Authentication Protocol Using Quantum Superposition States

Yoshito Kanamori[1], Seong-Moo Yoo[2], Don A. Gregory[3], and Frederick T. Sheldon[4]

(Corresponding author: Seong-Moo Yoo)

Department of Computer Information Systems, University of Alaska, Anchorage
Anchorage, AK 99508,USA[1]
Electrical and Computer Engineering Department[2]
Department of Physics[3]
University of Alabama in Huntsville, Huntsville, AL 35899, USA
Computational Sciences and Engineering Division, Oak Ridge National Laboratory,
Oak Ridge, TN 37831, USA[4]

Abstract

When it became known that quantum computers could break the RSA (named for its creators – Rivest, Shamir, and Adleman) encryption algorithm within a polynomial-time, quantum cryptography began to be actively studied. Other classical cryptographic algorithms are only secure when malicious users do not have sufficient computational power to break security within a practical amount of time. Recently, many quantum authentication protocols sharing quantum entangled particles between communicators have been proposed, providing unconditional security. An issue caused by sharing quantum entangled particles is that it may not be simple to apply these protocols to authenticate a specific user in a group of many users. An authentication protocol using quantum superposition states instead of quantum entangled particles is proposed. The random number shared between a sender and a receiver can be used for classical encryption after the authentication has succeeded. The proposed protocol can be implemented with the current technologies we introduce in this paper.

Keywords: Authentication, encryption, photon, polarization, quantum cryptography, superposition states

1 Introduction

One of the essential tasks to be done prior to communication is the authentication that guarantees that the origin of the message is genuine because, if a malicious user masquerades as a legitimate user, the key distribution schemes and encryption schemes can be easily compromised. In an authentication scheme, a sender registers secret information as his identification code in the receiver's database prior to the communication. Then, by showing the secret information to the receiver, the sender proves his legitimacy. Using an authentication protocol, a receiver can verify that the sender is a legitimate user before the connection is established.

A simple authentication scheme can be implemented by utilizing a symmetric key encryption algorithm. In such a scheme, a sender (Alice) and a receiver (Bob) share a secret key for the encryption algorithm prior to the communication. Alice sends Bob an encrypted message that includes a nonce (e.g., timestamp, a sequence number) and the identifier of the receiver. Since Bob believes that the key is shared only between Alice and himself, he can deduce that the sender is Alice [6]. When the number of users to be authenticated is large, a trusted third party may need to be introduced in the network because it is not practical for each user to keep secret keys for each one of a large number of users.

A significant problem is that the security of classical authentication protocols, in general, relies on the computational complexity of solving mathematical problems utilized in the cryptographic scheme. In other words, these algorithms are only secure when malicious users do not have enough computational power to break security within a practical amount of time.

Since it became known that a quantum computer could break the RSA encryption algorithm within a polynomial-time [17], quantum cryptography has been actively studied to circumvent the above problem in classical cryptography. The difference between quantum cryptography and classical cryptography is the physical resource for data transmission. Quantum cryptography uses particles, instead of electrical signals used in classical computers, and utilizes quantum mechanical properties such as the no-cloning theorem and quantum entangled states.

The no-cloning theorem says that replication of an ar-

bitrary quantum state is not possible [14, 19]. A quantum entangled state is a correlated state between two particles such that the result of a measurement on one particle affects the state of the other particle that is physically separated from the measured particle [5]. In general, photons are used as the media. For example, the BB84 protocol [4] (which is the most famous and thoroughly researched quantum key distribution (QKD) protocol that has been implemented in a practical application [9]), uses polarized photons. Alice sends polarized photons, referenced to one of two different orthogonal base sets (i.e., {horizontal, vertical} or {+45, −45}), and Bob observes the received photon, randomly choosing one of the two bases. After a certain amount of data is transmitted, Alice and Bob determine which data bits should be discarded by exchanging information about the bases they used for polarizations and measurements using a classical channel. They keep the rest of the data bits after sifting as the key for cryptography.

Although the QKD scheme provides unbreakable security, it still requires an authentication prior to the communication [18]. Thus, many quantum authentication protocols have been proposed recently. In most of these protocols, quantum entangled states are shared prior to the communication, as will be shown in the next section. An issue caused by sharing quantum-entangled particles is that it may not be easy to apply these protocols to authenticate a specific user in a group of many users, which is the most practical use for authentication protocols. If the entangled particles must be shared prior to the communication, each party must share the same number of entangled particles as the other parties. When the number of parties is increased to hundreds, thousands or more, it is no longer easy for the authenticator to maintain such a large number of entangled particles.

In this paper, a two-party authentication protocol that utilizes quantum superposition states instead of sharing quantum entangled states is proposed. The random number shared between a sender and a receiver can be used for classical encryption after the authentication has succeeded. Therefore, our authentication protocols can perform both a user authentication and a key distribution during the same session. It will be also shown that these superposition states can be realized by current technologies. A multiple-party authentication protocol (not mentioned in this paper) can be made as an extension of two-party protocol for practical use.

