



ISSN 1022-4653

CODEN CHJEEW



CHINESE JOURNAL OF ELECTRONICS



A Publication of CIE

Vol.15 No.1 January 2006

Published by

- Chinese Institute of Electronics(CIE)
- School of Information Science and Technology, Tsinghua University
- Faculty of Information Engineering Science, Peking University
- Institute of Semiconductors, Chinese Academy of Sciences
- University of Electronic Science and Technology of China
- Xidian University
- The Chinese University of Hong Kong
- Shenzhen University
- Technology Exchange Ltd.

A Quantum Identification Scheme Based on Phase Modulation*

HE Guangqiang and ZENG Guihua

(The State Key Laboratory on Fiber-Optic Local Area Networks and Advanced Optical Communication Systems, Electronic Engineering Department, Shanghai Jiaotong University, Shanghai 200030, China)

Abstract — A quantum identification scheme including registration and identification phases is proposed. The users' passwords are transmitted by qubit string and recorded as a set of quantum operators. The security of the proposed scheme is guaranteed by the no-cloning theorem. Based on photon phase modulation, an experimental approach is also designed to implement our proposed scheme.

Key words — Quantum identification, Quantum cryptography, Cryptography, Phase modulation.

I. Introduction

Quantum cryptography^[1] is a field of study which combines quantum and information theories. Since the first quantum key distribution protocol-BB84 protocol^[2] was presented by the C.H.Bennett and G.Brassard, many advanced topics in quantum cryptography have been put forward in recent years, including enhanced sights into the basic theory^[3], quantum key management^[4], quantum secret sharing^[5], quantum authentication^[6], quantum-bit commitment^[7]. In contrast to the classical cryptography, which is only relatively secure, quantum cryptography shows absolute security due to its intrinsic quantum characters^[8,9]. In particular, Quantum key distribution (QKD) attracts lots of attention from both academic and commercial societies because of its unconditional security and more possibility of implementation.

Experiments on quantum key distribution may be implemented through two quantum channels: free space and optic fiber. M.Halder in Ludwig-Maximilians-University reported on a BB84 based free space quantum cryptography system^[10] over 23.4km in 2002. The research group led by professor N.Gisin in Geneva university designed auto-compensating plug & play system^[11] over the installed optic fiber in 2002, and the keys were exchanged over a distance of 67km. Many papers on quantum identification system^[12-17] were published. In this paper, a quantum identification scheme to dynamically build the users' database according to the password and the identity card of the legitimate user is presented. The security of the scheme is guaranteed by the no-cloning theorem of the unknown quantum state.

A new quantum identification scheme is introduced in de-

tail in Section II. The proposed scheme includes a registration phase, an identification phase. In Section III, we discuss the security of the proposed scheme. In Section IV, the experimental system based on photon phase modulation is set up in order to carry out this quantum identification scheme. Conclusions are drawn in Section V.

II. Description of the Proposed Quantum Identification Scheme

In the proposed scheme, U^k denotes the k -th user, IS is the identification system. The proposed scheme includes a registry phase and an identification phase. During the registry phase, the identification system dynamically builds the users' information in the users' database after it receives the users' registry requests. In the identification phase, the identification system verifies the user's identity according to the corresponding user's information in the users' database.

The proposed scheme (Fig.1.) is described as follows:

