Quantum identification schemes with entanglements

Takashi Mihara*
Department of Management Science, Kyushu Tokai University, 9-1-1, Toroku, Kumamoto, 862-8652, Japan
(Received 5 December 2001; published 8 May 2002)

We need secure identification schemes because many situations exist in which a person must be identified. In this paper, we propose three quantum identification schemes with entanglements. First, we propose a *quantum one-time pad password scheme*. In this scheme, entanglements play the role of a one-time pad password. Next, we propose a *quantum identification scheme* that requires a trusted authority. Finally, we propose a *quantum message authentication scheme* that is constructed by combining a different quantum cryptosystem with an ordinary authentication tag.

DOI: 10.1103/PhysRevA.65.052326 PACS number(s): 03.67.Dd, 03.67.Hk

Due to the popularization of several global networks, we need many techniques to transmit information securely. Recently, information security techniques based on *quantum physics* have been actively studied because it is thought that these are more secure than classical ones. The most famous scheme is a *quantum key distribution scheme* [1–3], and some protocols of this scheme have proved to be unconditionally secure protocols [4–8]. Other quantum security schemes are also proposed, e.g., a quantum identification scheme [9–11] and a quantum digital signature scheme [12]. These schemes use entanglements effectively. Also in the quantum communication complexity theory, we use some type of entanglements being shared among parties. The entanglements used in it are called *prior entanglements* because these are prepared beforehand among the parties [13–15]. The central role of prior entanglements is that parties can *share* some property related to the input values of a given problem without communication among the parties.

In this paper, we propose three quantum information security schemes with entanglements, a quantum one-time pad password scheme, a quantum identification scheme, and a quantum message authentication scheme. These schemes are very significant for today's electronic society. We construct unconditionally secure protocols under prior entanglements. That is, the probability that any eavesdropper guesses secret information is the same as that of deciding a value at random. First, the *quantum one-time pad password scheme* is a quantum analogy of classical ones. In this scheme, a user uses some prior entanglements as a password in order to be identified by a system. Next, we propose a *quantum identification scheme*, which authenticates a person's identity to another person and is thought to be an extension of the password scheme. Our identification scheme requires a trusted authority (TA). Some identification schemes between two persons are proposed [9–11]; however, these schemes are only a defense against eavesdroppers. Although the methods that do not use any TA are simple and convenient, there is a problem such that a verifier cannot confirm that a prover is the person who is identified. Therefore, we think that the existence of a TA is reasonable for the real world because the information on a person's identity must exist somewhere in order to confirm the person. Finally, we propose a *quantum message authentication scheme*, which is a scheme confirming that a person's message is indeed the person's message to another specific person only once. Our protocol is constructed by combining a quantum cryptosystem with an ordinary authentication tag. Therefore, we also denote a different quantum cryptosystem used in the protocol.

Throughout this paper, we assume that entanglements can be securely shared among parties and can be kept for a long time. The technique of sharing entanglements securely through an insecure channel is shown by Refs. [4,16]. Moreover, we construct our protocols under the assumption that the communication channels used in them are error free or noiseless, and a public channel is a channel such that anyone can read messages but cannot alter them.

In general, a user will have to be identified by a mechanical system for security if he wishes to use it. However, if he stays at a place remote from there (e.g., due to travel), he needs to send his identification data such as a password through an insecure channel. This involves many risks because an eavesdropper may steal his identification data. In order to avoid this situation, we consider an identification scheme between a user and a mechanical system, where the mechanical system means a system that does not cheat anyone. We then propose a quantum one-time pad password scheme that regards prior entanglements as a password.

Before a user goes out, he and the system prepare a set of n prior entanglements $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle$ taking the form

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle), \tag{1}$$

where the user has a set of the first qubits and the system has a set of the second qubits. Throughout this paper, we take $\mathcal{B}=\{|0\rangle,|1\rangle\}$ as a basis. Moreover, the system assigns an (ordinary) password $p=(p_1,p_2,\ldots,p_n)$ to the user, where $p_i \in \{0,1\}(i \in \{1,2,\ldots,n\})$. Each entanglement $|\psi_i\rangle$ is related to each p_i. If they think that they need not use the password p, the system takes only $p=(0,0,\ldots,0)$.

Quantum password

(1) A user requires the use of a system. [They share n prior entanglements $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle$ taking the form of Eq. (1).]