This paper is organized as follows. Previously developed quantum authentication protocols are introduced in the next section. A proposed encryption scheme is introduced in Section 3, and a two-party authentication protocol is proposed in Section 4. Finally, conclusions are presented in Section 5.

2 Existing Quantum Authentication Protocol

Recently, many quantum authentication protocols have been proposed and a formal definition of quantum authentication has been introduced [2]. Some protocols use classical cryptography with QKD. For instance, Dušek [8] proposed a secure quantum identification scheme where the BB84 QKD is used to share an identification sequence (IS) triad as common secret information. After Alice and Bob share these secret codes, they use a classical channel. First, Alice sends the first IS of the triad to Bob and he verifies it. Second, Bob sends the second IS of the triad to Alice and she verifies it. Finally, Alice repeats the first step and Bob verifies that the sender is Alice. In this protocol, an additional authentication is required because the BB84 needs an authentication before the parties start communication.

Kuhn [12] proposed an authentication scheme that is a combination of QKD and classical cryptography. This scheme assumes that a trusted server shares a secret key with Alice and Bob separately (i.e., the trusted server has two secret keys) and that authentication between each party and the server is made by a classical authentication protocol. First, Alice sends a request to the server. Then, the trusted server sends a stream of authentication bits that is one half of a pair of entangled photons and the classically encrypted information in order to measure the bits without error. To authenticate her identity to Bob, Alice sends a portion of the authentication bits to Bob. The rest of the authentication bits can be used as a session key. The advantage of this scheme is that the trusted server does not know the session keys. However, since the protocol relies on classical cryptography, it is a conditionally secure protocol.

Most of the other proposed authentication schemes [1, 7, 10, 13, 20, 21, 22] utilize quantum-entangled states. For example, Curty [7] proposes an authentication scheme sharing one-qubit key between the communication partners. Initially, Alice and Bob share a two-qubit maximally entangled state: $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB})$. Each owns one half of the entangled qubits. When Alice needs to send a one-bit message $|\psi\rangle$, she performs a unitary operation I or U_ε on $|\psi\rangle$ depending on her shared key qubit. Then Alice sends it to Bob. Bob also operates with I or $U_\varepsilon^\dagger$ on the received qubit depending on his shared key qubit. Then, Bob decodes the message. If he received a certified message, he is confident about the authenticity of the message and the sender.

Zeng [22] uses a trusted center to help the legitimate users obtain the sharing message. The center generates the same two entangled pairs and sends one half of each of the entangled pairs to Alice and to Bob, respectively. The center keeps the rest of each entangled pair. Similar to BB84, Alice and Bob measure their particles with a randomly chosen base (horizontal-vertical or diagonally polarized). Then, only Alice and Bob exchange infor-
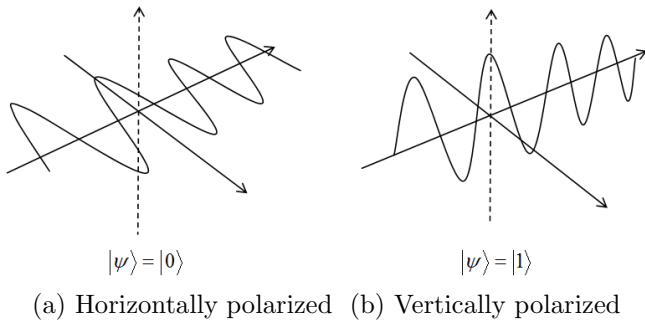
$|\psi\rangle = |0\rangle$ $|\psi\rangle = |1\rangle$

(a) Horizontally polarized (b) Vertically polarized

Figure 1: Horizontal-vertical polarization base

(a) Horizontally polarized   (b) Rotation angle θ

Figure 2: Randomly chosen angle used as a secret key

mation about which base they used for measurements in order to share a session key so that the trusted center does not know the session keys. In this protocol, both authentication and QKD are implemented. However, the trusted center has to set up a quantum channel between Alice and the center, and between Bob and the center, prior to the communication.

3 Quantum Commutative Encryption

In this section, the proposed encryption scheme used in the proposed authentication protocol is introduced in detail.

3.1 Encoding by Polarization of Photons

Only a horizontal-vertical polarization base for encoding and measuring a sequence of polarized photons (Figure 1) is used in this scheme. Here, "polarized photon" means a very short pulse of polarized light, each pulse containing a single photon. The horizontally polarized photon represents zero in a binary representation. The vertically polarized photon represents one. The states of a horizontally and vertically polarized photon can be represented as vectors: $|0\rangle = (\ 1\quad 0\ )^T$ and $|1\rangle = (\ 0\quad 1\ )^T$, respectively. In our protocol, all transmitted polarized photons are encrypted before the transmission, as shown in the next section.