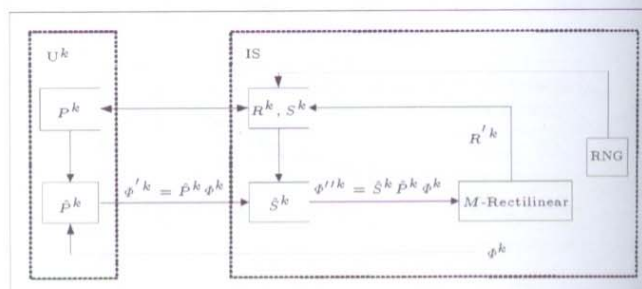


Fig. 1. Quantum identification scheme

1. Registration phase

(1) When the Identification system (IS) receives the registry requirement of the user U^k , it prepares a set of initial quantum states, $\Phi^k = (|\phi_1^k\rangle, |\phi_2^k\rangle, \dots, |\phi_n^k\rangle)$ taking the form $|\phi_1^k\rangle = |0\rangle$, $i \in \{1, 2, \dots, n\}$. The user U^k sets up the password $P^k = (p_1^k, p_2^k, \dots, p_n^k)$, $p_i^k \in \{1, 2, \dots, m\}$, $i \in \{1, 2, \dots, n\}$. P^k corresponds to a set of quantum operations, which are denoted by a set of quantum operators $\hat{P}^k = (\hat{p}_1^k, \hat{p}_2^k, \dots, \hat{p}_n^k)$. Note that the number p_i^k corresponds to the special quantum

*Manuscript Received Aug. 2004; Accepted May 2005. This work is supported by the National Natural Science Foundation of China (No.60472018).

operator \hat{p}_i^k . If $p_i^k \neq p_j^k$, then $\hat{p}_i^k \neq \hat{p}_j^k$. The password P^k is transmitted to IS by quantum key distribution (for example BB84 protocol^[2]) or secure channel. Then IS knows the corresponding quantum operator $\hat{P}^k = (\hat{p}_1^k, \hat{p}_2^k, \dots, \hat{p}_n^k)$. Both IS and U don't know the key during quantum key distribution, they gain the key after finishing quantum key distribution^[1].

(2) IS prepares a n -bit random number

$$R^k = (r_1^k, r_2^k, \dots, r_n^k), r_i^k \in \{0, 1\}, i \in \{1, 2, \dots, n\}$$

for the user U^k , at the same time, and sets up the information of the user U^k ,

$$S^k = (s_1^k, s_2^k, \dots, s_n^k), s_i^k \in \{1, 2, \dots, m\}, i \in \{1, 2, \dots, n\}$$

in the users' database. S^k corresponds to a set of quantum operations, which are denoted by a set of quantum functors $\hat{S}^k = (\hat{s}_1^k, \hat{s}_2^k, \dots, \hat{s}_n^k)$ subjected to the following conditions:

For $1 \leq i \leq n$,

if $r_i^k = 0$, then $|\phi_i''^k\rangle = \hat{s}_i^k \hat{p}_i^k |\phi_i^k\rangle = |0\rangle$, that is to say, $\hat{s}_i^k \hat{p}_i^k = I$

if $r_i^k = 1$, then $|\phi_i''^k\rangle = \hat{s}_i^k \hat{p}_i^k |\phi_i^k\rangle = |1\rangle$, that is to say, $\hat{s}_i^k \hat{p}_i^k = \hat{\sigma}_x$

Now the messages $R^k = (r_1^k, r_2^k, \dots, r_n^k)$, $r_i^k \in \{0, 1\}$, $i \in \{1, 2, \dots, n\}$ and $S^k = (s_1^k, s_2^k, \dots, s_n^k)$, $s_i^k \in \{1, 2, \dots, m\}$, $i \in \{1, 2, \dots, n\}$ are used as the information of the user U^k in the users' database. When the user U^k sets up the certainly password $P^k = (p_1^k, p_2^k, \dots, p_n^k)$, $p_i^k \in \{1, 2, \dots, m\}$, $i \in \{1, 2, \dots, n\}$ then $R^k = (r_1^k, r_2^k, \dots, r_n^k)$, $r_i^k \in \{0, 1\}$, $i \in \{1, 2, \dots, n\}$ has the certainly corresponding relation with $S^k = (s_1^k, s_2^k, \dots, s_n^k)$, $s_i^k \in \{1, 2, \dots, m\}$. The fact must be emphasized.

After the user completes the registry phase, the password of the user U^k is $P^k = (p_1^k, p_2^k, \dots, p_n^k)$, $p_i^k \in \{1, 2, \dots, m\}$, $i \in \{1, 2, \dots, n\}$, the file named as U^k in the users' database contains the user U^k 's identity messages

$$R^k = (r_1^k, r_2^k, \dots, r_n^k), r_i^k \in \{0, 1\}, i \in \{1, 2, \dots, n\}$$

and

$$S^k = (s_1^k, s_2^k, \dots, s_n^k), s_i^k \in \{1, 2, \dots, m\}, i \in \{1, 2, \dots, n\}.$$

Repeat the steps (1) and (2), many users can register the quantum identification system.

