一种基于双偏振分束器的量子秘密共享方案*

韦克金[1)] 马海强[1)2)†] 汪龙[1)]

1) (北京邮电大学理学院, 北京 100876)

2) (中国科学院物理研究所, 北京 100190)

(2012年11月26日收到; 2013年1月9日收到修改稿)

提出一个基于双偏振分束器的单量子比特全光纤量子秘密共享方案, 该方案具有自动补偿光纤及光学器件的双折射效应和相位抖动的功能, 在干涉对比度测试和稳定性测试时, 该方案在 5 km 通信距离中, 获得的干涉对比度优于 993%, 且可长时间保持稳定.

关键词: 量子秘密共享, 偏振分束器, 单光子干涉

PACS: 42.50.Ar, 03.67.−a, 42.79.Sz, 07.20.Dt **DOI:** 10.7498/aps.62.104205

1 引 言

秘密共享是密码学一个重要的分支, 它主要完成的任务就是将一条秘密信息分割, 并把分割后得到的子信息分发给多个合法用户. 任何单个用户无法恢复这条信息, 这些用户解开这条秘密信息的惟一方式: 共享他们所接收到的子信息. 秘密共享作为一种特殊的密码协议, 被广泛地用于群体间的保密通信、密钥管理协议、电子拍卖协议等. 传统的秘密共享都是在经典信道中进行, 特别容易受到攻击及监听, 而量子密码的出现, 给秘密共享带来了新的曙光 [1,2]. 1999 年, Hillery 等 [3] 基于三纠缠态 (GHZ) 首次提出了量子秘密共享 (quantum secret sharing, QSS) 的概念, 从理论上克服了经典秘密共享的缺陷, 并掀起了 QSS 研究的热潮. 与经典秘密共享不同的是, 量子秘密共享不仅可以用于共享经典信息, 还可以用于共享量子密钥等量子信息 [4]. 现有的众多 QSS 协议和实验方案主要是基于纠缠态 [5−10], 但是, 量子纠缠态的制备效率是非常低的, 而且在光纤网络中不易于传输, 从而限制了基于纠缠态的 QSS 协议的实用性. 非纠缠态的 QSS 方案很好地解决了上述问题. 2003 年, Guo 等 [11] 采用直接编码的方式对密钥分发中的量子比特实现秘密共享; 2005 年, Schmid 等 [12] 提出了一种基于单光子的秘密共享协议, 该方案很好地保证了秘密传输过程中的稳定性和实用性; 诸如此类的协议以及方案还有许多 [13,14]. 虽然非纠缠的协议已经有很多, 但是实验上的工作成果却是相当少. 最近, Bogdanski 等 [15] 完成了基于单光子协议的实验方案, 获得了 99.3%的干涉对比度 [16].

本文基于 Schmid 的协议, 提出了一种基于双偏振分束器的量子秘密共享实验方案, 相对于 Bogdanski 等提出的方案, 具有自动补偿光纤及光学器件的双折射效应和相位抖动的功能, 而且器件简单易于实现, 无需任何调节的情况下保持长时间的稳定. 实验中可以获得干涉的对比度最高可达 99.94%, 在系统测试的半个月时间里, 每次开机的干涉对比度都优于 99.3%, 而且不需要对系统进行任何调节.

2 实验原理和实验方案

Schmid 的单量子比特的 N 方量子秘密共享协议如图 1 所示. 假设一共有 N 个用户 (R_1, R_2, ⋯, R_{N-1}, R_N). 一个初态为 $(|0\rangle+|1\rangle)/\sqrt{2}$ 量子比特被制备并通过量子通道, 从 R_1 传到 R_N, 最终在 R_N 进行探测.

* 国家重点基础研究发展计划 (批准号: 2010CB23202)、国家自然科学基金 (批准号: 10805006, 61178010, 61177085) 和中央高校基本科研业务费专项资金 (批准号: BUPT2010ZX04) 资助的课题.