3.2 Encryption by Rotation of Polarized Photon

In order to prevent malicious parties from reading and copying the transmitted photon, the sender makes each polarized photon a superposition of a horizontally polarized state and a vertically polarized state by rotating its polarization by a certain angle (Figure 2). A sender and a receiver share a set of randomly chosen angles prior to communicating.

In our protocols, we define the shared set of angles (a different angle for each bit) as a secret key $K = \{\theta_i : 0 \leq \theta_i < \pi, i = 1, 2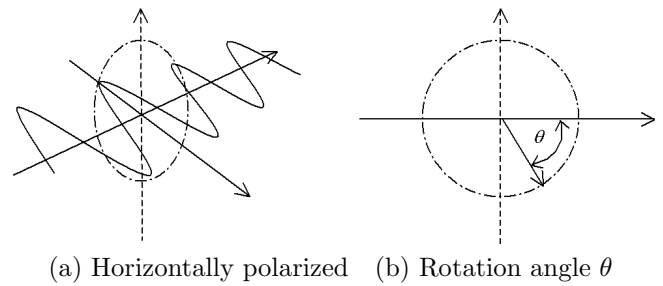, 3, \ldots, n\}$ for an n-bit message, where the subscript indicates the position in the message where the encryption with the angle θ_i is applied. We also define the rotation operation as encryption (i.e., a process of disguising to hide its original polarization). Let $E_K[M]$ be an encryption of data M with a secret key K. Then, in order to read the disguised photons correctly, the receiver must rotate the received photon by the angle θ_i in the opposite direction of what the sender rotated. We define this operation as decryption. Let $D_K[M]$ be a decryption of data M with the secret key K. These operations can be represented mathematically as shown below.

In the following discussion, without losing generality, we can assume that a message M is a single photon encoded as $M : |\psi_0\rangle = |0\rangle$ for simplicity. By using the Jones matrix representation, the rotation operation can be represented by the following matrix:

$$R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta. \end{pmatrix}$$

.

A sender encrypts the data qubit $|\psi_0\rangle$ with θ_A. (θ_A is randomly chosen and is shared between a sender and a receiver prior to the communication.)

$$
\begin{aligned}
E_K[M] &= R(\theta_A) \cdot |0\rangle \\
&= \begin{pmatrix} \cos\theta_A & \sin\theta_A \\ -\sin\theta_A & \cos\theta_A \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} \cos\theta_A \\ -\sin\theta_A \end{pmatrix} = \cos\theta_A \cdot |0\rangle - \sin\theta_A \cdot |1\rangle \\
&= |\psi_1\rangle .
\end{aligned}
$$

The sender sends the superposition states $|\psi_1\rangle$ to a receiver.

Before the receiver measures the received photon, he needs to rotate the received photon by θ_A in the opposite direction of the sender's rotation. This decryption can be represented as follows:
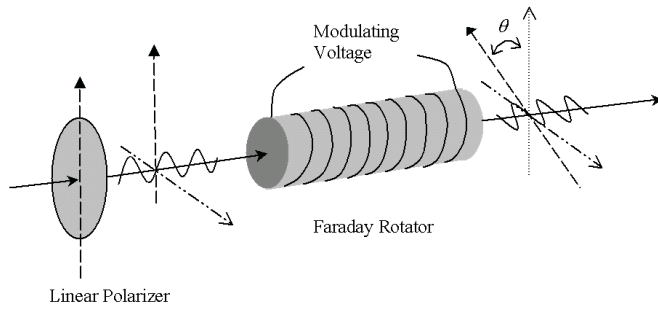
Figure 3: An example of an experimental realization

$$
\begin{aligned}
& R(-\theta_A) \cdot |\psi_1\rangle \\
&= \begin{pmatrix} \cos(-\theta_A) & \sin(-\theta_A) \\ -\sin(-\theta_A) & \cos(-\theta_A) \end{pmatrix} \cdot \begin{pmatrix} \cos\theta_A \\ -\sin\theta_A \end{pmatrix} \\
&= \begin{pmatrix} \cos^2\theta_A + \sin^2\theta_A \\ \sin\theta_A \cdot \cos\theta_A - \cos\theta_A \cdot \sin\theta_A \end{pmatrix} \\
&= \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle.
\end{aligned}
$$

The main advantage of this encryption/decryption scheme is that a receiver does not have to decrypt a cipher text in the exact reverse order as encrypted with different secret keys. For instance, even if Alice encrypts a message with K_1 and then encrypts it with K_2, Bob can decrypt the cipher text with K_1 and then decrypt it with K_2.