2. Identification phase

(3) IS finds the file U^k from the users' database according to the file name U^k when it receives the identification requirement of the user U^k . The registry messages $R^k = (r_1^k, r_2^k, \dots, r_n^k)$, $r_i^k \in \{0, 1\}$, $i \in \{1, 2, \dots, n\}$ and $S^k = (s_1^k, s_2^k, \dots, s_n^k)$, $s_i^k \in \{1, 2, \dots, m\}$, $i \in \{1, 2, \dots, n\}$ are used to identify the user U^k .

(4) The user U^k inputs the password $P^k = (p_1^k, p_2^k, \dots, p_n^k)$, $p_i^k \in \{1, 2, \dots, m\}$, $i \in \{1, 2, \dots, n\}$, IS applies a set of corresponding quantum operators $\hat{P}^k = (\hat{p}_1^k, \hat{p}_2^k, \dots, \hat{p}_n^k)$ to a set of initial quantum states $\Phi^k = (|\phi_1^k\rangle, |\phi_2^k\rangle, \dots, |\phi_n^k\rangle)$, $|\phi_i^k\rangle = |0\rangle$, $i \in \{1, 2, \dots, n\}$, and obtains a set of quantum states $\Phi'^k = (|\phi_1'^k\rangle, |\phi_2'^k\rangle, \dots, |\phi_n'^k\rangle)$, $|\phi_i'^k\rangle = \hat{p}_i^k |\phi_i^k\rangle$, $i \in \{1, 2, \dots, n\}$.

(5) IS verifies whether the information

$$S^k = (s_1^k, s_2^k, \dots, s_n^k), s_i^k \in \{1, 2, \dots, m\}, i \in \{1, 2, \dots, n\}$$

is right or not. IS applies a set of corresponding quantum operators $\hat{S}^k = (\hat{s}_1^k, \hat{s}_2^k, \dots, \hat{s}_n^k)$ to a set of initial quantum states

$$\Phi'^k = (|\phi_1'^k\rangle, |\phi_2'^k\rangle, \dots, |\phi_n'^k\rangle), |\phi_i'^k\rangle = \hat{p}_i^k |\phi_i^k\rangle, i \in \{1, 2, \dots, n\}$$

and obtains a set of quantum states

$$\begin{aligned} \Phi''^k &= (|\phi_1''^k\rangle, |\phi_2''^k\rangle, \dots, |\phi_n''^k\rangle), \\ |\phi_i''^k\rangle &= \hat{s}_i^k \hat{p}_i^k |\phi_i^k\rangle, i \in \{1, 2, \dots, n\} \end{aligned}$$

(6) IS measures a set of quantum states

$$\begin{aligned} \Phi''^k &= (|\phi_1''^k\rangle, |\phi_2''^k\rangle, \dots, |\phi_n''^k\rangle), \\ |\phi_i''^k\rangle &= \hat{s}_i^k \hat{p}_i^k |\phi_i^k\rangle, i \in \{1, 2, \dots, n\} \end{aligned}$$

adopting rectilinear base, and obtains a set of quantum states

$$R'^k = (|r_1'^k\rangle, |r_2'^k\rangle, \dots, |r_n'^k\rangle), r_i'^k \in \{0, 1\}$$

According to the following rule: $0 \leftrightarrow |0\rangle$, $1 \leftrightarrow |1\rangle$, we can obtain n -bit random number

$$R'^k = (r_1'^k, r_2'^k, \dots, r_n'^k), r_i'^k \in \{0, 1\}.$$

(7) Comparing $R'^k = (r_1'^k, r_2'^k, \dots, r_n'^k)$, $r_i'^k \in \{0, 1\}$ with $R^k = (r_1^k, r_2^k, \dots, r_n^k)$, $r_i^k \in \{0, 1\}$. For $1 \leq i \leq n$, if $r_i'^k = r_i^k$, $i \in \{1, 2, \dots, n\}$, then identification is successful; otherwise identification is failed.

