文章编号：0258-7025(2007)07-0924-06

可光纤集成的相干态量子身份认证系统

何广强[1]，曾贵华[1]，朱 俊[1]，张哲珅[1]，王 倩[1]，周晓奇[1]，钱旭东[1]，彭进业[2]

([1] 上海交通大学电子工程系区域光纤通信网与新型光通信系统国家重点实验室，上海 200240
[2] 西北大学电子工程系，陕西 西安 710069)

摘要 报道了可光纤集成相干态量子身份认证实验系统。该系统采用偏振相干态的斯托克斯矢量作为量子信号载体，采用动态偏振控制器作为信号调制器，利用固有的相干态量子噪声保证系统的安全性。自行设计了脉冲激光驱动电路、微弱窄脉冲激光探测电路、信号同步模块，采用 Socket 网络通信程序在 TCP/IP 局域网中实现了量子保密通信所需要的经典通信。该相干态量子身份认证系统采用的运行密钥为 12 位，每个光脉冲包含 40000 个光子，传输速率达到8 kbit/s，合法用户间误码率(BER)小于 10^{-4}。每传输一个比特信息，攻击者所能窃取的信息量 $I(\mathrm{Alice},\mathrm{Eve})<10^{-14}$ bit。

关键词 量子光学；量子密码；量子身份认证；动态偏振控制器；相干态量子噪声

中图分类号 O 431.2；TN 911.74 **文献标识码** A

An Integrable Optic-Fiber Coherent State Quantum Identification System

HE Guang-qiang[1], ZENG Gui-hua[1], ZHU Jun[1], ZHANG Zhe-shen[1], WANG Qian[1], ZHOU Xiao-qi[1], QIAN Xu-dong[1], PENG Jin-ye[2]

([1] *State Key Laboratory on Fiber-Optic Local Area Networks and Advanced Optical Communication Systems, Department of Electronics Engineering, Shanghai Jiaotong University, Shanghai, 200240, China*
[2] *Department of Electronics Engineering, Northwest University, Xi'an, Shaanxi 710069, China*)

Abstract An integrable optic-fiber coherent state quantum identification system is presented. In the scheme, the Stokes vectors of polarization coherent state are employed as quantum signal carrier, the dynamic polarization controller serves as a modulation device, and the inherent quantum noise guarantees the security. The driving circuit of laser pulses, detection circuit for weak narrow laser pulses, and signal synchronous module, are self-designed. Classical communication needed by quantum secret communication is implemented by Socket network communication program running on the TCP/IP local area network. The running key employed in the system is 12 bit. The transmission rate of identity picture is 8 kbit/s, the bit error rate between legal users is less than 10^{-4}, and the information $I(\mathrm{Alice},\mathrm{Eve})$ per bit obtained by an attacker is less than 10^{-14}.

Key words quantum optics; quantum cryptography; quantum identification; dynamic polarization controller; quantum noise of coherent state

1 引 言

量子密码[1~6]是一种基于量子物理与经典密码学的新兴密码体制，其安全性由量子物理的基本规律保证[7~9]。然而，所谓的中间人攻击成为量子密码(量子密钥分发)的主要障碍之一。量子身份认证是克服中间人攻击的一种有效手段。最近学术界提出了多种量子身份认证方案[10~14]。实验上，量子密钥分发和量子身份认证主要有两种量子载波：单光子和连续变量载波。因为单光子的产生和检测在技

收稿日期：2006-11-27；收到修改稿日期：2007-02-27

基金项目：国家自然科学基金(60472018)，2006 年度上海交通大学青年教师校内科研启动基金(A2831B)，“十一五”国防基础科研项目(A3220061163)和上海交通大学第 11 期 PRP 项目(T03011030)资助课题。

作者简介：何广强(1977—)，男，山东人，讲师，主要从事连续变量量子信息与量子通信研究。E-mail：gqhe@sjtu.edu.cn

导师简介：曾贵华(1966—)，男，湖南人，教授，博士生导师，主要从事密码学、网络与通信安全、多媒体检索等方面的研究。E-mail：ghzeng@sjtu.edu.cn