Also, an exclusive-OR (XOR) operation can be performed on the plaintext in the encrypted state without decrypting it. Rotating the encrypted photon by 90 degree changes the plaintext, logic-one to logic-zero or logic-zero to logic-one [11].

3.3 An Example of Experimental Realization and Measurement of Photons

The photon is linearly polarized by a polarizing apparatus called linear polarizer and the direction can be determined by the orientation of the polarizer. In order to rotate the polarized photon, the photon is passed through a Faraday effect modulator (i.e., Faraday rotator [15]). The rotation angle is controlled by the strength of the magnetic field parallel to the light beam as shown in Figure 3.

The output polarization from the Faraday rotator is rotated by the angle θ. When the input state is $|\psi\rangle = |0\rangle$, the state of the output photon is represented as $R(\theta) \cdot |0\rangle = \cos\theta \cdot |0\rangle - \sin\theta \cdot |1\rangle$. Since this is a superposition state of: $|0\rangle$ and $|1\rangle$, when we measure the state with a horizontal-vertical polarization base, either $|0\rangle$ or $|1\rangle$ will be obtained with a certain probability. In quantum mechanics, the coefficients of the vectors are called probability amplitudes and the square of the probability amplitude indicates the probability of finding the photon in that state. For instance, when the angle is 30 degrees, the state of the photon is represented by $|\psi\rangle = \cos 30 \cdot |0\rangle - \sin 30 \cdot |1\rangle = \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle$.

Therefore, if we measure this photon with a horizontal-vertical polarization base, we will obtain $|0\rangle$ with the probability $(\frac{\sqrt{3}}{2})^2 = \frac{3}{4}$ and $|1\rangle$ with the probability $(-\frac{1}{2})^2 = \frac{1}{4}$. In other words, the measurement result depends on the angle θ. Likewise, when the angle is zero, we will always obtain $|0\rangle$ in the above example, theoretically. When the angle is 90 degrees, we will find the photon to be in the state $|1\rangle$ with the probability 1.

3.4 Security Analysis of The Encryption by Rotation of Polarized Photon

The security of this encryption relies on the no-cloning theorem, a quantum mechanical property that says that no one can make a copy of any unknown non-orthogonal state. Hence, by transmitting data as a superposition of state, no one can make a copy of the transmitted data without errors. Also, when a superposition state is measured (with a horizontal-vertical base in this scheme), the result will be one of two orthogonal states (i.e., $|0\rangle$, or $|1\rangle$) and no information regarding the rotation angle is left. Thus, intercept/resend attack and beam-splitting attack are not possible against the proposed authentication protocol as shown below.

3.4.1 Intercept/Resend Attack

Let us assume that an eavesdropper (Eve) intercepts the transmitted photon from Alice. After a measurement of the photon, Eve resends it to Bob. This attack cannot break our authentication scheme because she cannot obtain the original state without knowing the rotation angle. For example, let us assume Alice transmits a quantum state $|\psi\rangle$ that is $|1\rangle$ with rotation by $\theta = 45$ degrees (i.e., represented as $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$). If Eve intercepted the state $|\psi\rangle$, which was unknown to Eve, and measured it in a horizontal-vertical polarization base, Eve will get zero or one with a probability of 50%. In our protocol, the angles θ_i for each bit are chosen randomly. Therefore, Eve will get zero or one randomly on the average when she measures the sequence of polarized photons. Since half of Eve's measured data may be correct because $|\psi\rangle$ is $|0\rangle$ or $|1\rangle$ anyway, if Eve resends the measured results to Bob, the transmission error rate (incorrect data/all data) will rise to 50 %. Thus, we can easily detect the existence of an eavesdropper.

3.4.2 Beam-splitting Attack

It is not easy to build a single photon source with current technologies. As a matter of fact, in general, the light pulse called a single photon in the laboratory is not a pure single-photon state (i.e., zero, one or multiple photons in the same state.) Therefore, the following attack is possible against BB84 [3].

First, Eve collects a fraction of the multiple photons by putting a beam-splitter in the path between Alice and Bob. Then, Eve measures the collected photons without being detected by Bob. She can read the transmitted data from Alice with an error rate of 50%. Moreover, if Eve can store the collected photons until Alice and Bob disclose their measurement bases, Eve can read all the collected photons without errors. Similar to the passive attack in classical cryptography, it is not easy to detect this attack if the loss in the intensity of the transmitted light pulse is very small.

This attack is not possible against our authentication protocol. Although Eve can collect a fraction of the transmitted photons without being detected by Bob, it is still very difficult to find the secret angle from a couple of transmitted photons because the rotation angles are chosen randomly and will never be disclosed in public.