III. Security Analyses

We take quantum attack and classical one into account in order to analyse the security of the quantum identification scheme.

Quantum attack clone the string of quantum bits Φ' . The attacker needs a specially designed quantum machine which can clone the string of quantum bits Φ' . Quantum bits transmitted by the quantum channel are unknown to eavesdropper, so no-cloning theorem prevents eavesdropper from copying the string of quantum states Φ' .

Classical attack guess the user's password

$$P^k = (p_1^k, p_2^k, \dots, p_n^k), p_i^k \in \{1, 2, \dots, m\}, i \in \{1, 2, \dots, n\}$$

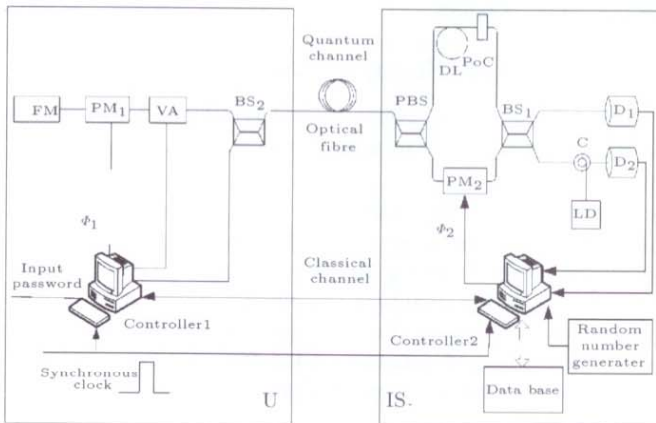
that is to say, forecast the quantum manipulations $\hat{P}^k = (\hat{p}_1^k, \hat{p}_2^k, \dots, \hat{p}_n^k)$. If \hat{p}_i^k is one of the m quantum manipulations then the probability that the eavesdropper guesses the user's password correctly is $1/m^n$ which will be 0 if IS increases m .

To sum up, the proposed scheme can efficiently prevent against eavesdropping and cheating, it is secure to quantum attack.

IV. Quantum Identification System Based on Phase Modulation

The quantum identification system based on phase modulation consists of Identification server terminal (IS) and use terminal (U). There are two kinds of information modulation methods in quantum cryptography: polarization modulation and phase modulation. The proposed identification scheme

adopts the phase modulation. The principle of M-Z interferometer is the working foundation of the quantum identification scheme based on phase modulation. A laser pulse emitted by Laser diode (LD) is separated at 50/50 beam splitter (BS₁). The short arm includes a phase modulator (PM₂), the long arm includes a Delay line (DL) and a Polarization controller (PoC). The linear polarization of the pulse is turned by 90° in long arm, so two pulses exit from the Polarization beam splitter (PBS) in the same port. The pulses travel down to U, are reflected on a Faraday mirror (FM), attenuated and come back orthogonally polarized. In turn, both pulses now take the other path at IS and arrive at the same time at BS₁ where they interfere. Then they are detected either in D₁, or in D₂. Since the two pulses take the same path, inside IS in reversed order, this interferometer is auto-compensated. To implement quantum identification scheme, U applies phase shift Φ_1 on the first pulse with PM₁. IS applies the phase shift Φ_2 on the second pulse with PM₂ on its way back. The probability that single photon detector (D₁) detects the photon is $P_1 = \cos^2 \left| \frac{\Phi_1 - \Phi_2}{2} \right|$, while the probability that single photon detector (D₂) detects the photon is $P_2 = \sin^2 \left| \frac{\Phi_1 - \Phi_2}{2} \right|$. Here Φ_1 is the modulated phases by UIC and PM₁ respectively, Φ_2 is the modulated phases by PM₂, then



LD: diode laser; C: Circulator; D₁, D₂: single photon detector; BS₁, BS₂: beam splitter; PoC: polarization controller; DL: delay line; PBS: polarization beam splitter; VA: variable attenuator; PM₁, PM₂: phase modulator; FM: Faraday mirror; Controller 1, Controller 2: main controller.