† 通讯作者. E-mail: hqma@bupt.edu.cn

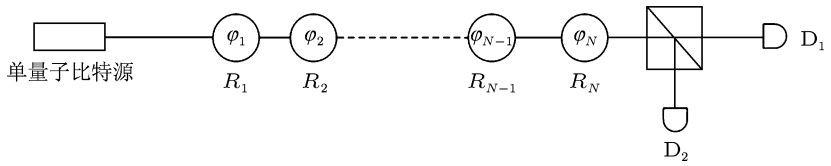

图 1 单比特量子秘密共享协议

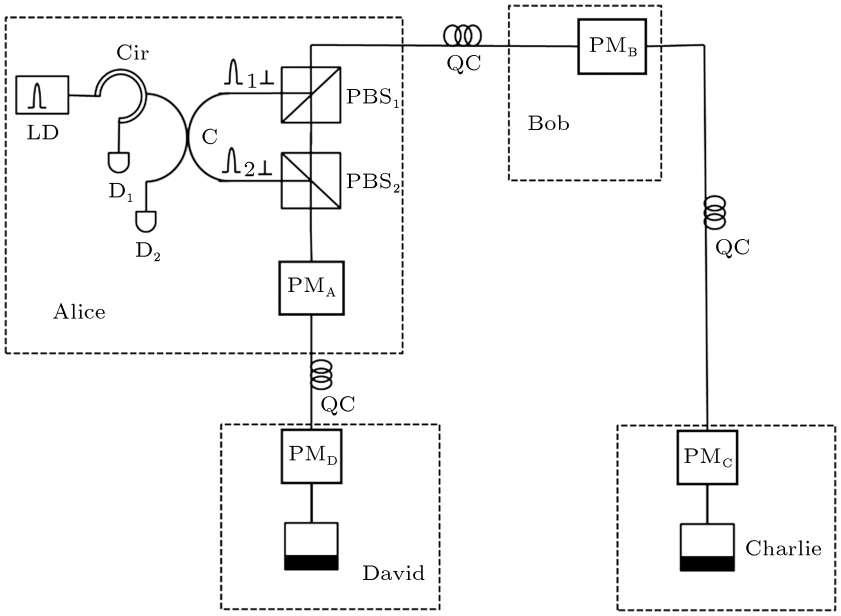

图 2 基于双偏振分束器的量子秘密共享实验方案 LD, 激光器; Cir, 环路器; C, 2×2 的光纤耦合器; PBS, 偏振分束器; QC, 光纤; PM, 相位调制器

每一个用户 R_j ($j=1, 2, \cdots, N-1$), 通过相位调制器对光进行随机的相位调制, 调制的相位 $\varphi_j \in \left(0, \pi/2, \pi, 3\pi/2\right)$.

$$\hat{U}(\varphi_j) = \{|0\rangle \to |0\rangle, |1\rangle \to \mathrm{e}^{\mathrm{i}\varphi_j}|1\rangle\}. \tag{1}$$

当通过所有用户以后, 粒子的态为

$$|X_N\rangle = \left(|0\rangle + \mathrm{e}^{\mathrm{i}(\Sigma_j^N \varphi_j)}|1\rangle\right)/\sqrt{2}. \tag{2}$$

将 $R_1, R_2, \cdots, R_{N-1}$ 调制相位 $\varphi_j \in \left(0, \pi/2, \pi, 3\pi/2\right)$ 划分为两个基, X 对应的是 $\varphi_j \in (0, \pi)$, Y 对应的是 $\varphi_j \in \left(\pi/2, 3\pi/2\right)$. 由于 R_N 要进行测量, 所以 R_N 的调制相位只需选择 0 (属于 X 基) 或 $\pi/2$ (属于 Y 基) 即可.

最后一个用户 R_N 在 $(|0\rangle \pm |1\rangle)/\sqrt{2}$ 态上进行测量, 概率为

$$p_\pm = (\varphi_1 \cdots \varphi_N) = \frac{1}{2}\left(1 \pm \cos\sum_j^N \varphi_j\right). \tag{3}$$

当 R_N 完成测量以后, 各个用户将 R_i ($i=1, 2, \cdots, N$) 以相反的顺序在公共信道中公布自己选择的基 [17], 但是不公布它们准确的调制相位. 由 (3) 式可知, 所有的用户可以通过公布的基推算最后的测量结果的确定性. 如果结果是确定的, 也就是 $p_- = 1$ 或 $p_+ = 1$, 则传输的数据为有效数据, 如果结果是不确定的, 就把这次的数据判定为无效并抛掉. 在这些有效的数据中, 任何 $N-1$ 方的用户想推测出剩余用户的调制相位的惟一方式, 就是共享自己所调制的相位或者探测结果. 通过以上方式, 完成了量子秘密共享过程 [7].