3.4.3 Other Possible Attack

If Eve can make many copies of the transmitted photon, she can try to find the secret angle by measuring each copied photon with a measurement base rotated by a different angle. However, the no-cloning theorem forbids copying unknown states without errors. Instead, Eve can intercept a large number of transmitted photons without being detected if she collects a small fraction of transmitted photons at a time and spends a long period of time so that the transmission error rate caused by the interceptions does not increase noticeably. Then, she can utilize a statistic with a large amount of the measurement results with the collected photons. By using this method, the rotation angle can be found when the plaintext is known to Eve. Thus, no information that can be known to Eve should not be encrypted with QCE when the encryption key is reused. On the contrary, when the plaintext is an unknown random bit sequence, there is no chance that the encryption key will be uncovered by Eve [11].

4 Two-Party Authentication Protocol

4.1 Protocol Description

A classical channel is used only to request an authentication before the authentication process starts. The authentication scheme itself does not require a classical channel.

Let us assume that Bob needs to verify the origin of the message from Alice and that Alice and Bob share a secret key $K = \{\theta_i : 0 \leq \theta_i < \pi, i = 1, 2, 3, \ldots, n\}$ prior to the communication. Figure 4 shows the two-party authentication protocol.

The numbers in Figure 4 correspond to each step in the protocol described below.

1) After Bob's authentication request, Alice generates an n-bit random number R_A and encodes it into n photons. $|\psi_{R_A}\rangle = |\psi_{R_A,1}\rangle \otimes |\psi_{R_A,2}\rangle \otimes \ldots \otimes |\psi_{R_A,n}\rangle$,
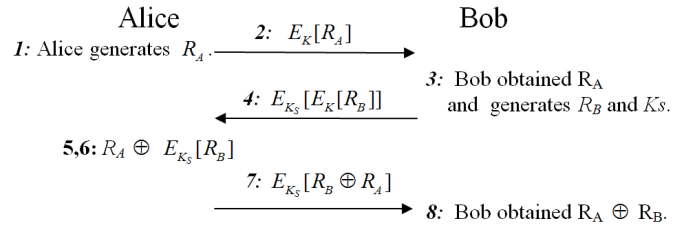

Figure 4: Two-party authentication protocol

where $|\psi_{R_A,i}\rangle$ is either $|0\rangle$ or $|1\rangle$ and the symbol '$\otimes$' represents a tensor product. The subscript 'R_A' indicates the random bit generated by Alice. The second subscript (i.e., 'i') shows the position of the bit in a message (i.e., R_A). Alice encrypts $|\psi_{R_A}\rangle$ with K. The resulting state can be written as

$$E_K[R_A] = R(\theta_1) \cdot |\psi_{R_A,1}\rangle \otimes R(\theta_2) \cdot |\psi_{R_A,2}\rangle \otimes$$
$$\ldots \otimes R(\theta_n) \cdot |\psi_{R_A,n}\rangle.$$

2) Alice sends $E_K[R_A]$ to Bob.

3) Bob decrypts $E_K[R_A]$ and measures $|\psi_{R_A}\rangle$, thus obtaining R_A from Alice. Bob generates an n-bit random number R_B and a session key $K_S = \{\theta'_i : 0 \leq \theta'_i < \pi, i = 1, 2, 3, \ldots, n\}$. He encrypts R_B with both K and K_S.

$$E_{K_S}[E_K[R_B]]$$
$$= R(\theta'_1) \cdot R(\theta_1) \cdot |\psi_{R_B,1}\rangle \otimes$$
$$R(\theta'_2) \cdot R(\theta_2) \cdot |\psi_{R_B,2}\rangle \otimes$$
$$\ldots \otimes R(\theta'_n) \cdot R(\theta_n) \cdot |\psi_{R_B,n}\rangle.$$

The subscript 'R_B' indicates the random bit generated by Bob. The second subscript (i.e., 'i') shows the position of the bit in a message (i.e., R_B).

4) He sends $E_{K_S}[E_K[R_B]]$ to Alice.

5) Alice decrypts $E_{K_S}[E_K[R_B]]$ with the key K.

$$D_K[E_{K_S}[E_K[R_B]]]$$
$$= R(-\theta_1) \cdot R(\theta'_1) \cdot R(\theta_1) \cdot |\psi_{R_B,1}\rangle \otimes$$
$$R(-\theta_2) \cdot R(\theta'_2) \cdot R(\theta_2) \cdot |\psi_{R_B,2}\rangle \otimes$$
$$\ldots \otimes R(-\theta_n) \cdot R(\theta'_n) \cdot R(\theta_n) \cdot |\psi_{R_B,n}\rangle$$
$$= R(\theta'_1) \cdot |\psi_{R_B,1}\rangle \otimes R(\theta'_2) \cdot |\psi_{R_B,2}\rangle \otimes$$
$$\ldots \otimes R(\theta'_n) \cdot |\psi_{R_B,n}\rangle$$
$$= E_{K_S}[R_B].$$

6) By using the technique introduced in Section 3.2, Alice performs an exclusive-OR (XOR) operation be-

tween R_A and $E_{K_S}[R_B]$ without decrypting it.

