beyond his position, whereas eavesdroppers are allowed to share an arbitrarily large entanglement [8]. They showed that the security of any position-based quantum cryptographic scheme can be destroyed by eavesdroppers through teleporting quantum states back and forth and performing instantaneous nonlocal quantum computation, an idea introduced by Vaidman [10]. However, they proved that if eavesdroppers do not share any entanglement (no pre-shared entanglement [No-PE] model), then secure PBQC is possible. Furthermore, Beigi and Konig showed that if eavesdroppers possess an exponential (in n) amount of entanglement, then they can successfully attack any PBQC scheme where verifiers share a secret n-bit string [11].

In the search for unconditional security, some authors proposed that secure PBQC is possible if the prover and the verifiers pre-share some data [7–9]. However, we show in section 4 that these schemes will remain no more secure if channels between the distant verifiers are insecure. In this article, we propose that position-based quantum cryptography can be made unconditionally secure even over untrusted networks through entanglement swapping [12]. In our proposed schemes, only the position of the prover and the reference stations are secure from an adversary while all channels between them are insecure. The only advantage the honest prover has over eavesdroppers is publicly known pre-shared entangled states with the verifiers. These entangled states can be shared through a source between them that emits labeled pairs of entangled qubits (photons in our case). Furthermore, our schemes require only quantum channels where adversaries can easily be detected by the quantum measurement principle and the quantum no-cloning theorem [13]. If our QPV
schemes are performed $N$ times successively and no adversaries are detected, then the same schemes establish secret keys and can be used for authentication and secret information transfer between the prover and verifiers. Our article is organized as follows. In section 2, we introduce QPV; the protocol most often used in different QPV schemes, entanglement swapping, is described in section 3. We review existing QPV schemes and analyze them in standard cryptographic settings in section 4; in section 5, we present our proposed QPV schemes. In sections 6 and 7, we extend our QPV schemes to position-based key generation and position-based authentication, respectively. Finally, we analyze our schemes under known attacks in section 8 and summarize the article in section 9.

2. Introduction to quantum position verification

In a general position verification scheme, an honest prover located at a specified position convinces a set of $N$ verifiers at distant reference stations that he/she is indeed at the specific position. Different verifiers send a secret message and a key to decrypt that message in pieces, i.e., each verifier sends a bit of key to $P$ such that all the key bits and the message arrive at the position of $P$ concurrently. If $P$ decrypts the message correctly and sends the result to all verifiers in time, then the position verification scheme will enable the verifiers to verify his/her position jointly. But if one or a set of dishonest provers, not at the specified position, intercepts the communication and tries to convince verifiers that he/she is at the specified position, then a secure position verification scheme will enable the verifiers to reject it with high probability. Such secure position verification is impossible in classical cryptography because of cloning, but the quantum measurement principle and quantum no-cloning theorem can help in developing secure position verification schemes. To introduce the idea of quantum position verification in detail, we review the basic one-round QPV scheme $PV_{BB84}$ based on the BB84 encoding [14]. More detailed analysis of this scheme can be found elsewhere [8]. An explicit procedure of the scheme for two verifiers follows:

1) $V_0$ prepares two secret random bits $x, y \in [0, 1]$ and sends them to $V_1$ through a secure channel between them.
2) $V_0$ prepares the qubit $H^x|y\rangle$ and sends it to $P$. Concurrently, $V_1$ sends the bit $y$ to $P$ such that $H^y|y\rangle$ and $y$ arrive at the same time at $P$.
3) $P$ measures the qubit in basis $y$ and sends the result to both $V_0$ and $V_1$ immediately.
4) $V_0$ and $V_1$ can verify the position of $P$ by confirming the validity of the result and comparing the arrival time of response.

The authors showed that this scheme is secure only in the no-pre-shared entanglement (No-PE) model, where the adversaries do not have pre-shared entangled quantum data but have full power of quantum computing [8]. This scheme can easily be generalized to higher dimensions where multiple verifiers send secret information to $P$ in pieces.

3. Entanglement swapping

Entanglement swapping [12] is an interesting extension of teleportation [15], in fact, teleportation of entanglement. It causes two quantum particles to become non-locally correlated even if they have never interacted. Let Alice possess two particles 1 and 2 and let Bob have particle 3, while Charlie keeps particle 4 in his possession. Moreover, suppose Bob and Charlie never meet each other (particles 3 and 4 are initially uncorrelated) but Bob’s particle 3 is entangled with Alice’s particle 1 while Charlie’s particle 4 is entangled with Alice’s particle 2 in one of the Bell states:

$$|\psi_{u, u}^{x y}\rangle = \frac{|0\rangle|u\rangle + (-1)^{u_1}|1\rangle|1 \oplus u_1\rangle}{\sqrt{2}}$$

where $u_1, u_2 \in [0, 1]$ and $\oplus$ denotes addition with mod 2. The initial quantum state of four particles 1, 2, 3, and 4 will be:

$$|\psi_{v, v}^{x y}\rangle \otimes |\psi_{u, u}^{x y}\rangle = \frac{|0\rangle|v_1\rangle + (-1)^{v_1}|1\rangle|1 \oplus v_1\rangle}{\sqrt{2}}$$