基于双偏振分束器的量子秘密共享实验装置如图 2 所示.

Alice 从激光器 (LD) 发射一个垂直偏振的单光子脉冲, 通过环形器 (Cir) 进入一个 2×2 的光纤耦合器 (C) 后, 被分成两个相同的光脉冲, 它们的偏振方向仍为垂直偏振态, 图上以脚标 1, 2 表示, 假设两个光脉冲的初始相位分别为 $\varphi_1 = 0$, $\varphi_2 = 0$. 脉冲 1, 2 经过耦合器出口的上端和下端分别传输到偏振分束器 1, 2 (PBS_1, PBS_2). 脉冲 1 的行程: 脉冲 1 以垂直偏振态到达 PBS_1, PBS_1 的工作原理是透射平行偏振态光, 反射垂直偏振态光. 因此, 脉冲 1 就被 PBS_1 反射耦合进量子信道 (QC), 经过相位调

制器 B(PM_B), 相位调制器 C (PM_C) 后被法拉第旋转镜 2(FM_2) 反射回来. 虽然两次经过 Bob, Charlie 的相位调制器, 但是脉冲 1 没有被加载任何信息. 同时, 它的偏振态也改变了 90°, 即垂直偏振的脉冲 1 在沿原路返回时, 偏振态变成了平行偏振态. 当脉冲 1 返回到 PBS_1 时, 由于其偏振态为平行偏振态, 就会被透射耦合进入到 PBS_2, 再次从 PBS_2 透射进入量子通道中, 经相位调制器 A (PM_A)、相位调制器 D (PM_D) 后, 到达法拉第旋转镜 1 (FM_1) 被返回, 同时偏振方向旋转 90°, 即在被 FM_1 返回后, 脉冲 1 的偏振态变为垂直偏振, 再次经过 PM_A, PM_D 到达 PBS_2. 在从 FM_1 返回时, David, Alice 通过相位控制器, 把它们的信息加载到脉冲 1 上, 此时 $\varphi_1 = \varphi_{PM_A} + \varphi_{PM_D}$. 当脉冲 1 返回到 PBS_2 时, 由于它是垂直偏振, 就会经 PBS_2 反射到达 2 × 2 的光纤耦合器, 循环了一周后又回到与脉冲 2 分离处. 同理, 脉冲 2 逆向沿着脉冲 1 的路径后, 加载完 Bob, Charlie 的相位信息后回到光纤耦合器与脉冲 1 会合, 此时 $\varphi_2 = \varphi_{PM_B} + \varphi_{PM_C}$. 在分束器, 我们使用两个单光子探测器 D_1, D_2 进行探测, 如果用户所调节的相位引起的结果是干涉相长, 则 D_1 有计数, 相消则 D_2 有计数. 与现有的秘密共享装置相比, 这套装置对光纤的双折射效应以及相位抖动具有自动补偿作用, 从而可以获得很高的干涉对比度.

在图 2 中, 除了环形器, 耦合器, PBS_1, PBS_2 的尾纤为保偏光纤外, 其他的光纤均为普通光纤. 其光纤的双折射效应以及相位抖动的自动补偿原因解释如下.

对于一个具有双折射效应的器件, 它的琼斯传输矩阵可表述为

$$\vec{\boldsymbol{T}} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \cdot \begin{pmatrix} \exp(-\mathrm{i}\theta_\mathrm{o}) & 0 \\ 0 & \exp(\mathrm{i}\theta_\mathrm{e}) \end{pmatrix} \times \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}, \tag{4}$$

$$\overleftarrow{\boldsymbol{T}} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \cdot \begin{pmatrix} \exp(-\mathrm{i}\theta_\mathrm{o}) & 0 \\ 0 & \exp(\mathrm{i}\theta_\mathrm{e}) \end{pmatrix} \times \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \tag{5}$$

(4) 式中, θ 为参考坐标与双折射快慢轴的夹角, θ_o, θ_e 是双折射器件引起的位相位的相移, $\overleftarrow{\boldsymbol{T}}$, $\vec{\boldsymbol{T}}$ 是反向与正向的传输矩阵.