$$
\begin{aligned}
&R_A \oplus E_{K_S}[R_B] \\
&= R(\phi_1) \cdot R(\theta'_1) \cdot |\psi_{R_B,1}\rangle \otimes \\
&\quad\quad R(\phi_2) \cdot R(\theta'_2) \cdot |\psi_{R_B,2}\rangle \otimes \\
&\quad\quad\quad\quad ... \otimes R(\phi_n) \cdot R(\theta'_n) \cdot |\psi_{R_B,n}\rangle \\
&= R(\theta'_1) \cdot |\psi_{R_A \oplus R_B,1}\rangle \otimes R(\theta'_2) \cdot |\psi_{R_A \oplus R_B,2}\rangle \otimes \\
&\quad\quad\quad\quad ... \otimes R(\theta'_n) \cdot |\psi_{R_A \oplus R_B,n}\rangle \\
&= E_{K_S}[R_A \oplus R_B],
\end{aligned}
$$

where $\phi_i = \{0 \text{ for } R_{A,i} = 0, \ \frac{\pi}{2} \text{ for } R_{A,i} = 1\}$, where the subscript (i.e., 'i') shows the position of the bit in a message (i.e., R_A.) The symbol '$\oplus$' indicates a bit-wise XOR operation.

7) Alice sends $E_{K_S}[R_A \oplus R_B]$ to Bob.

8) Bob decrypts $E_{K_S}[R_A \oplus R_B]$ with K_S.

$$
\begin{aligned}
&D_{K_S}[E_{K_S}[R_A \oplus R_B]] \\
&= R(-\theta'_1) \cdot R(\theta'_1) \cdot |\psi_{R_A \oplus R_B,1}\rangle \otimes \\
&\quad\quad R(-\theta'_2) \cdot R(\theta'_2) \cdot |\psi_{R_A \oplus R_B,2}\rangle \otimes \\
&\quad\quad\quad\quad ... \otimes R(-\theta'_n) \cdot R(\theta'_n) \cdot |\psi_{R_A \oplus R_B,n}\rangle \\
&= |\psi_{R_A \oplus R_B,1}\rangle \otimes |\psi_{R_A \oplus R_B,2}\rangle \otimes ... \otimes |\psi_{R_A \oplus R_B,n}\rangle \\
&= |\psi_{R_A \oplus R_B}\rangle .
\end{aligned}
$$

The result of Bob's measurement on $|\psi_{R_A \oplus R_B}\rangle$ is supposed to be the sequence of the classical bit $R_A \oplus R_B$. Bob verifies the resulting sequence by performing an XOR operation between the resulting classical bit sequence and R_A. If the result of the XORing is R_B, the authentication succeeded. Otherwise, he aborts the session. Also, after this session, Alice and Bob share a random number, R_A, that can be used as a session key for other secure communication.

4.2 Security of the Two-Party Authentication Protocol

In order to design a secure protocol utilizing the Quantum Commutative Encryption (QCE), two critical conditions must be always satisfied as introduced in section 3.4.3: (i) No malicious user knows the plaintext, (ii) The states $|0\rangle$ and $|1\rangle$ appear randomly at each bit in the plaintext.

In the proposed protocol, these two conditions (i) and (ii) are clearly satisfied. Since the plaintexts in this protocol are random numbers: $R_A, R_B, R_A \oplus R_B$, data bits $|0\rangle$ and $|1\rangle$ appear randomly in the plaintexts. Also, since these numbers were generated during the session and a new session requires new random numbers, malicious users cannot know these plaintexts.

Since it is assumed that the shared key K is distributed prior to the authentication, if the random number R_A is also shared, the authentication is completed in step 3 because only Alice and Bob know the shared key. However, it violates the condition (ii). If Alice sends $E_K[R_A]$ repeatedly, the replay attack is possible because Eve can re-generate the same state as $E_K[R_A]$ after she has collected a large number of intercepted photons though she cannot exactly know what K and R_A are. Thus, R_A should be used only for the session as a plaintext and the protocol requires steps 3 through 8.

If Eve intercepts $E_{K_S}[E_K[R_B]]$ in step 4 and resends her photons with arbitrary states to Alice, Alice has to blindly decrypt the photon inserted by Eve. However, since the decrypted bits are also XORed with a random number R_A, whatever Eve encoded into her photons and sent to Alice, the plaintext in the transmitted photons from Alice in Step 7 is still a random number. As a result, Eve cannot find the encryption key even if she can collect an unlimited number of the photons from Alice during Steps 4 through 7.

