This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2005 proceedings.

On Quantum Authentication Protocols

Yoshito Kanamori[1], Seong-Moo Yoo[1], Don A. Gregory[2]
[1]Electrical and Computer Engineering Department
[2]Department of Physics
The University of Alabama in Huntsville
Huntsville, AL 35899, USA
{yoshitok, yoos, gregoryd}@email.uah.edu

Frederick T. Sheldon
Computational Sciences and Engineering Division
Oak Ridge National Laboratory*
Oak Ridge, TN 37831 USA
SheldonFT@ornl.gov

***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 computational power enough 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. We propose an authentication protocol using quantum superposition states instead of quantum entangled particles. Our protocol can be implemented with the current technologies we introduce in this paper.**

Keywords- Authentication, Encryption, Photon, Polarization, Quantum cryptography, Superposition states.

I. INTRODUCTION

Computer networks are always threatened by malicious users. For example, someone who is not authorized reads an important message deliberately. A message may also be modified with intent to annoy. If someone masquerades as a sender, a receiver cannot be sure that the origin of the message is authentic. Therefore, cryptography plays a significant role in computer networks.

Encryption schemes assure senders of the confidentiality of communication. A sender (Alice) encrypts a message (plain text) with a key that is shared with a receiver (Bob) and sends it to Bob. Bob decrypts the message with the key. Even if an eavesdropper (Eve) intercepts it, she cannot read the encrypted message (cipher text) without the key. However, it is not an easy task to share the secret keys between Alice and Bob prior to the communication because Alice cannot send a secret key to Bob by an open channel to the public. Thus, key distribution must be done by some other scheme.

A more important task 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 will be easily compromised. In the authentication scheme, a sender registers secret information as his identification code in the receiver's database prior to the communication. Then showing the secret information, a sender proves himself to be a legitimate person. Using an authentication protocol, a receiver can verify that the sender is a legitimate user before the connection is established.

As mentioned above, cryptography is widely diffused throughout computer networks. A significant problem is that most practical algorithms utilized in cryptography rely on computational complexity. In other words, these algorithms are only secure when malicious users do not have computational power enough 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 [1], 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 arbitrary quantum state is not possible [2][3]. 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 [4]. In general, photons are used as the media. For example, the BB84 protocol [5] (which is the most famous and thoroughly researched quantum key distribution (QKD) protocol that has been implemented in a practical application [6]), uses polarized photons. Alice sends polarized photons, referenced to one of two different orthogonal base sets (i.e., {horizontal, vertical} or

* This manuscript has been authored by UT-Battelle, a contractor of the U.S. Government (USG) under Department of Energy Contract DE-AC05-00OR22725. The USG retains a non-exclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for USG purposes.

$\{+45, -45\}$), 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.

Similar to the QKD, a quantum authentication scheme can also provide unconditional security. 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, we propose a two-party authentication protocol that utilizes quantum superposition states instead of sharing quantum entangled states. We will also show 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 and in section 3 our authentication protocol is proposed. Finally, conclusions are presented in section 4.

II. EXISTING QUANTUM AUTHENTICATION PROTOCOL

Recently, many quantum authentication protocols have been proposed and a formal definition of quantum authentication has been introduced [7]. 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 [9] 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 cannot 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 ([10], [11], [12], [13], [14], [15], [16]) utilize quantum-entangled states. For example, Curty [15] 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 [16] uses a trusted center to help the legitimate users obtain the sharing message. The trusted center sets up a quantum channel between Alice and the center, and between Bob and the center. 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 information about which base they used for measurements in order to share a session key so that the trusted center cannot know the session keys. In this protocol, both authentication and QKD are implemented.

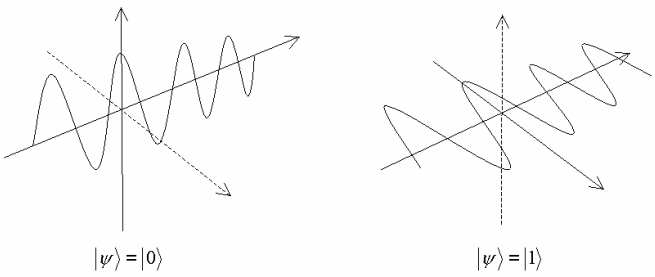
III. PROPOSED AUTHENTICATION PROTOCOL

In this section, the proposed quantum authentication protocol is explained in details.

A. General

1) Encoding by polarization of photons

We use only a horizontal-vertical polarization base for encoding and measuring a sequence of polarized photons (Figure 1). Here, "polarized photon" means a very short pulse of polarized light, each pulse containing a single photon. The vertically polarized photon represents zero in a binary representation. The horizontally polarized photon represents one. In our protocol, all transmitted polarized photons are encrypted before the transmission, as shown in next section.