术上存在较大的困难，目前主要采用微弱激光脉冲近似单光子。微弱激光脉冲所包含的平均光子数为0.1。相对于离散变量，连续变量在实验上容易实现产生和检测，操作也非常容易，通信容量大，因此连续变量载波是量子信息处理的一种非常有竞争力的处理方法[15]，引起了各国学者的关注，已经成为量子信息领域的研究热点。最近美国西北大学采用相干态在光纤通信网络上实现了高速的量子密钥分发(扩张)[16~21]。

本文提出了一种基于相干态的量子身份认证协议，通过把庞加莱球一个大圆上的偏振态推广到整个庞加莱球球面上，来提高系统的安全性。在美国西北大学方案的基础上，采用动态偏振器代替相位调制器对实验方案进行了改进，可把初始偏振态加密为任意的椭圆偏振态，并自行设计了脉冲激光发射模块、偏振调制/解调模块、微弱窄脉冲激光探测模块以及同步模块，详细介绍了该实验系统的工作过程，给出了实验结果。

2　实验方案

简单介绍相干态量子身份认证协议[14]。假设通信双方 Alice 和 Bob 采用相干态作为量子信号，并且已经通过安全方式(如 BB84 量子密钥分发方案或安全信使)共享了认证密钥 k。$k=(k_1,k_2,k_3)$ 为二进制比特串，k_1 表示认证信息，如请求认证者的照片等，k_2 和 k_3 表示为加密认证信息 k_1 采用的原始密钥，$k_1=(k_1^1,k_1^2,\cdots,k_1^l)$，$k_2=(k_2^1,k_2^2,\cdots,k_2^m)$，$k_3=(k_3^1,k_3^2,\cdots,k_3^n)$，比特串 k_2，k_3 的长度 m，n 是比特串 k_1 长度 l 的整数倍，即满足关系 $\frac{m}{l}=r$，$\frac{n}{l}=s$，r，s 均为整数。该协议运行为：

1) 把比特串 k_2 分为 l 组，每组 r 个比特。把比特串 k_3 分为 l 组，每组 s 个比特。

2) 分别把 k_2，k_3 的第 i^{th} 组二进制比特串转化为十进制数 p_i，q_i，即

$$p_i=a_{i_r}2^{r-1}+a_{i_{r-1}}2^{r-2}+\cdots+a_{i_1},$$

$$q_i=b_{i_s}2^{s-1}+b_{i_{s-1}}2^{s-2}+\cdots+b_{i_1}, \quad (1)$$

式中 a_{i_j} $(j=1,2,\cdots,r)$ 和 b_{i_k} $(k=1,2,\cdots,s)$ 分别为 k_2，k_3 的第 i^{th} 组二进制比特串中的元素，$i=1,2,\cdots,l$。

3) 根据公式(1) 计算 Φ_{p_i}，Θ_{q_i}

$$\Phi_{p_i}=\frac{2\pi p_i}{2^r},\quad \Theta_{q_i}=\frac{2\pi q_i}{2^s}。 \quad (2)$$

4) 把二进制比特串 k_1 编码为相干态光束的偏振态，得到一串相干态偏振态载波 $|\Psi(k_1^i\pi,k_1^i\pi)\rangle$，$i=1,2,\cdots,l$。

5) 采用 Φ_{p_i}，Θ_{q_i} 作为旋转角构造旋转算符 $R=R(\Phi_{p_i},\Theta_{q_i})$。

6) 如图 1 所示，应用旋转算符 $R=R(\Phi_{p_i},\Theta_{q_i})$ 于偏振态 $|\Psi(k_1^i\pi,k_1^i\pi)\rangle$，当 p_i+q_i 为奇数时，得到 $|\Psi(k_1^i\pi+\Phi_{p_i},k_1^i\pi+\Theta_{q_i})\rangle$；当 p_i+q_i 为偶数时，得到 $|\Psi[(k_1^i\oplus 1)\pi+\Phi_{p_i},(k_1^i\oplus 1)\pi+\Theta_{q_i}]\rangle$。