*Electronic address: tmihara@ktmail.ktokai-u.ac.jp

(2) The system selects an n-bit number $r=(r_1,r_2,\ldots,r_n)$ at random, where $r_i\in\{0,1\}(i\in\{1,2,\ldots,n\})$.

(3) For $1\leqslant i\leqslant n$, execute the following.

(a) If $r_i\oplus p_i=0$, the system applies nothing to $|\psi_i\rangle$; otherwise the system applies

$$X=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

to $|\psi_i\rangle$.

(b) If $p_i=0$, the user applies nothing to $|\psi_i\rangle$; otherwise he applies X to $|\psi_i\rangle$. If $r_i=0$, then $|\psi_i\rangle\rightarrow|\psi_i'\rangle=(1/\sqrt{2})(|0,0\rangle+|1,1\rangle)$; otherwise $|\psi_i\rangle\rightarrow|\psi_i'\rangle=(1/\sqrt{2})(|0,1\rangle+|1,0\rangle)$.

(4) For $1\leqslant i\leqslant n$, execute the following.

(a) The user measures $|\psi_i'\rangle$ in $\mathcal{B}$ and sends the outcome u_i to the system through a public channel.

(b) The system also measures $|\psi_i'\rangle$ in $\mathcal{B}$ and obtains the outcome s_i.

(5) The system verifies whether $r_i=u_i\oplus s_i(i\in\{1,2,\ldots,n\})$.

If this protocol is correctly executed, the user can be identified by the system because $u_i\oplus s_i=r_i$. Therefore, we analyze the security of this protocol. Let $\varepsilon(0\leqslant\varepsilon<1/2)$ be the error rate of the device. That is, maximally εn errors occur. The probability that an eavesdropper impersonates the user, i.e., the probability that she guesses the user's outcome before step (4), is then at most $\Sigma_{l=0}^{\varepsilon n}\binom{n}{l}2^{-n}\leqslant\binom{n}{\varepsilon n}2^{-(1-\varepsilon)n}$ because she only guesses each bit at random with the probability 1/2. Thus, the probability approximates zero if n is sufficiently large, and she cannot cheat the system. Moreover, because the user's outcome is not reusable, she cannot use the outcome obtained in step (4) next time in order to access the system. This protocol is then secure providing that both of the shared entanglements and the password are not stolen.

Furthermore, we extend the protocol to a multiparty case. Let $B_1, B_2, \ldots, B_m$ be m parties. We consider a problem in which B_m wishes to use the system but he needs the aid of the other parties, $B_1,\ldots,B_{m-1}$, in order to use the system. Here, we consider only the case where $B_1,\ldots,B_{m-1}$ are honest.

Before all the parties and the system begin the protocol, they prepare a set of n prior entanglements $|\psi_1\rangle,|\psi_2\rangle,\ldots,|\psi_n\rangle$ taking the form

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|0,0,\ldots,0\rangle+|1,1,\ldots,1\rangle), \tag{2}$$

where its length is $m+1$ qubits, $B_j(j\in\{1,2,\ldots,m\})$ has a set of the jth qubits, and the system has a set of the $(m+1)$th qubits. Moreover, the system assigns an ordinary password p to B_m.

Multiparty quantum password

(1) Party B_m requires the use of a system. [They share n prior entanglements $|\psi_1\rangle,|\psi_2\rangle,\ldots,|\psi_n\rangle$ taking the form of Eq. (2).]

(2) The system selects an n-bit number $r=(r_1,r_2,\ldots,r_n)$ at random, where $r_i\in\{0,1\}(i\in\{1,2,\ldots,n\})$.

(3) For $1\leqslant i\leqslant n$, execute the following.

(a) If $r_i\oplus p_i=0$, the system applies nothing to $|\psi_i\rangle$; otherwise the system applies

$$Z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

to $|\psi_i\rangle$.

(b) If $p_i=0$, B_m applies nothing to $|\psi_i\rangle$; otherwise he applies Z to $|\psi_i\rangle$. If $r_i=0$, then $|\psi_i\rangle\rightarrow|\psi_i'\rangle=1/\sqrt{2}(|0,0,\ldots,0\rangle+|1,1,\ldots,1\rangle)$; otherwise $|\psi_i\rangle\rightarrow|\psi_i'\rangle=1/\sqrt{2}(|0,0,\ldots,0\rangle-|1,1,\ldots,1\rangle)$.