Also, Eve's intercept/resend attack between Steps 2 and 4 is useless. After Step 2, Eve may intercept photons from Alice and send her photons to Bob, instead. However, regardlessly what Eve resends to Bob, $E_{K_S}[E_K[R_B]]$ will not be changed. Since Bob will blindly decrypt the received photons with K, the resulting photons are in superposition states and Bob's measurement results in generating a random number that Eve cannot predict and will never know. As a result, the authentication will fail in Step 8.

While the shared key K is used to authenticate a user's identity, the session key, K_S, also has a vital role. If the data is not encrypted with K_S (i.e., $E_{K_S}[E_K[R_B]]$ becomes $E_K[R_B]$.), the transmitted polarized photon from Alice in Step 7 will be in one of the orthogonal states. Consequently, Eve can read $R_A \oplus R_B$ without any problem. Thus, the transmitted photons need to be encrypted with K_S.

Note that the encryption scheme used in this protocol can not be replaced with the one-time pad encryption scheme [16]. Apparently, if the one-time pad is used, the replay attack is possible. Since Eve can make a copy of $E_K[R_A]$ (i.e., $K \oplus R_A$) in Step 2 and use it in Steps 5 and 6, Eve can impersonate Alice. In the proposed authentication protocol, it is not physically possible for Eve to make a copy of $E_K[R_A]$ because of the No-cloning theorem. If Eve tries to read $E_K[R_A]$, she gets a random sequence of bits (as the result of the measurement), which is useless for the Steps 5 and 6. Even if Eve can keep the state $E_K[R_A]$ and resend it later, she has to generate $E_{K_S}[R_A \oplus R_B]$ for Step 7 in order to be authenticated as Alice. It is not possible for Eve to do so without knowing both K_S and R_A. Thus, the replay attack is not possible against the proposed protocol.

Needless to say, if this protocol uses only one encryption key (i.e., only shared key), the scheme itself becomes much simpler, as shown in Figure 5. Bob generates a random number R and encrypts it with a key, K. Then, Bob sends $E_K[R]$ to Alice. Alice decrypts it and adds one to

Alice $\xleftarrow{\quad E_K[R] \quad}$ Bob
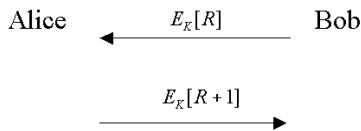
$\xrightarrow{\quad E_K[R+1] \quad}$

Figure 5: Simplified authentication protocol with QCE

the received random number R. Then, she encrypts it and sends $E_K[R+1]$ to Bob. Bob decrypts it and verifies the result.

Although this is simpler than the one introduced earlier, Eve has a chance to find the encryption key because this scheme violates the condition (i). Eve can resend all $|0\rangle$s instead of $E_K[R]$ and Alice blindly decrypts with K and sends them to Bob. Eve can intercept and measure all corresponding photons to identify the key (i.e. rotation angles) if given sufficient time to collect the intercepted photons.

5 Conclusion

We have proposed a two-party authentication protocol for a simple authentication case (our multi-party authentication protocol will be discussed in a future paper). To hide transmitted data from unauthorized users, this protocol uses quantum superpositioned states instead of quantum entangled states (similar to other quantum authentication protocols). Remember, to authenticate a specific user (the most common use of authentication protocols) within a group of many using quantum entangled states is a difficult problem. Our protocol works well using only one quantum channel within the protocol under the assumption that both parties *already* share a secret key (K). After the authentication has succeeded, the random number shared between a sender and a receiver (i.e., R_A) can be used as a session key for classical encryption. Furthermore, we showed that the superposition states can be realized using current technologies (e.g., linear polarizers and Faraday rotators).

References

[1] H. N. Barnum, "Quantum secure identification using entanglement and catalysis," *quant-ph/9910072*, 1999.

[2] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, "Authentication of Quantum Messages," *Proceeding 43rd Annual IEEE Symposium on the Foundations of Computer Science(FOCS '02)*, pp. 449-458, IEEE Press, 2002.

[3] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, no. 1, pp. 3-28, 1992.

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," *Proceeding IEEE Intenational Conference on Computers, Systems and Signal Processing*, pp. 175-179, Bangalore, India, 1984.

[5] D. Bouwmeester, A. Ekert, and A. Zeilinger, *The Physics of Quantum Information*, Springer, New York, 2000.

[6] J. Clark and J. Jacob, *A Survey of Authentication Protocol Literature: Version 1.0*, Nov. 1997. (http://www users.cs.york.ac.uk/{˜}jac/papers/drareview.ps.gz)

[7] M. Curty and D. J. Santos, "Quantum authentication of classical messages," *Physical Review A*, vol. 64, 1999.

[8] M. Dušek, O. Haderka, M. Hendrych, and R. Myška, "Quantum identification system," *Physical Review A*, vol. 60, pp. 149-156, 1999.

[9] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Applied Physics Letters*, vol. 84, no. 19, pp. 3762, 2004.