7) 接收者 Bob 应用旋转算符的逆算符 R^{-1} 作用于接收到的偏振态，并结合 p_i+q_i 的奇偶性来判断解调偏振态所携带的比特值。

最后，如果收到的比特值与 k_1 完全一致，则发送者为合法通信者 Alice，否则，则认证失败，通信者为非法用户。

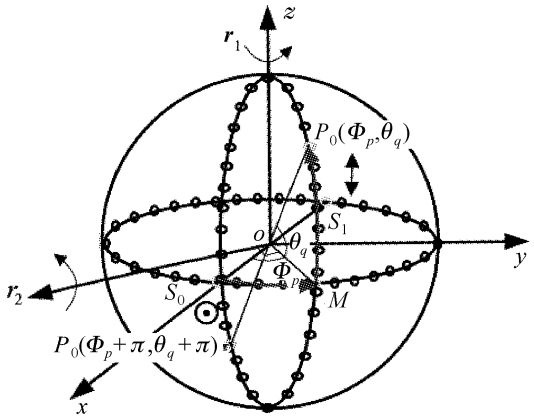

图 1　偏振加/解密变换

Fig. 1　Polarization encoding/decoding transform

从图 1 可以看出，Φ_p 和 Θ_q 分别表示偏振态对应点的经度和纬度，(Φ_p,Θ_q) 表示球面上的任意一点，即表示任意的偏振态。采用不同的运行密钥，也就是用不同的 (p_i,q_i) 可以把初始态变换为任意椭圆偏振态。

实验中，采用动态偏振控制器(PCD-002-4X-FC/PC-7-C)作为偏振调制器件，该器件原理上可以把任意的椭圆偏振态变换为另一任意椭圆偏振态。然而，同时调节动态偏振控制器的两个端口产生的应力双折射并不服从我们所期望的线性关系。所以在实验中，首先设定 $\Phi_p=\pi/2$，通过调节 Θ_q 实现偏振变换，这意味着把 k_2 作为定值，只通过密钥 k_3 加密认证信息。直接调节动态偏振控制器的端口 2，其余端口均设为定值，即可完成此功能。在此情况下，入射的相干态可以表示为

$$|\psi_m\rangle=|\alpha\rangle_{\perp}\otimes|\alpha e^{i\theta_{qm}}\rangle_{/\!/},$$

$$|\psi_n\rangle = |\alpha\rangle_{\perp} \otimes |\alpha e^{i\theta_{qn}}\rangle_{/\!/}, \tag{3}$$

相干态$|\psi_m\rangle$和$|\psi_n\rangle$相重合的程度可以用保真度衡量

$$\begin{aligned} F = P_{\theta_m}(\theta_n) &= |\langle\psi_m|\psi_n\rangle|^2 = \\ &|_{/\!/}\langle\alpha e^{i\theta_m}|\otimes_{\perp}\langle\alpha|\alpha\rangle_{\perp}\otimes|\alpha e^{i\theta_n}\rangle_{/\!/}|^2 = \\ &\exp(-|\alpha e^{i\theta_m} - \alpha e^{i\theta_n}|^2) = \\ &\exp\{-\langle n\rangle[1-\cos(\theta_m-\theta_n)]\} = \\ &\exp\left[-\frac{(\theta_n-\theta_m)^2}{2(1/\langle n\rangle)}\right], \end{aligned} \tag{4}$$

式中$\langle n\rangle = 2|\alpha|^2$为平均光子数。可见，量子态$|\psi_m\rangle$与$|\psi_n\rangle$之间的保真度，即相干态$|\psi_n\rangle$与相干态$|\psi_m\rangle$的近似程度，服从以$\theta_m$为均值，以$\sigma^2 = 1/\langle n\rangle$为方差的高斯分布。在$\sigma$的范围内包含的偏振相干态的个数为

$$N_\sigma = \sigma\Big/\frac{\pi}{M} = \frac{M\sigma}{\pi} = \frac{M}{\pi\sqrt{\langle n\rangle}}, \tag{5}$$

式中$M = 2^r$，理论分析表明[11~16]N_σ与方案的安全性密切相关，它直接决定了窃听者 Eve 所能获得的信息量$I(\text{Alice},\text{Eve}) \propto f(N_\sigma) = f(M,\langle n\rangle)$，因此在实验中，必须对$M$和$\langle n\rangle$有严格的要求。