(4) For $1\leqslant i\leqslant n$, execute the following.

(a) All the parties and system apply the Walsh-Hadamard matrix H

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

to the state $|\psi_i'\rangle$. If $r_i=0$, then

$$|\psi_i'\rangle\rightarrow|\psi_i''\rangle=\frac{1}{\sqrt{2^m}}\sum_{\oplus_{j=1}^m b_{ij}\oplus s_i=0}|b_{i1},\ldots,b_{im},s_i\rangle;$$

otherwise

$$|\psi_i'\rangle\rightarrow|\psi_i''\rangle=\frac{1}{\sqrt{2^m}}\sum_{\oplus_{j=1}^m b_{ij}\oplus s_i=1}|b_{i1},\cdots,b_{im},s_i\rangle.$$

(5) For $1\leqslant i\leqslant n$, execute the following.

(a) Each party B_j measures $|\psi_i''\rangle$ in $\mathcal{B}$ and sends the outcome b_{ij} to the system.

(b) The system also measures $|\psi_i''\rangle$ in $\mathcal{B}$ and obtains the outcome s_i.

(6) The system verifies whether $r_i=\oplus_{j=1}^m b_{ij}\oplus s_i(i\in\{1,2,\ldots,n\})$.

Also in this case, if this protocol is correctly executed, party B_m can be identified by the system. Therefore, we analyze the security of this protocol. This protocol is also secure against any eavesdropper for the same reason as the previous protocol. Here, we consider a case in which B_m tries to cheat the system, i.e., B_m tries to use the system without the aid of the other parties, $B_1,\ldots,B_{m-1}$. Let

$$|\psi_i\rangle=(1/\sqrt{2})(|0,0,\ldots,0\rangle+|1,1,\ldots,1\rangle)$$
$$=(1/\sqrt{2})(|\mathbf{0},0,0\rangle+|\mathbf{1},1,1\rangle),$$

where $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$ are the collective bits of $B_1,\ldots,B_{m-1}$. Now, party B_m applies not H but a general unitary operator

$$U=\begin{pmatrix} a & -b \\ b^* & a^* \end{pmatrix}$$

to his qubit in the state $|\psi_i\rangle$, where a and b are complex numbers satisfying $|a|^2+|b|^2=1$. Then,

$$|\psi_i''\rangle=\tfrac{1}{2}[|\mathbf{0}\rangle(a|0,0\rangle+a|0,1\rangle+b^*|1,0\rangle+b^*|1,1\rangle) \pm|\mathbf{1}\rangle(-b|0,0\rangle+b|0,1\rangle+a^*|1,0\rangle-a^*|1,1\rangle)].$$

Thus, party B_m and the system obtain only one of four pairs (0,0), (0,1), (1,0), and (1,1) with the equal probability 1/4 independent of r_i as the measurement outcome. This means that B_m only guesses $b_{im}(1\leqslant i\leqslant n)$ at random and cannot cheat the system.

The entanglements in these protocols cannot be reused. However, because no secret information can be obtained by eavesdropping through a channel, the ordinary password p is reusable if the system can maintain it securely.

Next, we propose a quantum identification scheme that authenticates a person's identity to another person. If a person wishes only to verify whether he shares entanglements with another person, we can use the protocol mentioned above. For instance, this type of quantum identification scheme is proposed in Refs. [9–11]. Here, we consider another type of identification scheme including a method verifying whether a person is indeed the person whom another person wishes to confirm.

In our scheme, we require a TA. We think that for the real world, the existence of a TA is reasonable because the person's information must exist somewhere in order to confirm a person's identity. Now, we call the prover Alice and the verifier Bob. We then construct a protocol that authenticates Alice's identity to Bob. This protocol is constructed of two parts, ''issuing a certificate to Alice'' and ''identifying Alice to Bob.''

Issuing a certificate to Alice

(1) A TA establishes Alice's identity by means of conventional forms of identification, such as a passport, and forms an n-bit string $I(Alice)$.

(2) The TA splits $I(Alice)$ into $I_A(Alice)\oplus I_{pub}(Alice)\oplus I_{TA}(Alice)$.

(3) The TA gives $I_A(Alice)$ to Alice and opens $I_{pub}(Alice)$ to the public as Alice's public identification information. Moreover, the TA maintains $I(Alice)$ and $I_{TA}(Alice)$ securely.