By performing Bell state measurement (BSM) [16] on her particles 1 and 2, Alice can project Bob’s and Charlie’s particles (3 and 4) into one of the four possible Bell states:

$$|\psi_{w, w}^{x y}\rangle \otimes |\psi_{v, v}^{x y}\rangle = \frac{|0\rangle|w_1\rangle + (-1)^{w_1}|1\rangle|1 \oplus w_1\rangle}{\sqrt{2}}$$

Initially, entangled pairs were (1, 3) and (2, 4). But after BSM by Alice, irrespective of outcome, entangled pairs are (1, 2) and (3, 4). One can say that particles 3 and 4, initially uncorrelated, become non-locally correlated through entanglement swapping. To complete the protocol, Alice will have to communicate two classical bits, e.g., to Bob, who can then share a definite Bell state $|\psi_{u, u}^{x y}\rangle$ with Charlie after applying suitable unitary local transformations. If initial Bell states of entangled pairs (1, 3) and (2, 4) are known to Alice, then she will be certain about the Bell state of pair (3, 4) after performing BSM on qubits 1 and 2. For example, if initial Bell states of entangled pairs (1, 3) and (2, 4) were $|\psi_{u_0, u_0}^{x y}\rangle$ and $|\psi_{v_0, v_0}^{x y}\rangle$ and Alice measures particles 1 and 2 in the state $|\psi_{u_0, u_0}^{x y}\rangle$, then particles 3 and 4 will be entangled in state $|\psi_{w_0, w_0}^{x y}\rangle$. Detailed calculations can be found in the appendix. All possible BSM results of Alice and corresponding Bell states of particles 3 and 4 are summarized in table 1. For simplicity, we write $|\psi_{x y}\rangle$ as $u \oplus v$, $u \oplus v$ from now on.

4. Existing QPV schemes containing pre-shared data

For simplicity, we discuss all the existing schemes in one dimension. Higher-dimensional generalization of these schemes is straightforward and can be found in corresponding references. First, we review these schemes under their proposed assumptions in our analysis of these schemes; we
consider the standard assumptions of cryptography. That is, eavesdroppers have full control over the environment except position of the prover and reference stations. They have unlimited power of receiving, transmitting and manipulating quantum classical information in no time. Furthermore, they can jam the communication between the honest prover and verifiers.

### 4.1. QPV scheme-I

Kent proposed that secure QPV is possible if the prover and one of the verifiers pre-share some classical bit string unknown to eavesdroppers [7]. These secret data can be then used as a secret key to authenticate the communication. The prover and the verifier can generate the longer key to authenticate the communication. The prover retrieves the key bit in pairs, i.e. 1 and 2, and sends this bit to both V0 and V1 simultaneously.

1) V0 and V1 send randomly chosen bits x_i and y_i from their classical strings x and y, respectively. They send these data to P such that these bits arrive at P in pairs, i.e. x_1 and y_1 arriving simultaneously, then x_2 and y_2, and so on.

2) P retrieves the key bit k_{i2+j_2}, and sends this bit to both V0 and V1 simultaneously.

3) V0 can verify the position of P if the key bit is correct and arrives in time. If P succeeds N times by sending the correct bit, then V0 authenticates the position of P.

This scheme seems secure but impractical because security of this scheme is based on a pre-shared classical secret key that can be expanded through quantum key distribution.

### 4.2. QPV scheme-II

Buhrman et al proposed a scheme, PV_{BB84} EPR version, where one of the verifiers shares an entangled state with the prover [8]. The scheme also requires a secret bit string shared between the verifiers who send this secret information to the prover publically. In one dimension, the scheme is given as follows:

1) V0 prepares secret random bit y i.e. 0 or 1 and sends it to V1 through the secure channel between them.

2) V0 prepares a two-qubit Bell state, keeps one qubit and sends the other to P. Simultaneously, V1 sends bit y to P such that both entangled qubit and y reach P at the same time.

3) P measures the qubit in basis y and sends the result to both V0 and V1 immediately.

4) When the measurement result of P arrives, V0 then measures his qubit and sends the result to V1 through the secure channel.

5) V0 and V1 can verify the position of P by confirming the validity of the result and comparing the arrival time of response.

Again, this scheme is secure only in the No-PE model. In the cryptographic environment where eavesdroppers can possess and arbitrarily share large entangled states, security can be spoofed. Detailed security analysis and a higher-dimensional version of this scheme can be found elsewhere [8].