Fig. 2. Experimental set-up of quantum identification system

If $\Phi_1 - \Phi_2 = \pi/2 + n\pi$, then $P_1 = P_2 = 1/2$;

If $\Phi_1 - \Phi_2 = 0$, then $P_1 = 1, P_2 = 0$;

If $\Phi_1 - \Phi_2 = \pi$, then $P_1 = 0, P_2 = 1$.

Controller1 controls PM₁ according to the user's password. Controller2 controls PM₂ according to the users' registry information in users' database. Controller1 communicates with Controller2 by classical channel. Synchronous clock generator synchronizes Controller1 with Controller2. Random number generator produces random number for Controller2. The users' database stores the users' registry information. The proposed scheme includes a registry phase and an identification

phase.

1. Registration phase

(1) The user U^k applies for the registration and sets up the password.

The user U^k sets up the password $P^k = (p_1^k, p_2^k, \dots, p_n^k)$, $p_i^k \in \{0, 1\}$, $i \in \{1, 2, \dots, n\}$, p_i^k drives PM₁ during the i th time slot and changes the laser pulse's phase with an angle Φ_{1i}^k , Φ_{1i}^k corresponds to p_i^k . The password P^k is transmitted to IS by quantum key distribution (for example BB84 protocol^[2]) or secure channel. Then IS knows the corresponding angle $\Phi_1^k = (\Phi_{11}^k, \Phi_{12}^k, \dots, \Phi_{1n}^k)$. Both IS and U don't know the key during quantum key distribution, they gain the key after finishing quantum key distribution.

(2) IS builds the corresponding user's registry information in users' database.

Random number generator produces the random number $R^k = (r_1^k, r_2^k, \dots, r_n^k)$, $r_i^k \in \{0, 1\}$, $i \in \{1, 2, \dots, n\}$ needed by IS. IS adjusts PM₂ during the i th time slot and changes the laser pulse's phase with an angle Φ_{2i}^k subjected to the following conditions:

For $1 \leq i \leq n$,

if $r_i^k = 0$, then $\Phi_{1i}^k - \Phi_{2i}^k = 0$, that is to say, D₁ can detect single photon.

if $r_i^k = 1$, then $\Phi_{1i}^k - \Phi_{2i}^k = \pi$, that is to say, D₂ can detect single photon.

We can obtain a set of random phases

$$\Phi_2^k = (\Phi_{21}^k, \Phi_{22}^k, \dots, \Phi_{2n}^k)$$

corresponding to $R^k = (r_1^k, r_2^k, \dots, r_n^k)$.

(3) IS builds the user U^k file in the user database.

File name: U^k

File Content:

$$R^k = (r_1^k, r_2^k, \dots, r_n^k) \text{ and } \Phi_2^k = (\Phi_{21}^k, \Phi_{22}^k, \dots, \Phi_{2n}^k)$$

(4) Repeat steps (1)-(3), IS can build many users' registry information in the users' database. The random number must be subjected to the following condition:

$$\text{If } i \neq j, \text{ then } R^i = (r_1^i, r_2^i, \dots, r_n^i) \neq R^j = (r_1^j, r_2^j, \dots, r_n^j).$$

2. Identification phase

(5) The user applies for the identification, IS searches the file U^k in the users' database.

If the user U^k wants to enter IS, he tells IS the filename U^k via the classical channel. He inputs his password. IS finds the file U^k according to filename U^k :

$$U^k : R^k = (r_1^k, r_2^k, \dots, r_n^k) \text{ and } \Phi_2^k = (\Phi_{21}^k, \Phi_{22}^k, \dots, \Phi_{2n}^k)$$

(6) IS verifies the user U^k identity information.

The user U^k inputs the password p_i^k during the i th time slot. p_i^k changes the laser pulse's phase with an angle Φ_{1i}^k . PM₂ controlled by controller2 changes the laser pulse's phase with an angle Φ_{2i}^k further.