法拉第旋转镜的琼斯矩阵为

$$\boldsymbol{T}_\mathrm{FM} = \begin{pmatrix} \cos 45^\circ & \sin 45^\circ \\ -\sin 45^\circ & \cos 45^\circ \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} \cos 45^\circ & -\sin 45^\circ \\ \sin 45^\circ & \cos 45^\circ \end{pmatrix}, \tag{6}$$

则对于一个带法拉第旋转镜的双折射器件的琼斯矩阵

$$\boldsymbol{T} = \vec{T} \cdot \overleftarrow{T}_\mathrm{FM} \cdot \vec{T} = \exp\{\mathrm{i}(\theta_\mathrm{o} + \theta_\mathrm{e})\}\boldsymbol{T}_\mathrm{FM}. \tag{7}$$

由上式可知, 整体的传输矩阵与传输介质的双折射效应以及输入光的偏振态无关.

3 实验结果和讨论

实验中所用激光器为 Advanced Laser Diode Systems PIL131DFB-SM, 工作的中心波长是 1310 nm, 线宽为 0.1 nm, 光脉冲宽度约为 20 ps, 重复频率 1 MHz, 平均功率约为 500 nW. X 型耦合器采用的是 50/50 的光分路器, 经衰减后达到平均每脉冲光子数 $\langle n \rangle = 0.1$.

干涉对比度实验测试中, 整个光路的光纤总长度为 5 km, 激光器被衰减到单光子量级, 不给 Alice, Bob, Charlie 的相位调制器加驱动电压, 然后给 David 的相位调制器 PM_D 加范围为 0—8.5 V 的调控电压, 然后记录两个单光子探测器 D_1, D_2 计数率, 其结果如图 3 所示.

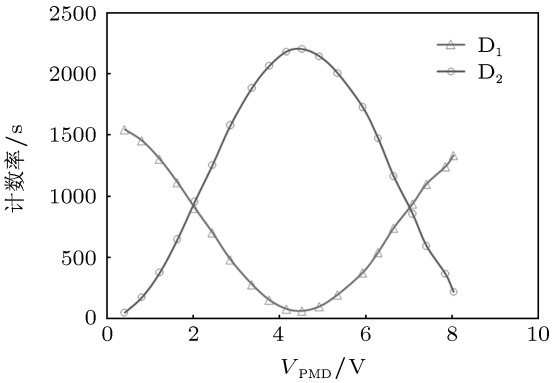

图 3 相位调制工作图

图 3 中, 横坐标为调制电压, 纵坐标为单光子计数器的计数率, 三角号的图线为 D_1 的计数, 空心圆的图线为 D_2 的计数. 经过计算, 干涉对比度达到了 99.94%. 而且由图 3 可知, 通过相位调制器, 可以很好地给信号光加载所需要的相位, 进而完成量子秘密共享过程.

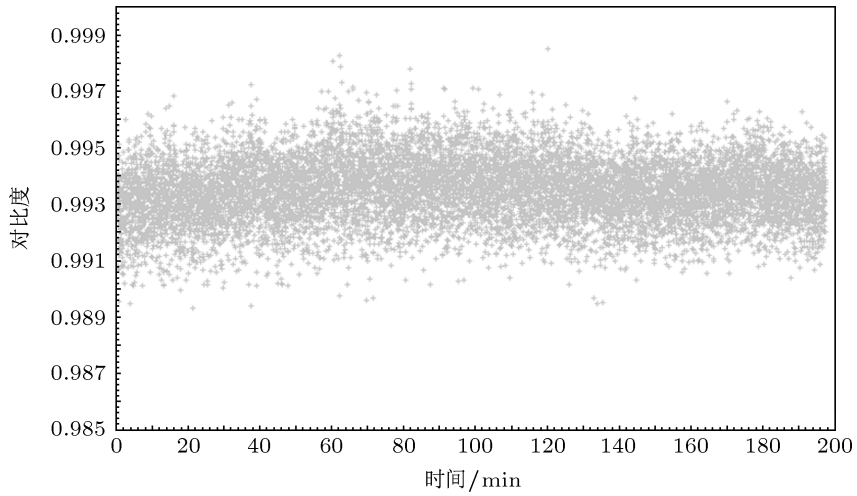

图 4 系统干涉对比度图

在系统稳定性测试过程中, 给 PM_D 加半波电压后, 用计算机按每秒 1 次的速率统计干涉对比度, 可以得到图 4.