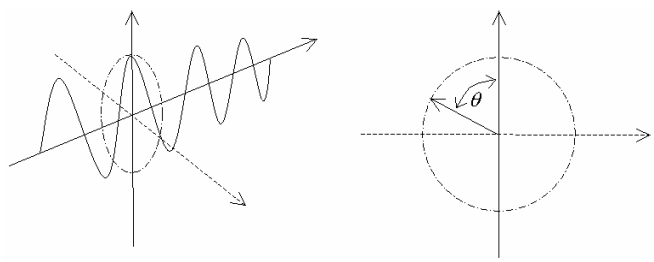


(a) (b)

Figure 1: Horizontal-vertical polarization base.

2) Encryption and decryption by rotation of polarized photons

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 θ_i ($i = 1,2,3,..., n$, for n-bit message) prior to the communication.



(a) (b)

Figure 2: A randomly chosen angle used as a secret key.

In our protocols, we define the shared set of angles as a secret key *K* and the rotation operation as encryption (i.e., a process of disguising to hide its substance) with a secret key *K*. Let $E_K[M]$ be an encryption of data *M*. Then, in order to read the disguised photons correctly, the receiver must rotate the transmitted photon by the angle θ_i in the opposite direction of what the sender rotated. We define this operation as decryption with the secret key *K* in our protocol. Let us $D_K[M]$ be a decryption of data *M*. These operations can be represented mathematically as shown below.

A polarized data particle is represented as a vector

$$|\psi\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ or } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

for the binary bit information '0' or '1' respectively. Rotating by θ can be represented as follows:

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

For example, if the data qubit is $|\psi\rangle = |0\rangle$. A sender (Alice) encrypts the data qubit $|\psi\rangle$ with θ_A. (θ_A is randomly chosen and is shared between Alice and Bob prior to the communication.)

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

Alice sends the superposition states $|\psi_1\rangle$ to a receiver (Bob).

Before Bob measures the received photon, he needs to rotate the received photon by θ_A in the opposite direction of what Alice rotated. The decryption (rotating by $-\theta_A$) can be represented as follows:

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

The main advantage of this encryption/decryption scheme is that a receiver doesn't have to decrypt a cipher text in the same 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_2 and then decrypt it with K_1.

3) An example of experimental realization and measurement of photons

The photon is linearly polarized by a polarizing apparatus, which is 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 [17]). 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. The state of the photon is represented as $|\psi\rangle = \cos\theta \cdot |0\rangle - \sin\theta \cdot |1\rangle$. Since this is a superposition state of: $|0\rangle$ and $|1\rangle$, when we measure the state with a horizontal-vertical polarization base, both $|0\rangle$ and $|1\rangle$ 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

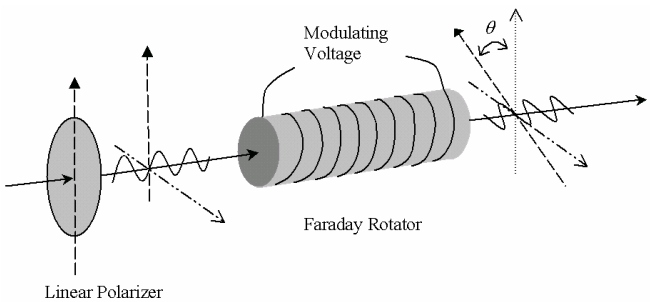


Figure 3: An Example of an experimental realization.

$$|\psi\rangle = \cos 30 \cdot |0\rangle - \sin 30 \cdot |1\rangle = \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle.$$

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. When the angle is 90 degrees, we will find the photon to be in the state $|1\rangle$ with the probability 1, theoretically.

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 states, no one can make a copy of the transmitted data without errors. Intercept/resend attack and beam splitting attacks are not possible against our authentication protocol as shown below.

a) Intercept/resend attack

Let us assume that an eavesdropper (Eve) intercepts the transmitted photons 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 $\theta_i = 45$ 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. 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.

If Eve can make a lot of 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, this operation is impossible because the no-cloning theorem forbids copying unknown states without errors.

b) 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 as 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 [18]. 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 photon until Alice and Bob announce 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. Also, since the secret keys are used only once or used with session secret keys, the angles found by Eve will no longer be useful after the transmission.

B. Two-Party Authentication Protocol

In this protocol, we use a classical channel and a quantum 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 *Ka* (i.e., a set of rotation angles, θ_i) prior to the communication.

1. Alice sends a request message with her name to Bob by a classical channel.
2. Bob generates a random number R_B and encodes it as polarized photons in a horizontal-vertical base.
3. Bob generates a session key *Ks*.