### 4.3. QPV scheme-III

Malaney proposed a large class of QPV schemes in which different distant verifiers and the prover share entangled data. His work was granted a US patent in 2012 [9]. One of his QPV schemes based on entanglement swapping is as follows:

1) Let V0 possess an entangled qubit pair (1, 2) and let V1 posses an entangled qubit pair (3, 4) in one of the four Bell states, for instance both in 11.

2) At time t_0, V0 sends qubit 2 to P and at time t_1, V1 sends qubit 3 to P through public channels.

3) P performs a BSM on qubits 2 and 3 and gets one of the Bell states, say 10. This measurement projects the qubits 1 and 4 into Bell state 10, only known to P at the moment. P immediately sends his/her measurement result to both V0 and V1 simultaneously.

4) Suppose V0 and V1 receive the BSM result from P at times T_0 and T_1, respectively. V1 immediately transmits his/her qubit 4, time T_1, and BSM result to V0 through the secure public channel between them.

5) V0 performs BSM on qubits 1 and 4 and confirms that his/her result (10) is consistent with that of P.

6) V0 and V1 can verify the position of P if times T_0–t_0 and T_1–t_1 are consistent with the position of P.

Unconditional security of this scheme is based on the unreal assumption that channels between distant verifiers are secure. If channels between the verifiers are not secure, then adversaries can easily break this scheme. They can intercept qubits 2 and 3, process them, and can get the secret BSM result from P. Moreover, both V0 and V1 cannot detect the presence of adversaries in this scheme. The cheating scheme by the adversaries is shown in figure 1 and is described as follows:

1) Let V0 possesses an entangled qubit pair (1, 2) and let V1 possesses an entangled qubit pair (3, 4) in one of the four Bell states, for instance both in 11. Moreover, suppose eavesdropper E_0 lying between V0 and P possesses entangled qubit pair (5, 6) in Bell state 00 while eavesdropper E_1 lying between V1 and P has entangled qubit pair (7, 8) also in Bell state 00.

2) At time t_0, V0 sends qubit 2 to P but E_0 intercepts it and sends his/her qubit 6 to P. Similarly at time t_1, V1 sends...
qubit 3 to \( P \) but \( E_1 \) intercepts it and sends his/her qubit 8 to \( P \). Simultaneously, \( E_1 \) sends qubit 7 to \( E_0 \).

3) \( P \) performs a BSM on qubits 6 and 8 and gets one of the Bell states, say 10. This measurement projects the qubits 5 and 7 into Bell state 10, only known to \( P \) at the moment. \( P \) immediately sends his/her measurement result to both \( V_0 \) and \( V_1 \) simultaneously.

4) \( V_0 \) and \( V_1 \) will receive the BSM result from \( P \) at times \( T_0 \) and \( T_1 \) as if no adversary happened. \( V_1 \) immediately transmits his qubit 4, time \( T_1 \) and BSM result to \( V_0 \) but \( E_0 \) intercepts, because the channel between them is not secure. \( E_0 \) performs BSM on qubits 5 and 7 and gets 10. Then, he/she applies unitary transformations on qubit 2 such that qubits 1 and 2 get entangled in the state 10 and sends it to \( V_0 \).

5) \( V_0 \) will perform BSM on qubits 1 and 2 and confirms that his/her result is consistent with that of \( P \).

6) Both \( V_0 \) and \( V_1 \) can verify the position of \( P \) by comparing the arrival time of response.

Because the measurements and timing of eavesdroppers are exactly the same as those of the honest prover, verifiers \( V_0 \) and \( V_1 \) cannot differentiate between the honest prover \( P \) at a certain position and eavesdroppers at different positions. Hence, eavesdroppers cheat the prover and verifiers without being detected.

### 4.4. QPV scheme-IV

Malani proposed another QPV scheme based on entanglement swapping [9]. This scheme is described as follows:

1) \( V_0 \) shares two entangled qubit pairs \((1, 2)\) and \((3, 4)\) with the prover \( P \) in one of the four Bell states, for instance, both in 00. Suppose he/she also shares an entangled qubit pair \((5, 6)\) with Bob in the Bell state 11. All this information is public.

2) \( V_0 \) performs a BSM on qubits 3 and 5 and gets one of the Bell states, say 01. This measurement projects the qubits 4 and 6 into 10, only known to \( V_0 \).

3) \( V_0 \) communicates with \( V_1 \) through a secure public channel between them and informs him/her about his BSM result, 01. Now \( V_1 \) also knows his/her qubit 6 is entangled with \( P \)'s qubit 4 in the Bell state 10.

4) Both \( V_0 \) and \( V_1 \) encode a 2-bit message on their qubits 1 and 6, respectively, through superdense coding [17], and send their encoded qubits to \( P \) simultaneously through public channels.