3 实验装置

可光纤集成的相干态量子身份认证系统如图 2 所示，主要包括脉冲激光发射模块、偏振调制模块、偏振解调模块、脉冲激光接收模块和同步控制模块五个部分。其中激光发射模块为中心波长 1550 nm，连续输出功率为1.5 mW的分布反馈半导体(DFB)激光器(飞通 PT3553-13-5-5FC)，自制脉冲/连续驱动电路，可根据实验需要自由选择脉冲工作模式和连续工作模式。其中，实验中采用的脉冲激光发射电路包括脉冲信号发生部分和信号放大部分，如图 3 所示。产生的脉冲宽度为300 ns，光脉冲的功率为850 μW，重复频率为8 kHz，每个脉冲的能量为2.55×10^{-10} J，单光子能量为$E = h\nu = \frac{hc}{\lambda} = \frac{6.62559\times10^{-34}\times3\times10^8}{1.55\times10^{-6}} = 1.282\times10^{-19}$ J，，每个脉冲中的光子数约为2×10^9，将该脉冲衰减47 dB，保证每个脉冲中的平均光子数为 40000，若采用的运行密钥为 12 位时，则非法窃听者所能获得的最大信息量小于10^{-14} bit[16~21]。

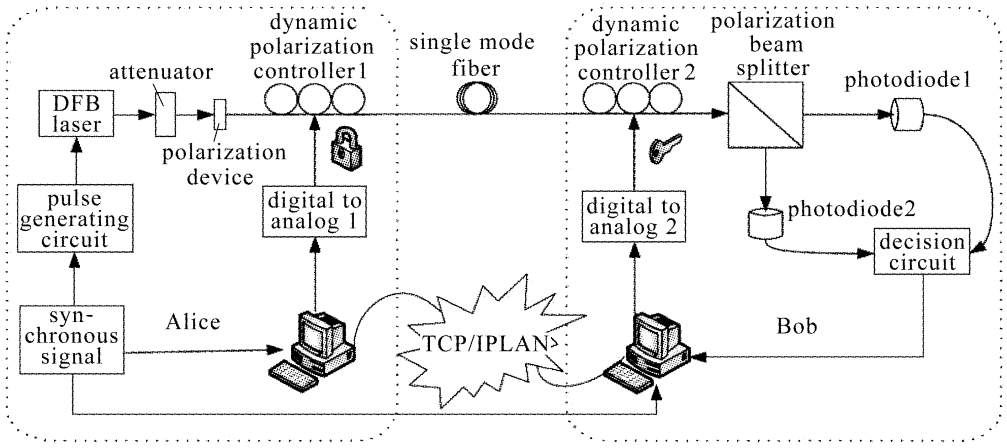

图 2 基于光纤的可集成相干光量子身份认证系统

Fig. 2 Experimental setup of an integrable optic-fiber coherent state quantum identification system

偏振调制模块和偏振解调模块采用美国 General Photonics 公司的全光纤动态偏振控制器(PCD-002-4X-FC/PC-7-C)，该模块可以把任意椭圆偏振态转换为另一任意椭圆偏振态。由于采用全光纤结构，它具有插入损耗低、偏振相关损耗低、带宽大(1260～1650 nm)、半波电压低等优点。采用光纤挤压器产生的应力双折射作为偏振调制原理，其调制速度达到33 kHz。实际工作过程中，由于采用的两个偏振控制器性能参数不完全一致，因此开发了光纤通信偏振相关器件性能检测系统，在实验前实时测试其性能参数，补偿两个偏振控制器之间的性能差异，初始化工作条件。

采用带尾纤的 PerkinElmer 公司的 C30637 型 PIN 作为脉冲接收模块的光电转换器件，该器件光电响应为0.95 A/W。为了探测功率为17 nW，脉冲宽度为300 ns的微弱窄脉冲，自行设计了检测电路。该电路分为光电转换、电流-电压转换和电压放大三个部分，如图 4 所示。放大电路输出波形如图 5 所示。采用该探测电路可以满足微弱信号探测的要求，采用比较器 LM361 作为判决器件判决传输的