图 4 中纵坐标为干涉对比度, 横坐标为系统运行时间. 在超过 3 h 的测试时间中, 由图 4 可知该系统的干涉对比度稳定在 99.3%左右. 而且在系统测试的半个月里, 在不对系统做任何调节的情况下, 每次开机对比度均可达到 99.3%. 优良的干涉对比度能保证量子秘密共享过程中较低的误码率, 从而确保量子秘密共享过程能稳定、正确地完成.

4 结 论

本文利用双偏振分束器构建了一个全光纤的量子秘密共享系统, 该系统是基于单量子比特的秘密共享协议, 相对基于纠缠的量子秘密共享系统有着更好的应用前景. 同时, 该系统能够自动补偿光纤和光学器件的双折射效应以及相位抖动, 而且通过长时间的测试, 该系统的稳定性也非常高. 该方案稳定的性能必能使其成为未来量子秘密共享应用中一个优秀的备选方案.

[1] Liu L L, Tsai C W, Hwang T 2012 *Int. J. Theor. Phys.* **51** 2291
[2] Du J Z, Sun Y, Qin S J, Wen Q Y, Zhu F C 2008 *Acta Phys. Sin*. **57** 4694 (in Chinese) [杜建忠, 孙莹, 秦素娟, 温巧燕, 朱甫臣 2008 物理学报 **57** 4694]
[3] Hillery M, Buzek V, Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[4] Zhang J, Wang F Q, Zhao F, Lu YQ, Liu S H 2008 *Acta Phys. Sin.* **57** 4946 (in Chinese) [张静, 王发强, 赵峰, 路轶群, 刘颂豪 2008 物理学报 **57** 4946]
[5] Zhu Z C, Zhang Y Q, Fu A M 2012 *Chin. Phys.* B **21** 010307
[6] Wang C, Zhang Y 2009 *Chin. Phys.* B **18** 3238
[7] Karlsson A, Koashi M, Imoto N 1999 *Phys. Rev.* A **59** 162
[8] Karimipour V, Bahraminasab A, Bagherinezhad S 2002 *Phys. Rev.* A **65** 042320
[9] Tittel W, Zbinden H, Gisin N 2001 *Phys. Rev.* A **63** 042301
[10] Chen Y A, Zhang A N, Zhao Z, Zhou X Q, Lu C Y, Peng C Z, Yang T, Pan J W 2005 *Phys. Rev. Lett.* **95** 200502
[11] Guo G P, Guo G C 2003 *Phys. Lett.* A **310** 247
[12] Schmid C, Trojek P, Weinfurter H, Bourennane M, Zukowski M, Kurtsiefer C 2005 *Phys. Rev. Lett*. **95** 230505
[13] Yang Y G, Wen Q Y, Zhu F C 2006 *Acta Phys. Sin*. **55** 3258 (in Chinese) [杨宇光, 温巧燕, 朱甫臣 2006 物理学报 **55** 3258]
[14] Wang T Y 2008 *Opt. Commun*. **281** 6130
[15] Bogdanski J, Rafiei N, Bourennane M 2008 *Phys. Rev.* A **78** 062307
[16] Bogdanski J, Rafiei N, Bourennane M 2009 *Opt. Express* **17** 4485
[17] Christian S, Pavel T, Mohamed B, Christian K, Marek Z, Harald W 2005 *Phys. Rev. Lett.* **98** 028902

A quantum secret sharing scheme based on two polarization beam splitters *

Wei Ke-Jin[1)] Ma Hai-Qiang[1)2)†] Wang Long[1)]

1) (*School of Sciences, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

2) (*Institute of Physics, Chinese Academy of Sciences, Beijing* 100190, *China*)

(Received 26 November 2012; revised manuscript received 9 January 2013)

Abstract

In this paper we present a quantum secret sharing scheme based on a single qubit protocol using two polarization beam splitters. This scheme guarantees an auto compensation of birefringence and phase jitter in single mode fiber and optical device. The visibility is higher than 99.3% over 5 km communication distance with an excellent stability.

Keywords: quantum secret sharing, polarization beam splitter, single photon interference

PACS: 42.50.Ar, 03.67.−a, 42.79.Sz, 07.20.Dt **DOI:** 10.7498/aps.62.104205

* Project supported by the National Basic Research Program of China (Grant No. 2010CB23202), the National Natural Science Foundation of China (Grant Nos. 10805006, 61178010, 6117085) and the Fundamental Research Funds for the Central Universities, China (Grant No. BUPT2010ZX04).

† Corresponding author. E-mail: hqma@bupt.edu.cn