[10] J. G. Jensen and R. Schack, "Quantum authentication and key distribution using catalysis," *quant-ph/0003104*, 2000.

[11] Y. Kanamori, S. M. Yoo, and F. Sheldon, "Bank transfer over quantum channel with digital checks," *IEEE Global Telecommunications Conference*, San Francisco, CA, 2006.

[12] D. R. Kuhn, "A hybrid authentication protocol using quantum entanglement and symmetric cryptography," *quant-ph/0301150*, 2003.

[13] R. A. C. Medeiros, F. M. D. Assis, B. L. Jior, and A. F. Lima, "Quantum authentication scheme based on algebraic coding," *quant-ph/0307095*, 2003.

[14] M. A. Nielsen and I. L. Chuang, *Quantum Computation And Quantum Information*, Cambridge University Press, Cambridge, 2000.

[15] B. E. A. Saleh and M. C. Teich, *Fundamentals of Photonics*, John Wiley, New York, 1991.

[16] B. Schneier, *Applied Cryptography*, John Wiley, New York, 1996.

[17] P. W. Shor, "Algorithm for quantum computation: discrete logarithm and factoring," *Proceeding 35th IEEE Annual Symposium on Foundations of Computer Science*, pp. 124-134, Santa Fe, NM, Nov., 1994.

[18] K. Svozil, "Feasibility of the interlock protocol against man-in-the-middle attacks on quantum cryptography," *International Journal of Quantum Information*, vol. 3, no. 4, pp. 649-654, 2005.

[19] W. K. Wootters and W. H. Zurek, "A single quantum cannot cloned," *Nature*, vol. 299, pp. 802-803, 1982.

[20] G. Zeng, G. Guo, "Quantum authentication protocol," *quant-ph/0001046*, 2000.

[21] Y. Zhang, C. Li, and G. Guo, "Quantum authentication using entangled state," *quant-ph/0008044*, 2000.

[22] G. Zeng and W. Zhang, "Identity verification in quantum key distribution," *Physical Review A*, vol. 61, 022303, 2000.

Yoshito Kanamori is an assistant professor in the Department of Computer Information Systems at the University of Alaska, Anchorage. His research interests include computer network security, quantum information processing, and optics. He received his Ph. D and M. Sc. degrees at the University of Alabama in Huntsville in 2006 and 2002 respectively. He is a member of the IEEE.

Seong-Moo Yoo received the B. S. degree in economics from Seoul National University, Seoul, Korea, and the M. S. and Ph. D. degree in computer science from the University of Texas at Arlington in 1989 and 1995, respectively. Since September 2001, he is an associate professor in Electrical and Computer Engineering Department of the University of Alabama in Huntsville, Huntsville, Alabama, U. S. A. From September 1996 to August 2001, he was an assistant professor in Computer Science Department of Columbus State University in Columbus, Georgia, U. S. A. Dr. Yoo is the conference chair of ACM Southeast Conference 2004, April, 2004, Huntsville, Alabama, U. S. A. He was the co-program chair of ISCA 16th International Conference on Parallel and Distributed Computing Systems (PDCS-2003), August 2003, Reno, Nevada, U. S. A. Dr. Yoo's research interests include wireless networks, parallel computer architecture, and computer network security. Dr. Yoo is a senior member of IEEE and a member of ACM.

Don Gregory is currently Professor of Physics at the University of Alabama in Huntsville. He also holds appointments in the Optical Science and Engineering and the Materials Science Programs. Previously, he was a Supervisory Research Physicist and Chief of the Photonics and Laser Sciences Branch of the US Army Missile Command, Redstone Arsenal, Alabama where he managed scientific research and engineering programs in fundamental physics, optics, and laser science. Prof. Gregory has more than 120 refereed publications in fields ranging from fundamental optical properties of materials to optical pattern recognition. He was named Outstanding Teacher of the Year at the University of Alabama in Huntsville in 2005 and has graduated 19 MS students (thesis) and 18 Ph. D.'s since joining UAH in 1992.

Frederick T. Sheldon has over 24 years of experience in the field of computer science and software engineering. He currently is a senior research staff scientist at ORNL. Formerly, he was assistant professor at Washington State University, UC at Colorado Springs and research staff at DaimlerChrysler, Lockheed Martin, Raytheon and a visiting researcher at NASA Langley/Ames. He received his Ph. D./MS at University of Texas at Arlington in '96/'89 and two undergraduate degrees from The University of Minnesota. He founded the Software Engineering for Secure and Dependable Systems Lab in 1999. He is a Senior Member of the IEEE and member of ACM, IASTED, AIAA, including the Tau Beta Pi and Upsilon Pi Epsilon and received the Sigma Xi award for an outstanding dissertation. He has published over seventy papers in various journals and international conferences. His research has been concerned with developing and validating/testing models, applications, methods and supporting tools for the creation of safe, secure and dependable software/systems.