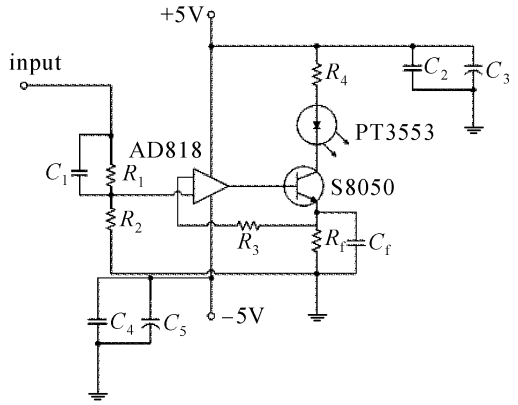

图 3　脉冲信号功率放大电路图

Fig. 3　Power amplification scheme of pulse signal

比特值为 0 还是 1，但由于脉冲宽度很窄，为了使控制系统有效读取判决器的输出，自行设计了一个脉冲展宽电路。

本系统采用同步信号来控制激光的产生、数据的接收等等，可以说整个系统的工作状态和速度都是由同步信号决定的。由于所采用的控制系统是以三星公司生产的 ARM7 芯片为核心的嵌入式操作系统，ARM7 处理运算指令时 ucLinux 系统的指令优先级要高于我们用来进行数据处理的程序，容易漏掉触发信号而使数据错位，无法精确同步。本系统采用自适应同步信号，在接收和发送双方的动态偏振控制器都调整到位之后，发送准备就绪信号，此时同步信号变为低电平，下降沿触发激光窄脉冲发射电路发射激光脉冲。在接收端收到数据之后，同步信号变为高电平，两个控制系统又回到就绪状态，准备进行下一次传输。

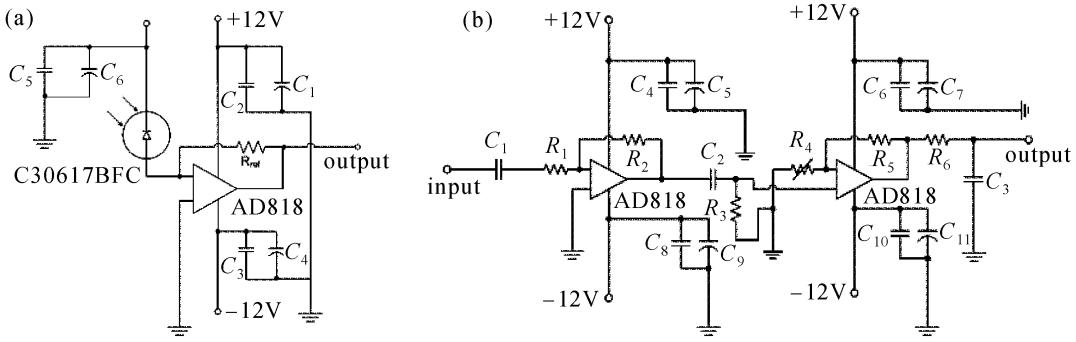

图 4　光电转换电路(a)和电压放大电路(b)

Fig. 4　Circuits for photoelectric transition (a) and voltage amplification (b)

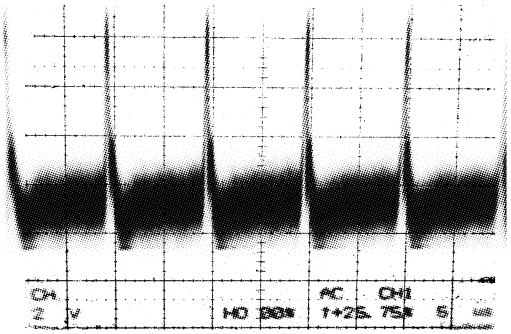

图 5　放大电路输出波形

Fig. 5　Output waveform of amplification circuit

实现同步的具体方案是，两个 ARM 控制系统分别提供一个数字信号给同步控制模块，高电平表示系统就绪，低电平表示正在接收数据(数据的发送方在将动态偏振控制器调整好之后也适当输出一段时间低电平)。这样就可以将逻辑描述为：在收发双方都为高电平时，同步信号也为高电平；双方都为低电平时同步信号为低电平；双方电平状态不同时，同步信号保持原来的状态不变。同步信号真值表如表 1 所示。

表 1　同步信号状态真值表

Table 1　True value table of the synchronization signal

State signal of receiver	0	1	0	1
State signal of sender	0	0	1	1
Synchronization signal	0	Keeping the front state	Keeping the front state	1

通过表 1 可以得到如图 6 所示的时序图。其中 A，B 分别为发送方和接收方的状态输出信号，C，D 分别为 A，B 信号的“与”和“或”的结果，E 为同步信号的输出。

