Vol 15 No 2, February 2006
1009-1963/2006/15(02)/0371-04

Chinese Physics

A secure identification system using coherent states*

He Guang-Qiang(何广强)† and Zeng Gui-Hua(曾贵华)

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

(Received 19 December 2004; revised manuscript received 6 July 2005)

A quantum identification system based on the transformation of polarization of a mesoscopic coherent state is proposed. Physically, an initial polarization state which carries the identity information is transformed into an arbitrary elliptical polarization state. To verify the identity of a communicator, a reverse procedure is performed by the receiver. For simply describing the transformation procedure, the analytical methods of Poincaré sphere and quaternion are adopted. Since quantum noise provides such a measurement uncertainty for the eavesdropping that the identity information cannot be retrieved from the elliptical polarization state, the proposed scheme is secure.

Keywords: quantum identification, polarization encryption and decryption, quantum noise, Poincaré sphere

PACC: 4250, 4230Q, 0365

1. Introduction

In the past two decades, quantum key distribution (QKD) has attracted much attention.[1−5] However, the so-called man-in-middle attack strategy[6,7] becomes an obstacle to application of QKD in practice. Quantum identity authentication[8,9] is an important way to circumvent this kind of attack strategy. Recently, lots of quantum identity authentication schemes have been presented. Experimentally, quantum identity authentication schemes as well as QKD are implemented by two approaches, i.e. single photon approach and quantum continuous variable approach. Since the difficulties in generating and detecting single photon, a faint laser beam acts as an approximate substitution. The most favourable quantum signal in experiments for quantum cryptography is the quantum continuous variable.[10] Especially, the mesoscopic coherent state (MCS) of light has been employed to obtain secure key distribution.[11,12]

In Section 2, the new quantum identification protocol is introduced in detail. We extend the linear polarization modulation of MCS [11,12] to the arbitrary elliptical polarization modulation. In Section 3, the experimental set-up is presented. In Section 4, the polarization encryption and decryption are analysed by utilizing the intuitive and simple analytical methods of Poincaré sphere and quaternion. In Section 5, the security of protocol is discussed. Conclusions are drawn in Section 6.

2. Quantum identification protocol

Firstly, we describe briefly the protocol. Let Alice and Bob be two communicators, and employ the MCS of light as the quantum signal. As usual, suppose Alice and Bob pre-share a private key k which consists of binary bits, i.e. $k = (k_1, k_2, k_3)$, where $k_1 = (k_1^1, k_1^2, \cdots, k_1^l)$, $k_2 = (k_2^1, k_2^2, \cdots, k_2^m)$ and $k_3 = (k_3^1, k_3^2, \cdots, k_3^n)$. The lengths l, m and n are chosen according to $m/l = r$ and $n/l = s$ where r and s are integers. The protocol executes in the following steps.

In Step 1, divide the strings k_2 and k_3 equally into l groups each with r and s bits, respectively. In Step 2, create p_i and q_i according to the following way: $p_i = a_{i_r} 2^{r-1} + a_{i_{r-1}} 2^{r-2} + \cdots + a_{i_1}$, and $q_i = b_{i_s} 2^{s-1} + b_{i_{s-1}} 2^{s-2} + \cdots + b_{i_1}$, where $a_{i_j} (j = 1, \cdots, r)$ and $b_{i_k} (k = 1, \cdots, s)$ are elements of the ith group in k_2 and k_3, respectively, and $i = 1, 2, \cdots, l$. In Step 3, calculate Φ_{p_i} and Θ_{q_i} from $\Phi_{p_i} = 2\pi p_i / 2^r$ and $\Theta_{q_i} = \pi q_i / 2^s$. In Step 4, encode k_1 into polarization states of MCS. Thus a

*Project supported by the National Natural Science Foundation of China (Grant No 60472018).