5) \( P \) retrieves the encoded 2-bit message by performing BSM on Bell pairs \((1, 2)\) and \((4, 6)\) and immediately sends messages to \( V_0 \) and \( V_1 \) through classical channels.

6) \( V_0 \) and \( V_1 \) can verify the position of \( P \) by comparing the arrival time of response.

Again, this scheme assumes that the channel between distant verifiers is secure, which is not a realistic scenario. In the other case, eavesdroppers can intercept and get BSM result of \( V_0 \). So, they will also be able to know that \( V_1 \) and \( P \) have an entangled qubit pair in state 10. Furthermore, eavesdroppers can intercept qubits sent from \( V_0 \) and \( V_1 \) and can find the encoded 2-bit message. The cheating strategy for this scheme is shown in figure 2 and is described here:

1) \( V_0 \) shares two entangled qubit pairs \((1, 2)\) and \((3, 4)\) with the prover \( P \) in one of the four Bell states, for instance, both in 00. Suppose he/she also shares an entangled qubit pair \((5, 6)\) with Bob in the Bell state 11. Moreover, suppose eavesdropper \( E_0 \) lying between \( V_0 \) and \( P \) possesses entangled qubit pair \((7, 8)\) in Bell state 00 while eavesdropper \( E_1 \) lying between \( V_1 \) and \( P \) has entangled qubit pair \((9, 10)\) in Bell state 00.

2) \( V_0 \) performs a BSM on qubits 3 and 5 and gets one of the Bell states, say 01. This measurement projects the qubits 4 and 6 into 10, only known to \( V_0 \).
3) $V_0$ communicates with $V_1$ through an insecure public channel and informs him about his BSM result, 01. Now, $V_1$ also knows his qubit 6 is entangled with $P$’s qubit 4 in the state $10$. Eavesdroppers intercept and also get this information.

4) Let $V_0$ encode a 2-bit message 10 on his qubit 1 and let $V_1$ encode a 2-bit message 11 on his qubit 6, respectively, through superdense coding, and send their encoded qubits to $P$ simultaneously through public channels. $E_0$ and $E_1$ intercept these qubits and send their qubits 7 and 9, respectively, to $P$.

5) $P$ performs BSM on Bell pairs (7, 2) and (9, 4) and immediately sends his BSM results 01 to $V_0$ and 10 to $V_1$ through classical channels. $E_0$ and $E_1$ intercept these results, perform BSM on their retained qubits (e.g. both 11), and they will know the 2-bit secret messages of $V_0$ (10) and $V_1$ (11). Although decoded message by $P$ will certainly be wrong, eavesdroppers can jam the signals of $P$ and send exact 2-bit messages to $V_0$ and $V_1$.

6) $V_0$ and $V_1$ will verify the position of $P$, as if no adversary has happened, by comparing the arrival time of response. Thus, measurement results and times of $V_0$ and $V_1$ are consistent as if no adversary has happened. Moreover, both $V_0$ and $V_1$ cannot detect the presence of adversaries in this scheme. Hence, eavesdroppers cheat the prover and verifiers without being detected.

5. Our QPV schemes

In this work, we propose QPV schemes under the more realistic and cryptographically standard assumptions. We assume that the positions of the honest prover and reference stations are secure from adversaries; enabling them to store and hide the quantum data and process. We also assume that the reference stations are trusted and known to each other. However, quantum/classical channels are not secure, neither between the prover and verifiers nor between different verifiers. Moreover, there is no bound on storage, computing, receiving, and transmitting powers of eavesdroppers. In short, eavesdroppers have full control of the environment except the prover’s position and reference stations. We also assume that all reference stations and the prover have fixed positions in Minkowski spacetime, where all verifiers have precise and synchronized clocks. Finally, we suppose that signals can be sent between prover and reference stations at the speed of light, while the time for information processing at the position of the honest prover and reference stations is negligible. For simplicity, we discuss our schemes for one honest prover $P$ and two verifiers $V_0$ and $V_1$ at distant reference stations $R_0$ and $R_1$ such that the prover is at a distance $d$ from both reference stations.

5.1. QPV scheme-A

This scheme is shown in figure 3 and its explicit procedure is as follows:

1) $V_0$ shares two entangled qubit pairs (2, 5) and (3, 7) with the prover $P$ in one of the four Bell states, for instance, both in 01. She also shares two entangled qubit pairs (1, 9) and (4, 12) with Bob in the Bell state 11. $V_1$ also shares two entangled qubit pairs (6, 10) and (8, 11) with the prover $P$ in one of the four Bell states, for instance, both in 01. All this information is public.

Figure 2. Cheating scheme for QPV scheme-IV.
Figure 3. Bell states written as $u_i u_j$ are public. The states $\{u_i u_j\}$ are known to $V_0$ only while $\{u_i u_j\}$ are known to $V_1$ only; $\{u_i u_j\}$ are known to both $P$ and $V_0$ while $\{u_i u_j\}$ are known to $P$ and $V_1$.