4. Bob encrypts the polarized photons using the session key *Ks*. (i.e., rotation by θ_i)
5. Bob encrypts the already encrypted polarized photons, $E_{Ks}[R_B]$ using the shared key *Ka*. (i.e., rotation by θ_j)
6. Bob sends $E_{Ka}[E_{Ks}[R_B]]$ to Alice by a quantum channel.
7. Alice decrypts the photons using the shared key *Ka*. (i.e., rotation by $-\theta_j$)
8. Alice sends the result $E_{Ks}[R_B]$ to Bob by a quantum channel.
9. Bob decrypts the photons $E_{Ks}[R_B]$ using the session key *Ks*. (i.e., rotation by $-\theta_i$)
10. Bob verifies the decrypted message $D_{Ks}\,E_{Ks}[R_B]$ and the original random number R_B. If they are same, Alice is authenticated.
11. The session key *Ks* and R_B are discarded.

Figure 4 shows the two-party authentication protocol.

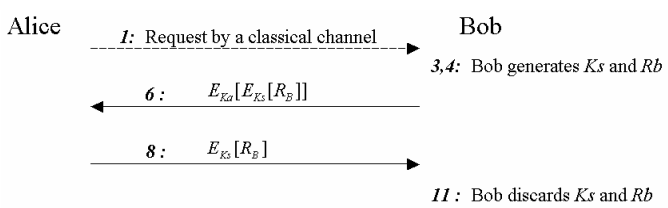


Figure 4: Two-party authentication protocol.

In this protocol, the session key *Ks* has a vital role. If the protocol does not have steps 3, 4 and 9, the transmitted polarized photon from Alice at step 8 is one of the orthogonal states. Therefore, an intercept/resend attack is possible. Eve can make a copy of the data without being detected by Bob. This is a significant security risk because, in general, random numbers are created by a pseudo-random algorithm. Eve may find the algorithm and can masquerade as Alice without knowing the shared key. Since not only Eve but also Alice does not know the session key *Ks*, Alice has no way to know the contents of the received photons. This will prevent potential security risks. (e.g., a passive cheating [19] by Alice: she follows the protocol, but tries to acquire information that she is not supposed to have). Needless to say, if this protocol uses only one shared key, the scheme itself becomes much simpler. However, the secret key will be reused repeatedly and Alice and Bob have to renew the shared key frequently to reduce the probability that Eve finds the key by observing the channel, although Bob can detect Eve's eavesdropping by checking the error rates as mentioned previously.

4. 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 under the assumption that both parties *already* share a secret key (Ka). Furthermore, we showed that the superposition states can be realized using current technologies (e.g., linear polarizers and Faraday rotators).

REFERENCES

[1] Peter W.Shor, Algorithm for quantum computation: discrete logarithm and factoring, Proc.35th IEEE Annual Symposium on Foundations of Computer Science, Santa Fe, NM, November, 1994, 24-134.

[2] W.K. Wootters, W.H. Zurek, A single quantum cannot cloned, Nature 299 (1982) 802-803.

[3] M.A. Nielsen, I.L. Chuang, Quantum computation and quantum information, Cambridge University Press, Cambridge, 2000.

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

[5] C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in: Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India (1984) 175-179.

[6] C.Gobby, Z. L. Yuan, and A. J. Shields, Quantum key distribution over 122 km of standard telecom fiber, Applied Physics Letters, Vol.84, 19 (2004) 3762.

[7] Howard Barnum, Claude Crepeau, Daniel Gottesman, Adam Smith, Alain Tapp, Authentication of Quantum Messages, Proc. 43rd Annual IEEE Symposium on the Foundations of Computer Science (FOCS '02), IEEE Press (2002) 449-458.

[8] Miloslav Dusek1, Ondrej Haderka, Martin Hendrych, Robert Myska, Quantum identification system, Phys. Rev. A 60 (1999) 149–156.

[9] D.R. Kuhn, A Hybrid Authentication Protocol Using Quantum Entanglement and Symmetric Cryptography, quant-ph/0301150.

[10] Yong-Sheng Zhang, Chuan-Feng Li, Guang-Can Guo, Quantum authentication using entangled state, quant-ph/0008044.

[11] Guihua Zeng, Guangcan Guo, Quantum authentication protocol, quant-ph/0001046.

[12] Jensen, Jens G, Schack, Ruediger, Quantum authentication and key distribution using catalysis, quant-ph/0003104.

[13] Rex A. C. Medeiros, Francisco M. de Assis, Bernardo L. Júior, Aércio F. Lima, Quantum authentication scheme based on algebraic coding, quant-ph/0307095.

[14] Howard N. Barnum, Quantum secure identification using entanglement and catalysis, quant-ph/9910072.

[15] Marcos Curty, David J. Santos, Quantum authentication of classical messages, Phys. Rev. A 64 (2001) 062309.

[16] Guihua Zeng, Weiping Zhang, Identity verification in quantum key distribution, Phys. Rev. A 61 (2000) 022303.

[17] Bahaa E. A. Saleh, Malvin Carl Teich, Fundamentals of Photonics, John Wiley, New York, 1991.

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

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