†E-mail: gqhe@sjtu.edu.cn

string of encoded polarization states $\left|\Psi(k_1^i\pi, k_1^i\pi)\right\rangle$ is obtained. In Step 5, construct a rotation operator $R_i = R(\Phi_{p_i}, \Theta_{q_i})$ by employing Φ_{p_i} and Θ_{q_i} as rotation angles. In Step 6, apply the operator R_i to the polarization state $\left|\Psi(k_1^i\pi, k_1^i\pi)\right\rangle$. Thus one obtains $\left|\Psi(k_1^i\pi + \Phi_{p_i}, k_1^i\pi + \Theta_{q_i})\right\rangle$ at $p_i + q_i$ being the odd number, and $\left|\Psi((k_1^i \oplus 1)\pi + \Phi_{p_i}, (k_1^i \oplus 1)\pi + \Theta_{q_i})\right\rangle$ at $p_i + q_i$ being the even number. In Step 7, apply R^{-1} to the resulting state. Thus the receiver judges the polarization according to the parity of $p_i + q_i$. If the k_1 can be obtained, the sender's identity is true, otherwise, it is false.

3. Experimental set-up

The proposed scheme may be experimentally implemented by the set-up illustrated in Fig.1. The quantum signal employed in this scheme is the MCS of light, which is created by DFB laser. After the MCS is generated, the quantum signal is modulated by changing the voltage of the polarization encoder (PE) controlled by the string k_1. The horizontal and vertical polarization states are encoded into bit 0 and bit 1, i.e. $0 \leftrightarrow \left|\Psi(0,0)\right\rangle$ and $1 \leftrightarrow \left|\Psi(\pi,\pi)\right\rangle$ respectively. Alice's main-controller controls the dynamical polarization controller (DPC) 1 to transform the encoded polarization states into arbitrary elliptical polarization states according to the pre-shared binary strings k_2 and k_3. After the quantum signal reaches Bob's side, the DPC2 transforms the elliptical polarization states into the original polarization states controlled by the main-controller 2 according to the strings k_2 and k_3.

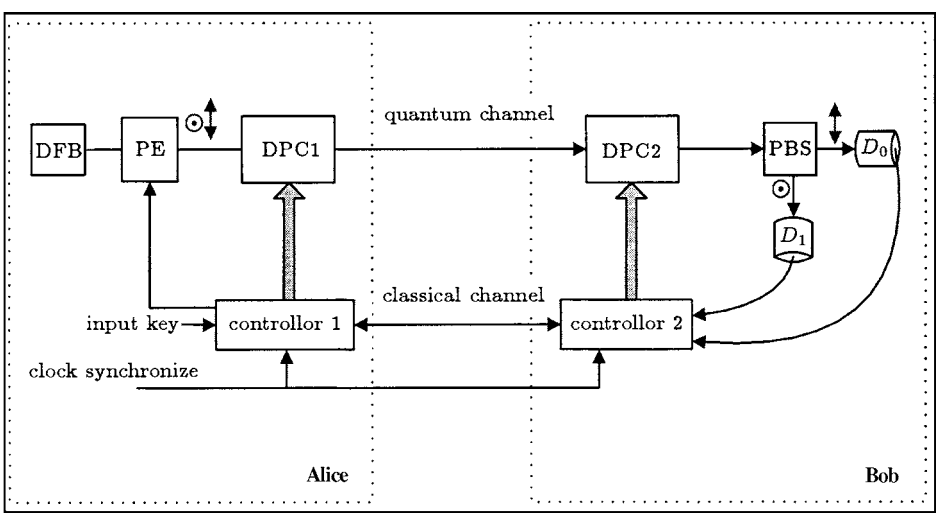

Fig.1. Basic scheme for quantum identification system.

There are two components in the output signal of DPC2, i.e. the horizontal and vertical polarization states, they are separated by the polarization beam splitter (PBS). Finally, the optical signal is detected by the PIN detectors D_0 and D_1 and the data are input into the main-controller 2.