控制系统 ARM_1 与 ARM_2 采用 Socket 网络通信程序在 TCP/IP 局域网实现量子保密通信所需要的经典通信，而主控制系统与各个驱动模块之间的直接通信通过信号线实现。

可光纤集成的相干态量子身份认证系统的工作

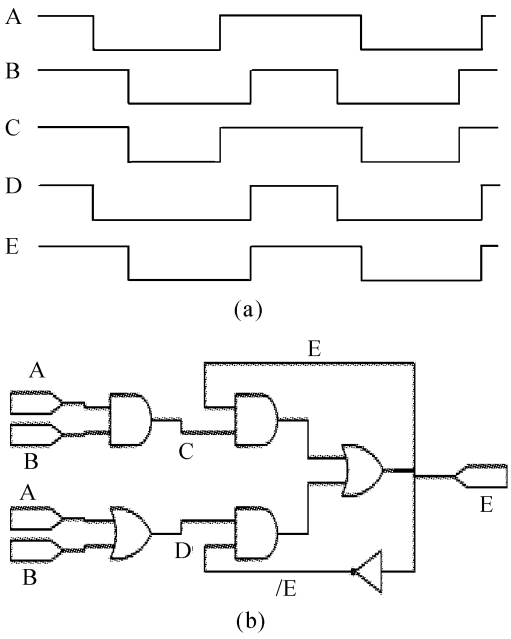

图 6 同步模块的时序图(a)和电路图(b)

Fig. 6 Synchronous module timing (a) and synchronous module circuit (b)

过程，采用美国 General Photonics 公司的 POL-001-P-15-SS-FC/PC 型起偏器把从分布反馈半导体激光器发出的激光初始化为 45°的线偏振光，每个光脉冲的功率为17 nW，脉冲宽度为300 ns，每个脉冲含 40000 个光子。Alice 通过动态偏振控制器 1 采用编码规则：比特 1 对应 45°偏振态，比特 0 对应 −45°偏振态(这实际上与实验方案中把比特 1 对应 0°偏振态，比特 0 对应 90°偏振态编码规则是一致的，可以通过程序很容易实现这种等效变换)，把认证码 k_1 编码为一串特定的偏振脉冲序列。我们设计的 12 位数模转换电路输出 0～4 V电压，通过自带的 15 倍放大电路产生 0～60 V工作电压驱动动态偏振控制器 1，2 工作。主控制器 ARM_1 通过 12 位线性反馈移位寄存器把初始共享密钥 k_3 扩展为 S_3，把 R_3 分为 l 块，每块的位数为 s，每一块作为一个运行密钥加密一个比特的有用信息，利用运行密钥，逻辑上通过动态偏振控制器 1 把数据偏振脉冲加密为任意偏振态。实际上，ARM_1 计算出一个总驱动电压，直接驱动动态偏振控制器 1 同时实现编码和加密过程。

保密偏振光脉冲通过单模光纤传输到 Bob 端的动态偏振控制器 2，Bob 采用相同的线性反馈移位寄存器把初始共享密钥 k_3 扩展为相同的运行密钥 S_3，主控制器 ARM_2 通过数模转换电路驱动动态偏振控制器 2 把保密偏振光脉冲解密为明文偏振光脉冲，即 45°，−45°光脉冲序列，把偏振光束分离器(FPBS)的两个出口 1 和 2 分别对准 45°和−45°，Bob 采用自制的激光脉冲探测模块分别测量光脉冲，如果出口 1 探测到光信号，则传输的为比特 1，出口 2 对应比特 0，该过程需要一个判决比较模块。

4 实验结果及讨论

采用设计的实验系统，进行了合法用户的身份图片传输实验，实验结果如图 7 所示。身份图片采用上海交通大学校徽和分色图片表示合法用户 Alice 的身份(也可采用指纹、声音、人物行为的视频段表示 Alice 的身份，物理上的实现原理一样)。实验结果表明合法用户之间的传输速率为8 kbit/s，误码率(BER)低于 10^{-4}，非法用户的误码率接近 50%，每传输一个比特的信息，窃听者所能窃取的信息量小于10^{-14} bit。