Note that only the TA knows the information of Alice's identification $I(Alice)$.

Next, we show the protocol of identifying Alice to Bob. Here, let

$$I(Alice)=(I_1,I_2,\ldots,I_n),$$

$$I_A(Alice)=(I_{A1},I_{A2},\ldots,I_{An}),$$

$$I_{pub}(Alice)=(I_{pub1},I_{pub2},\ldots,I_{pubn}),$$

and

$$I_{TA}(Alice)=(I_{TA1},I_{TA2},\ldots,I_{TAn}),$$

where each is a bit.

Identifying Alice to Bob

(1) Bob requires the authentication of Alice's identity to the TA.

(2) The TA makes a set of n entanglements $|\psi_1\rangle,|\psi_2\rangle,\ldots,|\psi_n\rangle$ taking the form

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|0,0,0\rangle+|1,1,1\rangle).$$

(3) The TA sends a set of the first qubits to Alice and a set of the second qubits to Bob.

(4) For $1\leqslant i\leqslant n$, execute the following.

(a) If $I_{Ai}=0$, Alice applies nothing to $|\psi_i\rangle$; otherwise she applies Z to $|\psi_i\rangle$.

(b) If $I_{pubi}=0$, Bob applies nothing to $|\psi_i\rangle$; otherwise he applies Z to $|\psi_i\rangle$.

(c) If $I_{TAi}=0$, the TA applies nothing to $|\psi_i\rangle$; otherwise it applies Z to $|\psi_i\rangle$. If $I_{Ai}\oplus I_{pubi}\oplus I_{TAi}=0$, $|\psi_i\rangle\rightarrow|\psi_i'\rangle=(1/\sqrt{2})(|0,0,0\rangle+|1,1,1\rangle)$; otherwise $|\psi_i\rangle\rightarrow|\psi_i'\rangle=(1/\sqrt{2})(|0,0,0\rangle-|1,1,1\rangle)$.

(5) Each party announces the completion of the procedure to the others through a public channel.

(6) All the parties apply H to every $|\psi_i'\rangle(i\in\{1,2,\ldots,n\})$. If

$$I_{Ai}\oplus I_{pubi}\oplus I_{TAi}=0,\quad |\psi_i'\rangle\rightarrow|\psi_i''\rangle=\frac{1}{2}\sum_{a_i\oplus b_i\oplus t_i=0}|a_i,b_i,t_i\rangle;$$

otherwise

$$|\psi_i'\rangle\rightarrow|\psi_i''\rangle=\frac{1}{2}\sum_{a_i\oplus b_i\oplus t_i=1}|a_i,b_i,t_i\rangle.$$

(7) Each party announces the completion of the procedure to the others through a public channel.

(8) Alice measures every $|\psi_i''\rangle(i\in\{1,2,\ldots,n\})$ in $\mathcal{B}$, obtains n-bit values $a=(a_1,a_2,\ldots,a_n)$, and sends a to the TA through a public channel.

(9) Bob also measures every $|\psi_i''\rangle$ in $\mathcal{B}$, obtains n-bit values $b=(b_1,b_2,\ldots,b_n)$, and sends b to the TA through a public channel.

(10) The TA also measures every $|\psi_i''\rangle$ in $\mathcal{B}$ and obtains n-bit values $t=(t_1,t_2,\ldots,t_n)$.

(11) The TA verifies whether $I(Alice)=a\oplus b\oplus t$ and sends the outcome to Bob through a public channel.

If this identifying protocol is correctly executed, Bob can identify Alice because $a\oplus b\oplus t=I_A\oplus I_{pub}\oplus I_{TA}=I(Alice)$. Therefore, we analyze the security of this protocol. Note that, in general, $a\oplus b\neq I_A\oplus I_{pub}$ although $a\oplus b\oplus t=I_A\oplus I_{pub}\oplus I_{TA}$. Even if Alice's value a and Bob's value b are stolen, any eavesdropper (including Bob) cannot then find the information for $I(Alice)$, $I_{TA}(Alice)$, or $I_A(Alice)$, and Alice also cannot find $I(Alice)$ or $I_{TA}(Alice)$. In other words, the probability that an eavesdropper obtains each of them is 2^{-n}

because she only guesses each bit at random with the probability 1/2. Next, we consider the case in which an eavesdropper tries to impersonate Alice either by using the value a or by stealing the entanglements. Because the value a is not reusable, no eavesdropper can impersonate Alice by using a next time. Moreover, because only Alice knows the value $I_A(Alice)$ even if the entanglements are stolen, the probability that an eavesdropper can cheat Bob is at most $\binom{n}{\varepsilon n}2^{-(1-\varepsilon)n}$ for the same reason with the previous protocols, where $\varepsilon(0\leqslant\varepsilon<1/2)$ is the error rate of the device.