4. Polarization encryption and decryption

For understanding clearly the proposed scheme, we give a brief theoretical description of the final two steps, i.e. Step 6 and Step 7. In Step 6, the initial polarization state is transformed into an arbitrary elliptical polarization state, which is actually a polarization encryption procedure. Step 7 is a reverse process

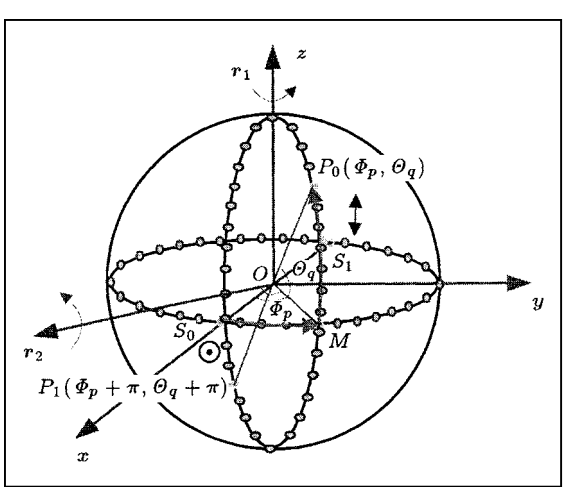

Fig.2. Polarization encryption and decryption.

of Step 6, therefore it is actually a decryption procedure. Since the encryption and decryption procedures are implemented by coherent light, these procedures can be described by employing the well-known Poincaré sphere shown in Fig.2.

In general, any polarization state of coherent light corresponds to a point $P(\Phi_p, \Theta_q)$ on the Poincaré sphere, whose longitude and latitude are $\Phi_p = 2\pi p/2^r$ and $\Theta_q = \pi q/2^s$ respectively. The point $P(\Phi_p, \Theta_q)$ can be converted into an arbitrary point $P(\Phi_s, \Theta_t)$ by a proper rotation operation R. In the proposed scheme, the rotation is physically implemented by the DPC. The Jones matrix of the DPC can be expressed by the Euler parameters as follows:[13]

$$T = \begin{pmatrix} \cos\left(\frac{\delta}{2}\right) - \mathrm{i}\sin\left(\frac{\delta}{2}\right) r_x & \sin\left(\frac{\delta}{2}\right)(-\mathrm{i}r_y + r_z) \\ -\sin\left(\frac{\delta}{2}\right)(\mathrm{i}r_y + r_z) & \cos\left(\frac{\delta}{2}\right) + \mathrm{i}\sin\left(\frac{\delta}{2}\right) r_x \end{pmatrix}. \tag{1}$$

The matrix T represents a rotation through an angle δ about the axis identified by the unit vector $\boldsymbol{r} = (r_x, r_y, r_z)$, i.e. the device fast axis; left-hand rotations are considered positive. A more compact notation for rotations is the unit quaternion,[14] which can be written as

$$Q = \left\{ \cos\left(\frac{\delta}{2}\right), \sin\left(\frac{\delta}{2}\right)\boldsymbol{r} \right\}. \tag{2}$$

Using the quaternion Q, a rotation of a point $s = (s_x, s_y, s_z)$ represented by the quaternion $\{0, s\}$ is

$$\{0, s_{\text{rotated}}\} = Q^{-1} * \{0, s\} * Q, \tag{3}$$

where the symbol "*" represents quaternion multiplication.

In the proposed scheme, after the identity information k_1 has been encoded into the initial polarization states, the DPC1 is employed in Step 6 to encrypt the initial polarization states into ciphertext states, which are arbitrary elliptical polarization states, according to the pair of number (p_i, q_i). Subsequently, $\left|\Psi(k_1^i\pi, k_1^i\pi)\right\rangle$ is mapped into $\left|\Psi(k_1^i\pi + \Phi_{p_i}, k_1^i\pi + \Theta_{q_i})\right\rangle$ when $p_i + q_i$ is an odd number, and is mapped into $\left|\Psi((k_1^i \oplus 1)\pi + \Phi_{p_i}, (k_1^i \oplus 1)\pi + \Theta_{q_i})\right\rangle$ when $p_i + q_i$ is an even number.