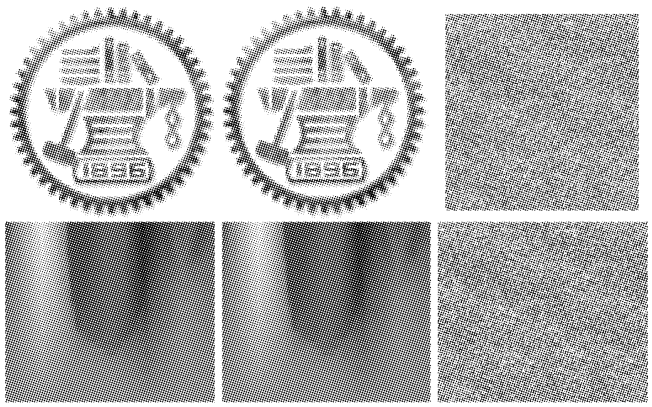

图 7 量子信息加/解密图像

(a) 原始图像；(b) 合法用户收到的图像；

(c) 非法用户收到的图像

Fig. 7 Quantum information encrypting/decrypting images

(a) origibal picture; (b) legal picture; (c) illegal picture

假设 Alice 和 Bob 之间共享了认证信息(当 Alice 需要向 Bob 证明其身份的情况下，可以共享 Alice 的照片)，当 Alice 向 Bob 进行身份认证时，通过该系统把认证信息(如照片)传输给 Bob，Bob 比较原始存储的图像和接收到的图像，统计出误码率(用 E_B 表示)。理想情况下，当 $E_B = 0$ 时，则可证明 Alice 的身份。实际情况下，由于信道的不完善，存在一定的误码率，可以根据实际系统预先统计出由于传输系统不完善所引起的误码率 E_{Bth}，当 $E_B < E_{Bth}$ 时，可以证实用户的合法身份。

对于攻击者，可以采用多种攻击方法：1) 猜测共享的认证信息，这种方法只有把所有的比特值全

部猜测正确才能认证成功，其成功的概率几乎为 0；2) 攻击该系统的传输线路以获得认证信息，这种情况可以由 Bob 模拟，即 Bob 不采用解密密钥 k_2 而采用随机密钥模拟 Eve 的窃听行为。理论计算表明[11~16]，当每个比特包含 40000 个光子，加密一个信息比特的加密密钥位数为 12 位时，I(Alice,Eve) $<10^{-14}$ bit，即误码率接近于 50%，即与第一种攻击方式相近。对这种攻击方式，所设计的系统可以认为是安全的。图 7(c)为这种情况下得到的照片，与图 7(a)相比较，显然，误码率非常高。这种情况下，非法用户几乎不可能假冒 Alice 的身份。

针对合法用户进行认证的情况，误码率 $E_B \neq 0$ 的情况存在以下原因，环境会影响光纤的双折射，很难精确保持传输光的偏振态，保偏光纤只可以保持偏振方向和快轴或慢轴平行的两种线偏振光，而系统经过加密操作后将出现任意椭圆偏振光，而在单模光纤中保持任意椭圆偏振态是非常困难的。另外，两个动态偏振控制器的半波电压并不完全一样，以及应力双折射效应并不严格服从线性关系，使得偏振调制与解调存在偏差，增大合法用户间的误码率。限制该系统传输速度的原因主要是控制系统 ARM 的处理速度。

5　结　论

自行设计了微弱窄脉冲激光光源、微弱激光脉冲接收模块、动态偏振控制器驱动模块和信号同步模块等关键性部件，采用偏振调制完成了可光纤集成相干态量子身份认证系统。经过各种偏振补偿措施，在每个光脉冲中的光子数为 40000 个，运行密钥的长度为 12 位的情况下，通信速率达到8 kbit/s，合法通信用户的误码率低于 10^{-4}，而非法用户所能窃听到的信息量 I(Alice,Eve) $<10^{-14}$ bit，即非法用户的误码率接近 50%。下一步的工作将采用 FPGA 代替控制系统 ARM 提高中心处理器的运算处理速度，继续提高光电探测模块的带宽，采用 $LiNbO_3$ 偏振控制器件提高偏振调制精度和速度，以提高量子保密通信速率，降低合法用户间的误码率，降低攻击者所能窃取的信息量，使相干态量子保密通信走向实用化。