2) $V_0$ performs a Bell state measurement on qubits 1 and 2 and gets one of the Bell states, e.g. 10. This measurement projects the qubits 5 and 9 into Bell state 00, only known to $V_0$. Similarly, $V_1$ also performs BSM on qubits 11 and 12 and gets one of the Bell states, e.g. 00. This measurement projects the qubits 4 and 8 into Bell state 10, only known to $V_1$.

3) $V_0$ performs BSM on 3 and 4 and announces the result publically, say 11. At this point only $V_1$ knows that the BSM result of $P$ on 7 and 8 will be 00. Concurrently, $V_1$ performs BSM on 9 and 10 and announces the result publically, say 10. At this point only $V_0$ knows that the BSM result of $P$ on 5 and 6 will be 11.

4) At time $t = 0$, $V_0$ sends an encoded message to $P$ such that this message can only be decoded with secret 2-bits 11, only known to $V_0$ and $P$. Simultaneously, $V_1$ sends an encoded message to $P$ such that this message can only be decoded with secret 2-bits 00, only known to $V_1$ and $P$.

5) $P$ retrieves the encoded message with corresponding secret 2-bits, obtained by performing BSM on Bell pairs (5, 6) and (7, 8). He immediately sends messages to $V_0$ and $V_1$.

6) $V_0$ and $V_1$ can verify the position of $P$ by comparing the arrival time of response, $t = 2d/c$.

If verifiers verify the position of $P$ by performing this scheme $N$ times successively, then $P$ is identified and his position is authenticated. In this scheme, no secret information is sent publically without properly encoding. The encoded message can only be decoded by $P$ having secret 2-bits.

Figure 4. Bell states written as $u_i u_j$ are public. The states $\{u_i u_j\}$ are known to $V_0$ only, $\{u_i u_j\}$ are known to $V_1$ only, and $\{u_i u_j\}$ are known to $P$ only; $\{u_i u_j\}$ are known to both $P$ and $V_0$ and $\{u_i u_j\}$ are known to $P$ and $V_1$. However, $\{u_i u_j\}$ are unknown to everyone.

### 5.2. QPV scheme-B

This scheme is shown in figure 4 and follows:

1) $V_0$ possesses an entangled qubit pair (1, 2) in Bell state 11 and also shares an entangled qubit pair (3, 4), in Bell state 01, with the prover $P$. $V_1$ also possesses an entangled qubit pair (11, 12) in Bell state 11 and shares an entangled qubit pair (9, 10) in Bell state 01, with the prover $P$. The prover $P$ possesses two entangled qubit pairs (5, 6) and (7, 8) both in the Bell state 00, say. All this information is public.

2) $V_0$, $P$ and $V_1$ simultaneously perform BSM as follows: $V_0$ on qubits 2 and 3, $P$ on qubits 4 and 6, and 8 and 9, with $V_1$ on 10 and 12, respectively. Their BSM results will be known only to them at this stage, e.g. 01 to $V_0$, 11 and 01 to $P$, and 10 to $V_1$. Moreover, these measurements will project the qubits 1 and 5 into 00, and 7 and 11 into 01, as shown in figure 4. These results will be unknown to everyone.

3) $V_0$ and $V_1$ send their qubits 1 and 11 to $P$ simultaneously. $P$ performs BSM on pairs (1, 5) and (7, 11) and immediately sends corresponding BSM results 00 and 01 to $V_0$ and $V_1$, respectively.

4) $V_0$ and $V_1$ note round trip time and now they will be aware of corresponding $P$’s BSM results 11 and 01, respectively. Similarly, $P$ will be aware of corresponding BSM results of $V_0$ and $V_1$, i.e. 01 and 10.

5) $V_0$ sends an encoded message to $P$ such that this message can only be decoded with secret 2-bits 11, only known to $V_0$ and $P$. Simultaneously, $V_1$ sends an encoded message to $P$ such that this message can only be decoded with secret 2-bits 01, only known to $V_1$ and $P$.

6) Only $P$ can retrieve the encoded message by corresponding secret 2-bits. He again encodes the same message such
that only $V_0$ and $V_1$ can decode it with their secret 2-bits and immediately sends messages to $V_0$ and $V_1$. 
7) $V_0$ and $V_1$ can verify the position of $P$ by validating messages and comparing round trip time, $t = 2d/c$.

By using a single QPV scheme, verifiers can verify the position of $P$ twice, in steps 4 and 7. At either stage, if they get the wrong response from $P$, then they can detect eavesdroppers in the middle. If verifiers verify the position of $P$ by performing this scheme $N$ times successively, then $P$ is identified and his position is authenticated. In QPV schemes A and B, secret messages can be encoded on qubits by applying arbitrary rotations.