In the case of $p_i + q_i$ being an odd number, two steps need to be executed, which are illustrated in Fig.2. Firstly, rotate through an angle Φ_{p_i} counterclockwise about the axis $\boldsymbol{r}_1 = (0, 0, 1)$, then an arbitrary point S on the equator (in the Fig.2 implies S_0 and S_1) will move to the point M along SM. The quaternion Q_1 representing this rotation operation is

$$Q_1 = \left\{ \cos\left(\frac{\Phi_{p_i}}{2}\right), \sin\left(\frac{\Phi_{p_i}}{2}\right)\boldsymbol{r}_1 \right\}. \tag{4}$$

Secondly, rotate through an angle Θ_{q_i} counterclockwise about the axis $\boldsymbol{r}_2 = (\sin\Phi_{p_i}, -\cos\Phi_{p_i}, 0)$, then the point M will move to the point P along MP. The quaternion Q_2 representing this rotation operation is

$$Q_2 = \left\{ \cos\left(\frac{\Theta_{q_i}}{2}\right), \sin\left(\frac{\Theta_{q_i}}{2}\right)\boldsymbol{r}_2 \right\}. \tag{5}$$

The Poincaré vectors of the initial polarization state and the point $P(\Phi_{p_i}, \Theta_{q_i})$ are OS and OP, respectively. Employing Eqs.(3), (4) and (5) yields

$$\{0, OP\} = \{Q_2 * Q_1\}^{-1} * \{0, OS\} * \{Q_2 * Q_1\}. \tag{6}$$

If the initial state is a horizontal polarization state, i.e. $OS = OS_0 = (1, 0, 0)$, Eq.(6) gives

$$OP = OP_0 = (\cos\Theta_{q_i}\cos\Phi_{p_i}, \cos\Theta_{q_i}\sin\Phi_{p_i}, \sin\Theta_{q_i}). \tag{7}$$

While $OS = OS_1 = (-1, 0, 0)$ that corresponds to an initially vertical polarization state, and Eq.(6) yields

$$\begin{aligned} OP = OP_1 = (&-\cos\Theta_{q_i}\cos\Phi_{p_i}, \\ &-\cos\Theta_{q_i}\sin\Phi_{p_i}, -\sin\Theta_{q_i}). \end{aligned} \tag{8}$$

For the condition of $p_i + q_i$ being an even number, one can obtain a corresponding Poincaré vector in a similar way. Therefore, by employing the number-pair (p_i, q_i) that is calculated in Step 2, an angle pair $(\Phi_{p_i}, \Theta_{q_i})$ can be obtained in Step 3. Subsequently, an initial polarization state $\left|\Psi(k_1^i\pi, k_1^i\pi)\right\rangle$ can be encrypted into a ciphertext, i.e. an arbitrary elliptical polarization state described by the point $P(\Phi_{p_i}, \Theta_{q_i})$, in Step 6.

Step 7 is a reverse operation of Step 6. Thus, this step is, in cryptography, a decryption procedure. To transform the elliptical polarization state into the original polarization state $\left|\Psi(k_1^i\pi, k_1^i\pi)\right\rangle$, Bob performs a

reverse rotation R^{-1} on the vector OP. This operation gives

$$\{0, OS'\} = \{Q_1^{-1} * Q_2^{-1}\}^{-1} * \{0, OP\} * \{Q_1^{-1} * Q_2^{-1}\}, \quad (9)$$

where Q_1^{-1} and Q_2^{-1} are the reverse of quaternities Q_1 and Q_2 respectively. In details, Q_2^{-1} represents the rotation operation of rotating through an angle Θ_{q_i} clockwise about the axis $\boldsymbol{r}_2 = (\sin \Phi_{p_i}, -\cos \Phi_{p_i}, 0)$. After this rotation, the point P moves to the point M along PM. Q_1^{-1} represents the rotation operation of rotating through an angle Φ_{p_i} clockwise about the axis $\boldsymbol{r}_1 = (0, 0, 1)$. Subsequently, the point M moves to the point S' along MS'.

One can easily obtain the following results from Eq.(9). When $p_i + q_i$ is an odd number, if one obtains $OS' = (1, 0, 0)$, then it means an initial polarization state $|\Phi(0, 0)\rangle$. If one obtain $OS' = (-1, 0, 0)$, then it implies an initial polarization state $|\Phi(\pi, \pi)\rangle$. For the case of $p_i + q_i$ being an even number, one can obtain a corresponding OS'. According to the encoding rules: $0 \leftrightarrow |\Psi(0, 0)\rangle$ and $1 \leftrightarrow |\Psi(\pi, \pi)\rangle$, Bob attains a binary string. If this string is the same as the k_1, Alice's identity is true. Otherwise it is false.