Finally, we consider a quantum message authentication scheme. In our protocols mentioned above, the information for communicating with each other might be stolen but must not be altered. Therefore, we used a public channel because of each party being able to verify it. Here, we propose a scheme verifying whether a message through a channel is altered.

Now, we consider that Alice has an n-bit message $s=(s_1,s_2,\ldots,s_n)$ and sends it to Bob through an insecure channel. First, we denote a quantum cryptosystem used in our message authentication protocols

Quantum cryptosystem

(1) Alice makes a set of n entanglements $|\psi_1\rangle,|\psi_2\rangle,\ldots,|\psi_n\rangle$, taking the form of Eq. (1), and sends a set of the second qubits to Bob.

(2) For $1\leqslant i\leqslant n$, execute the following.

(a) If $s_i=0$, Alice applies nothing to $|\psi_i\rangle$, i.e., $|\psi_i'\rangle=(1/\sqrt{2})(|0,0\rangle+|1,1\rangle)$; otherwise she applies X to $|\psi_i\rangle$, i.e., $|\psi_i'\rangle=(1/\sqrt{2})(|0,1\rangle+|1,0\rangle)$.

(3) Alice measures every $|\psi_i'\rangle(i\in\{1,2,\ldots,n\})$ in $\mathcal{B}$, obtains n-bit values $a=(a_1,a_2,\ldots,a_n)$, and sends a to Bob.

(4) Bob also measures every $|\psi_i'\rangle$ in $\mathcal{B}$ and obtains n-bit values $b=(b_1,b_2,\ldots,b_n)$.

(5) Bob recovers s by computing $a\oplus b$ because $a\oplus b=s$.

We describe the quantum cryptosystem for a message s as $Q_c(s)$.

We then propose a quantum message authentication protocol by combining the quantum cryptosystem with an ordinary security means, an authentication tag.

Quantum message authentication

(1) Alice selects a one-way hash function h, computes $t_s=h(s)$ as an authentication tag, and makes a triplet $m=(s,h,t_s)$.

(2) Alice sends m to Bob by using the $Q_c(m)$.

(3) Bob verifies whether $t_s=h(s)$.

Note that we can use not only a trapdoor function but a real one-way function as the function h.

Obviously, if this protocol is correctly executed, Bob can authenticate Alice's message. Part of authenticating a message depends on the one-way hash function h; therefore, we cannot precisely evaluate the security. However, because all the transmitted data including h are encrypted, we think that Bob will be able to detect it in step (3) with high probability even if an attacker tries to alter the message m. That is, an attacker only guesses the content of the message at random if our quantum cryptosystem is used. Moreover, an attacker cannot make m even if the attacker wishes to impersonate Alice, because the attacker does not share entanglements with Bob.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), p. 175.

[2] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[4] H.-K. Lo and H.F. Chau, Science **283**, 2050 (1999).

[5] D. Mayers, e-print quant-ph/9802025.

[6] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundation of Computer Science* (IEEE, Los Alamitos, 1998), p. 509.

[7] E. Biham *et al.*, in *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing* (ACM, New York, 2000), p. 715.

[8] P.W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[9] M. Dušek, O. Haderka, M. Hendrych, and R. Myška, Phys. Rev. A **60**, 149 (1999).

[10] H. Barnum, e-print quant-ph/9910072.

[11] J.G. Jensen and R. Schack, e-print quant-ph/0003104.

[12] D. Gottesman and I.L. Chuang, e-print quant-ph/0105032.

[13] H. Buhrman, R. Cleve, and W. van Dam, SIAM J. Comput. **30**, 1829 (2000).

[14] H. Buhrman, W. van Dam, P. Høyer, and A. Tapp, Phys. Rev. A **60**, 2737 (1999).

[15] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).

[16] C.H. Bennett *et al.*, Phys. Rev. A **54**, 3824 (1996).