6. Key establishment in PBQC

If position of the prover $P$ is verified $N$ times successively, then each verifier will have established two different secret keys of length $2N$ with $P$ i.e.

$$K_V = \{v_1, v_2, ..., v_{2N}\} \quad (4)$$

and

$$K_P = \{p_1, p_2, ..., p_{2N}\} \quad (5)$$

where $v_i, p_i \in [0,1]$. In our QPV scheme A, both of the keys $K_V$ and $K_P$ will be known to corresponding verifiers, but the prover will know only one of these, $K_P$. However, in our QPV scheme B, both of the keys $K_V$ and $K_P$ will be known to the prover and corresponding verifiers. These keys can be used further for identification of the prover and authentication of the message transferred. Our position-based key establishment is similar to the one proposed by Ekert [18] based on shared entanglement states but is different in the sense that verifiers and provers perform BSM on entangled pairs instead of measurement on single entangled particle. Cabello also proposed a quantum key distribution scheme based on entanglement swapping where distant parties transfer entangled particles through public channels instead of pre-shared entangled states [19]. An eavesdropping attack on Cabello’s scheme and further modifications to attain security can be found elsewhere [20, 21].

7. Authentication in PBQC

Authentication is a procedure to verify that the received message comes from the valid entity and has not been altered. Generally, authentication can be achieved through following three mechanisms: message encryption (symmetric or asymmetric), message authentication code (MAC), or hash functions. Buhrman et al introduced the idea of position-based authentication, a message authentication code based on their position-verification scheme [8]. We show that our proposed QPV schemes can be used as message encryption authentication straightforward schemes.

In the following position-based authentication, we use a photon as a qubit. The horizontally polarized state of the photon is denoted by $|0\rangle$ while the vertically polarized state is denoted by $|1\rangle$. The scheme works as follows:

1) The prover $P$ chooses a large positive integer $z$, prepares a $2^N$ qubit state $|\psi_P\rangle = |0\rangle \otimes |V_0\rangle$ and generates a classical $2$-bit string $S = \{s_1, s_2, ..., s_{2N}\}$ where $s_i$ is any random integer. $P$ encodes string $S$ on $2$-N qubits and sends the state $|\psi_P\rangle$ to $V_0$:

$$|\psi_P\rangle = \bigotimes_{i=1}^{2N} R(s_i |\psi(0)\rangle \otimes |V_0\rangle \otimes |V_0\rangle \quad (6)$$

where $R(s_i |\psi)\rangle$ is the rotation operator with $\theta = \pi/4^z$. 
2) Verifier $V_0$ chooses a different large positive integer $z$ and generates a classical $2$-N bit string $T = \{t_1, t_2, ..., t_{2N}\}$, where $t_i$ is any random integer. $V_0$ encodes string $T$ on $|\psi_P\rangle$ and sends the state $|\psi_{ST}\rangle$ to $P$:

$$|\psi_{ST}\rangle = \bigotimes_{i=1}^{2N} R(t_i |\psi(0)\rangle \otimes |V_0\rangle \otimes |V_0\rangle \quad (7)$$

where $R(t_i |\psi)\rangle$ is the rotation operator with $\theta = \pi/4^z$.
3) $P$ applies rotation $R(-s_i |\psi)\rangle$ on the state $|\psi_{ST}\rangle$ and then encrypts message $M = \{m_1, m_2, ..., m_{2N}; m_i \in [0,1]\}$ with his $2$-N bit secret key $K_P$ by applying a further rotation $R([p_i \oplus m_i]/2)$ on the $i$th qubit, i.e.

$$|\psi_{T_M}\rangle = \bigotimes_{i=1}^{2N} R([p_i \oplus m_i]/2) R(t_i |\psi(0)\rangle \otimes |V_0\rangle \otimes |V_0\rangle \quad (8)$$

and sends the state $|\psi_{T_M}\rangle$ back to $V_0$. 
4) To identify the prover $P$, $V_0$ applies $R(-t_i |\psi)$ on the $i$th qubit and measures the state

$$|\psi_{TM}\rangle = \bigotimes_{i=1}^{2N} R([p_i \oplus m_i]/2) R(t_i |\psi(0)\rangle \otimes |V_0\rangle \otimes |V_0\rangle \quad (9)$$

in $|0\rangle$, $|1\rangle$ basis. He will get $p_i \oplus m_i$, where $m_i$ can only be retrieved by exact key $p_i$. 
5) $V_0$ executes XOR of $p_i \oplus m_i$ and $p_i$. He will get message $M = \{m_1, m_2, ..., m_{2N}\}$.

Simultaneously, all other verifiers can perform the same scheme with $P$. Furthermore, all verifiers can note the round trip time of response from $P$.