5. Security analysis

Now we move to the security of the proposed scheme. The overlap $|\langle \Psi(\Phi_j, \Theta_k)|\ \Psi(\Phi_p, \Theta_q)\rangle|^2$ between states $|\Psi(\Phi_j, \Theta_k)\rangle$ and $|\Psi(\Phi_p, \Theta_q)\rangle$ gives

$$|\langle \Psi(\Phi_j, \Theta_k)|\ \Psi(\Phi_p, \Theta_q)\rangle|^2 \approx \exp\left[-\frac{(\Phi_j - \Phi_p)^2 + (\Theta_k - \Theta_q)^2}{2 \times \frac{1}{\langle n \rangle}}\right]. \quad (10)$$

The above equation defines the uncertainty of polarization angle generated by the shot noise associated with the coherent states. $\sigma^2 = \frac{1}{\langle n \rangle}$ is the uncertainty associated with light's shot noise. We stress here that σ cannot be overcome regardless of one's precise measurement capabilities.[11,12] Without knowing the precise basis sent, an eavesdropper cannot obtain the sent bits. The number of bases N_σ within σ is $N_\sigma = 2^{r+s}\sigma^2/\pi^2 = 2^{r+s}/(\pi^2 \langle n \rangle)$. To warrant the security of the proposed scheme, N_σ will introduce more complexity into the scheme. Thus a proper N_σ is necessary for designing an optimal scheme.

The minimum probability of error for an eavesdropping can be made arbitrarily close to $\frac{1}{2}$ for a fixed average number of photons $|\alpha|^2$ with r and s increasing, where α is the amplitude of the coherent state. However, the probability of error for the receiver is $P_e^{\rm svr} = \frac{1}{2}(1 - \sqrt{1 - \exp(-2T|\alpha|^2)})$, where T is transmissivity of the channel.[11,12] For large $|\alpha|^2$, $P_s^{\rm svr}$ may be negligible since it approaches zero. In this situation, the received quantum signal can be recovered excellently by the legitimate receiver.

6. Conclusion

In conclusion, a quantum identification system based on polarization modulation of mesoscopic coherent light is proposed. First, the MCS of light is modulated by a pre-shared key k_1 into a horizontal and vertical polarization states. Then the initial polarization state is encrypted into an arbitrary polarization state, which is then sent to Bob. To verify Alice's identity, Bob decrypts the received MCS, and obtains finally a binary string which should be the same as the pre-shared key k_1 if the sender's identity is true. The analytical methods of Poincaré sphere and quaternion are adopted. The security of the scheme is guaranteed by the quantum noise of coherent light. Especially, the security may be improved by increasing the number-pair (p_i, q_i). In practice, the proposed scheme can be implemented in fibre or free-space.

References

[1] Bennett C H and Brassard G *1984 Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India) 175–179
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[4] Gisin N Ribordy G Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[5] Liang C, Fu D H, Liang B, Liao J, Wu L AN, Yao D C and Lü S W 2001 *Acta Phys. Sin.* **50** 1429 (in Chinese)
[6] Zeng G H and Zhang W P 2000 *Phys. Rev.* A **61** 2303
[7] Lo H K and Chau H F 1999 *Science* **283** 2050
[8] Dusek M, Haderka O, Hendrych M and Myska R 1999 *Phys. Rev.* A **60** 149
[9] He G Q and Zeng G H 2005 *Chin. Phys.* **14** 541
[10] Grosshans F, Assche G V, Wenger J, Brourl R, Cerf N J and Grangler P 2003 *Nature* **421** 238
[11] Barbosa G A, Corndorf E, Kumar P and Yuen H P 2003 *Phys. Rew. Lett.* **90** 227901
[12] Barbosa G A 2003 *Phys. Rev.* A **68** 052307
[13] Martinelli M and Chipman R A 2003 IEEE*J. Lightwave Technol.* **21** 2089
[14] Kuipers J B 1999 *Quaternions and Rotation Sequences* (Princeton, NJ: Princeton University Press)