参　考　文　献

1 N. Gisin, G. Ribordy, W. Tittel *et al.*. Quantum cryptography [J]. *Rev. Mod. Phys.*, 2002, **74**(1):145～195

2 Zeng Guihua. Quantum Cryptography [M]. Beijing: Science Press, 2006. 67～100
曾贵华. 量子密码学[M]. 北京：科学出版社，2006. 67～100

3 Liu Wenyu, Li Ning, Wang Cangqiang *et al.*. Quantum key distribution based on six-photon quantum error-avoiding codes [J]. *Acta Optica Sinica*, 2005, **25**(11):1568～1572
刘文予，李　宁，王长强 等. 基于六光子量子避错码的量子密钥分发方案[J]. 光学学报，2005，**25**(11)：1568～1572

4 Wang Xiaoxin, Liu Yu, Wang Changqiang. Experimental scheme of secure plaintext transmission with quantum direct communication [J]. *Acta Optica Sinica*, 2005, **25**(3):425～428
王晓鑫，刘　玉，王长强. 安全传送明文的量子直传实验方案设计[J]. 光学学报，2005，**25**(3)：425～428

5 Zhao Huan, Ma Haiqiang, Li Yaling *et al.*. Polarization control for optical fiber quantum cryptography [J]. *Acta Sinica Quantum Optica*, 2005, **11**(2):74～78
赵　环，马海强，李亚玲 等. 全光纤量子保密通信中的偏振控制[J]. 量子光学学报，2005，**11**(2)：74～78

6 Wu Guang, Zhou Chunyuan, Chen Xiuliang *et al.*. A stable long-distance quantum key distribution system [J]. *Acta Physica Sinica*, 2005, **54**(8):3622～3626
吴　光，周春源，陈修亮 等. 长距离长期稳定的量子密钥分发系统[J]. 物理学报，2005，**54**(8)：3622～3626

7 H. K. Lo, H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances [J]. *Science*, 1999, **283**(5410):2050～2056

8 P. W. Shor, J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol [J]. *Phys. Rew. Lett.*, 2000, **85**(2):441～444

9 D. Mayers. Unconditional security in quantum cryptography [J]. *J. ACM*, 2001, **48**(3):351～406

10 Guihua Zeng, Weiping Zhang. Identity verification in quantum key distribution [J]. *Phys. Rew. A*, 2000, **61**(2):022303-1～022303-5

11 Takashi Mikara. Quantum identification schemes with entanglements [J]. *Phys. Rew. A*, 2002, **65**(5):052326-1～052326-4

12 M. Dušek, O. Haderka, M. Hendrych *et al.*. Quantum identification system [J]. *Phys. Rew. A*, 1999, **60**(1):149～156

13 Guangqiang He, Guihua Zeng. A quantum identification scheme based on polarization modulation [J]. *Chinese Physics*, 2005, **14**(3):541～545

14 Guangqiang He, Guihua Zeng. A secure identification system using coherent states [J]. *Chinese Physics*, 2006, **15**(2):371～374

15 S. L. Braunstein, P. van Loock. Quantum information with continuous variables [J]. *Rev. Mod. Phys.*, 2005, **77**(2):513～577

16 G. A. Barbosa, E. Corndorf, P. Kumar *et al.*. Secure communication using mesoscopic coherent states [J]. *Phys. Rev. Lett.*, 2003, **90**(22):227901-1～227901-4

17 E. Corndorf, G. Barbosa, C. Liang *et al.*. High-speed data encryption over 25 km of fiber by two-mode coherent-state quantum cryptography [J]. *Opt. Lett.*, 2003, **28**(21):2040～2042

18 G. A. Barbosa. Fast and secure key distribution using mesoscopic coherent states of light [J]. *Phys. Rev. A*, 2003, **68**(5):052307-1～052307-8

19 E. Corndorf, P. Kumar, C. Liang *et al.*. Efficient quantum cryptography with coherent-state light in optical fibers at Gbps rates [C]. *SPIE*, 2004, **5161**:310～319

20 E. Corndorf, C. Liang, G. S. Kanter *et al.*. Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks [J]. *Phys. Rev. A*, 2005, **71**(6):062326-1～062326-10

21 G. A. Barboda. Information theory for key distribution systems secured by mesoscopic coherent states [J]. *Phys. Rev. A*, 2005, **71**(6):062333-1～062333-15