8. Security analysis

The security of our scheme relies on the fact that no secret information, which could help in spoofing, is sent directly through public channels but is encrypted properly such that only prover and verifiers can decrypt it. In short, proposed QPV schemes remain secure in general and under known entanglement-based attacks, even if eavesdroppers have an infinite amount of pre-shared entanglement and power of non-local quantum measurements in negligible time.

In our QPV scheme A, eavesdroppers cannot obtain any information about the secret measurement results of $V_0$, $V_1$ and $P$ through public announcements of $V_0$ and $V_1$. Furthermore, eavesdroppers cannot perform intercept/resend or teleportation-based attacks because no entangled qubit is transferred between the prover and verifiers. Hence, BSM results are known only to the honest prover and verifiers, and only the honest prover can respond to verifiers accurately. The verifiers
can easily detect adversaries if they try to intercept encrypted communication.

Again, in our QPV scheme B, eavesdroppers cannot get any information about secret BSM results of verifiers and the prover through public announcements of P or by intercepting qubits I and 11 sent by V0 and V1 to P over public channels. Suppose the eavesdropper between V0 and P possesses already entangled qubit pair (13,14), intercepts qubit 1, performs BSM on 1 and 13, and sends qubit 14 to P. In that case, V0 can easily detect eavesdroppers because announcements of P will not be consistent with the BSM results of V0 and P. When V0 sends encoded messages to P in step (5) of the scheme, surely P will decode these messages incorrectly. Similarly, P and V1 can detect eavesdropper E1 lying between them.

Finally, our position-based authentication scheme can be made secure by choosing arbitrarily large integer z. If z ≫ 1 (or θ ≪ 1), then the number of non-orthogonal states increases and it becomes impossible to differentiate them, i.e., distance between nearest neighbors \( \sqrt{1 - \left(\mu_z(\theta)\mu_z(\theta')\right)} \) approaches zero. Moreover, only one bit of classical information can be obtained from the single qubit [22], whereas 2-N bits are required to identify any randomly chosen \( s_j \) (or \( t_j \)) from 2-N bit string \( S \) (or \( T \)). Hence, the encoding applied in steps 1 and 2 acts as a quantum one-way function provided z ≫ 1, and only authorized users can extract secret information. Detailed discussions of quantum one-way function can be found elsewhere [23, 24]. Hence, position-based authentication presented in this article is secure against known attacks such as intercept/forward attacks, chosen plain text attacks, forward search attacks, and chosen ciphertext attacks.

9. Conclusion

In this article, we review already proposed QPV schemes based on pre-shared data between the prover and verifiers. QPV scheme I proposed by Kent seems secure but requires a pre-shared classical secret key between the prover and one of verifiers. Scheme II proposed by Buhrman et al is based on pre-shared entangled states between the prover and verifiers, but the authors showed that this scheme is secure only if eavesdroppers do not have any entangled data. We have shown that schemes III and IV proposed by Malani, also based on pre-shared entangled states between the prover and verifiers, are insecure if channels between distant verifiers are not secure.

We propose two different QPV schemes to show that theoretic information position-based quantum cryptography is possible even over untrusted networks if the honest prover pre-shares some entangled states with verifiers. Our schemes have numerous advantages over previously proposed schemes in this field. First, our proposed schemes are secure even over untrusted networks, whereas all previous schemes may be secure only if channels between distant verifiers are secure. Second, our schemes verify the position as well as serve as a protocol for position-based QKD, which can be used for authentication and communication between the prover and verifiers. However, previously proposed schemes cannot be used for secret communication. For example, in scheme IV, adversaries can spoof position verification as well as get the secret 2-bits of the verifiers. These bits cannot be reused for further communication. Third, in existing scheme IV, verifiers also use classical channels to communicate secret information with the prover in case of an N shared entangled pair between them [9]. In principle, eavesdroppers can always monitor classical channels without being detected by authorized users. However, our schemes require only quantum channels while sending secret information. Finally, our proposed QPV schemes can easily detect adversaries while previously proposed schemes can be spoofed by eavesdroppers without being detected.

We presented a formula that verifies position, establishes secret keys and authenticates the honest prover using a single scheme in position-based quantum cryptography. Our proposed position-based authentication scheme can be modified to a more robust authentication mechanism based on hash functions by using secret keys established in our QPV schemes.

Acknowledgments

I am grateful to R Malaney for introducing me to his work [9].