(7) IS detects quasi-single photon and verifies the user U^k identity.

Monitoring single photon detectors (D₁ and D₂), IS gains the classical bit r_i^k according to the following rule:

If D₁ detects photon, then $r_i^k = 0$; If D₂ detects photon, then $r_i^k = 1$.

Repeat steps (5)-(7), for $1 \leq i \leq n$, if $r_i^k = r_i^k$, $i \in \{1, 2, \dots, n\}$, then identification is successful; otherwise identification is failed.

V. Conclusions

A quantum identification scheme based on the manipulation of quantum state is proposed in this paper. This scheme can verify the identity of the legitimate user, and can prevent the eavesdropper from impersonating the legitimate user. The quantum states transmitted by the quantum channel are unknown to the eavesdropper, so this scheme is absolutely secure to quantum attack according to no-cloning theorem. In addition, a quantum identification experimental scheme based on phase modulation is designed in order to implement the proposed quantum identification scheme.

References

- [1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, "Quantum cryptography", *Reviews of Modern Physics*, Vol.74, pp.145-195, 2002.
- [2] C.H. Bennett, G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing", *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pp.175-179, 1984.
- [3] B. Schumacher, M.D. Westmoreland, "Quantum privacy and quantum coherence", *Physical Review Letters*, Vol.80, pp.5695-5697, 1998.
- [4] P.W. Shor, J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol", *Physical Review Letters*, Vol.85, pp.441-444, 2000.
- [5] M. Hillery, V. Buzek, A. Berthiaume, "Quantum secret sharing", *Physical Review A*, Vol.59, pp.1829-1834, 1999.
- [6] G. Zeng, W. Zhang, "Identity verification in quantum key distribution", *Physical Review A*, Vol.61, pp.022303-1-5, 2000.
- [7] A. Kent, "Unconditionally secure bit commitment", *Physical Review Letters*, Vol.83, pp.1447-1450, 1999.
- [8] H.K. Lo, H.F. Chau, "Unconditional security of quantum key distribution over arbitrary long distances", *Nature*, Vol.283, pp.2050-2056, 1999.
- [9] D. Mayers, "Unconditional security in quantum cryptography", *Journal of the ACM*, Vol.48, No.3, pp.351-406, 2001.
- [10] C. Kurtsiefer *et al.*, "Quantum cryptography: A step towards global key distribution", *Nature*, Vol.419, pp.450-450, 2002.
- [11] D. Stucki, N. Gisin *et al.*, "Quantum key distribution over 67km with a plug & play system", *New Journal of Physics*, Vol.4, pp.41.1-41.8.
- [12] M. Dušek, O. Haderka *et al.*, "Quantum identification system", *Physical Review A*, Vol.60, No.1, pp.149-154, 1999.
- [13] D. Ljunggren, M. Bourennane, A. Karlsson, "Authority-based user authentication in quantum key distribution", *Physical Review A*, Vol.62, pp.022305-1-7, 2000.
- [14] M. Curty, D. Santos, "Quantum authentication of classical messages", *Physical Review A*, Vol.64, pp.062309-1-6, 2001.
- [15] A. Fujiwara, "Quantum channel identification problem", *Physical Review A*, Vol.63, pp.042304-1-4, 2001.
- [16] T. Mihara, "Quantum identification schemes with entanglements", *Physical Review A*, Vol.65, pp.052326-1-4, 2002.
- [17] M. Curty *et al.*, "Qubit authentication", *Physical Review A*, Vol.66, pp.022301-1-4, 2002.



HE Guangqiang received the M.S. degree from Huazhong University of Science and Technology in 2002. He is currently working toward the Ph.D. degree at Shanghai Jiaotong University. His current research interests include quantum communication and quantum information. (Email: gqhe@sjtu.edu.cn.)

ZENG Guihua received the Ph.D. degree in 1997 from Shanghai Institute of Optics and Fine Mechanics, Chinese Academy of Sciences (CAS), China. He is a professor in Electronic Engineering Department of Shanghai Jiaotong University. His current research interests are in quantum information system, communication security and video-database security.