Appendix

In section 3, we write four Bell states compactly as

\[
|\psi_{uu}\rangle = \frac{\left|0\right\rangle|u_i\rangle + (-1)^{u}|1\rangle|1\oplus u_i\rangle}{\sqrt{2}} \tag{A.1}
\]

where \( u_i \), \( u_j \in \{0, 1\} \) and \( \oplus \) denotes addition with mod 2. The corresponding four Bell states \( \{0\rangle \) and \( \{1\rangle \) representation will be

\[
|\psi_{00}\rangle = \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} \tag{A.2}
\]

\[
|\psi_{01}\rangle = \frac{|0\rangle|1\rangle + |1\rangle|0\rangle}{\sqrt{2}} \tag{A.3}
\]

\[
|\psi_{10}\rangle = \frac{|0\rangle|0\rangle - |1\rangle|1\rangle}{\sqrt{2}} \tag{A.4}
\]

\[
|\psi_{11}\rangle = \frac{|0\rangle|1\rangle - |1\rangle|0\rangle}{\sqrt{2}} \tag{A.5}
\]

Suppose qubit pairs (1, 3) and (2, 4) are entangled in Bell states \( |\psi_{01}\rangle_{13} \) and \( |\psi_{00}\rangle_{24} \). Initially, these four particles will be in state

\[
|\psi_{01}\rangle_{13} \otimes |\psi_{00}\rangle_{24} = \frac{|01\rangle_{13} + |10\rangle_{13}}{\sqrt{2}} \otimes \frac{|00\rangle_{24} + |11\rangle_{24}}{\sqrt{2}} \tag{A.6}
\]
By simple algebraic tricks (adding and subtracting terms like $|i\rangle_1|j\rangle_2$ and $|j\rangle_1|i\rangle_2$), we will get

\begin{equation}
|\psi_0\rangle_{13} \otimes |\psi_0\rangle_{24} = \frac{1}{2}(|00\rangle_{12}|00\rangle_{24} + |01\rangle_{12}|11\rangle_{24} + |10\rangle_{12}|00\rangle_{24} + |11\rangle_{12}|11\rangle_{24}) \tag{A.7}
\end{equation}

\begin{equation}
|\psi_1\rangle_{13} \otimes |\psi_1\rangle_{24} = \frac{1}{2}(|00\rangle_{12}|11\rangle_{24} + |01\rangle_{12}|00\rangle_{24} + |10\rangle_{12}|00\rangle_{24} + |11\rangle_{12}|11\rangle_{24}) \tag{A.8}
\end{equation}

By performing Bell state measurement on particles 1 and 2, Alice can project particles 3 and 4 into one of the four possible Bell states: $|\psi_{00}\rangle$, $|\psi_{01}\rangle$, $|\psi_{10}\rangle$ or $|\psi_{11}\rangle$.

References

[1] Chandran N, Goyal V, Moriarty R and Ostrovsky R 2009 Advances in Cryptology—CRYPTO 2009 (Lecture Notes on Computer Science vol 5677) ed S Halevi (Berlin: Springer) pp 391–407
[2] Kent A P, Munro W J, Spiller T P and Beausoleil R G 2006 Tagging systems US Patent 7075438
[3] Kent A, Munro B and Spiller T 2011 Phys. Rev. A 84 042326
[4] Malaney R 2010 Phys. Rev. A 81 042319
[5] Malaney R 2010 GLOBECOM 2010: IEEE Global Telecommunications Conf. (Miami, FL, 6–10 Dec. 2010)
[6] Lau H K and Lo H K 2011 Phys. Rev. A 83 012322
[7] Kent A 2011 Phys. Rev. A 84 022335
[8] Buhman H et al 2011 Advances in Cryptology—CRYPTO 2011 (Lecture Notes on Computer Science vol 6841) ed P Rogaway (Berlin: Springer) pp 429–46
[9] Malaney R 2010 Location verification in quantum communications US Patent 0195597
[10] Vaidman L 2003 Phys. Rev. Lett. 90 010402
[11] Beigi S and Konig R 2011 New J. Phys. 13 093036
[12] Zukowski M, Zeilinger A, Horne M and Ekert A 1993 Phys. Rev. Lett. 71 4287
[13] Wootters W K and Zurek W H 1982 Nature 299 802
[14] Bennett C H and Brassard G 1984 Quantum Cryptography, Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India) pp 175–9
[15] Bennett C H, Brassard G, Crepeau C, Jozsa R, Peres A and Wootters W K 1993 Phys. Rev. Lett. 70 1895
[16] Braunstein S L, Mann A and Revzen M 1992 Phys. Rev. Lett. 68 3259
[17] Bennett C H and Wiesner S J 1992 Phys. Rev. Lett. 69 2881
[18] Ekert A K 1991 Phys. Rev. Lett. 67 661
[19] Cabello A 2000 Phys. Rev. A 61 052312
[20] Zhang Y S, Li C F and Guo G C 2001 Phys. Rev. A 63 036301
[21] Cabello A 2001 Phys. Rev. A 63 036302 (arXiv:quant-ph/0009051v3)
[22] Holevo A S 1977 Rep. Math. Phys. 12 273–8
[23] Buhrman H, Cleve R, Watrous J and de Wolf R 2001 Phys. Rev. Lett. 87 167902
[24] Gottesman D and Chuang I L 2001 Technical Report (arXiv:quant-ph/0105032)