文章编号:1004-4213(2011)08-1248-5

基于 N 个有序纠缠光子对的量子机密共享方案

袁素真,孙志富,田俊龙
(安阳师范学院 物理与电气工程学院,河南 安阳 455002)

摘 要:提出了一种基于 N 个有序纠缠光子对量子机密共享方案.用纠缠光子作为信息的载体,密钥管理者 Alice 将纠缠光子对分成两个序列,其中一个序列直接发送给合作者之一 Bob,在确保第一个序列发送安全后,再对第二个序列进行编码,发送给另一个合作者 Charlie. Bob 和 Charlie 分别对他们所接收到的光子序列进行 Bell 基联合测量,从而得到 Alice 所发布的密钥,完整密钥的获得需要管理者和所有合作者共同实现.本方案采用两体纠缠态,相对三体纠缠态来说,在实验上更容易实现,仅需要线性光学元件和简单的纠缠源.

关键词:量子机密共享;纠缠光子对;幺正操作;单光子测量
中图分类号:070201 **文献标识码**:A **doi**:10.3788/gzxb20114008.1248

0 引言

随着量子计算技术的发展,对基于经典大数因子分解算法的加密体系构成了极大的威胁,信息的安全传输受到了极大的挑战,量子密钥技术在这种背景下受到广泛的重视,国内外的一些科研小组在这方面已经取得了突破性进展,如国内的郭光灿小组[1-2]、邓富国小组[3-5],他们提出了很多量子密钥方案来保证通讯安全.由于很多保密通讯系统的安全完全依赖于用来加密信息的密钥,因此,对密钥的管理就变得十分重要.为了降低密钥的泄露或丢失,密钥的管理者希望能将一个重要的密钥分成很多份,交给不同的人来管理,其中每个人都只得到了密钥的一部分,在所有成员共同合作的情况下才能完整的恢复这个密钥,从而可以防止因为成员中某个人的不诚实行为而泄密.经典通信中,机密共享一般用在一些特殊场合,如 Alice 是管理者,Bob 和 Charlie 是她的两个合作者,一般来说 Alice 与 Bob 和 Charlie 相距较远,而 Bob 与 Charlie 相距较近.但 Alice 有一项很重要的工作需要在 Bob 和 Charlie 所在的地方完成这个工作,为了让 Bob 和 Charlie 能相互监督,Alice 希望这个工作由 Bob 和 Charlie 合作来完成,从而阻止其中某个不可靠的合作者的破坏行为.1979 年 Blakley[6] 和 Shamir[7] 提出了第一个经典的机密共享方案,由于经典的信号可以被恶意的窃听者(如 Eve)任意、完全的复制而不会被发现,因此,从理论上来说,如果仅靠经典的物理方法很难保证这些合作者安全地重建密钥,也就无法达到想要的绝对安全.

量子机密共享(Quantum Secret Sharing, QSS)[4,8-9]是将经典机密共享推广到量子领域内的一项技术,该技术为信息的传输提供了一种新的更安全的途径.它利用一些基本的量子力学原理,并辅以一些特殊的传输过程设计,从而使得外界窃听者 Eve 或合作者之一(不妨假设为 Bob)的窃听行为都无法躲避 Alice 和 Charlie 的安全检测.自从 1999 年,Hillery, Buzek 和 Berthiaume[8] 利用一个(Greenbeger-Horne-Zeilinger,GHZ)态提出了第一个量子 QSS 方案,称之为 HBB99 方案.到目前为止,很多研究组在 QSS 方面已经做了大量研究工作,提出了很多理论和实验方案[10-19],包括共享一个未知态的一些方案[20-22].本文借鉴龙桂鲁-刘晓曙教授研究组提出的 Long-Liu 2002 量子密钥分配方案[5]的思想,给出基于 N 个有序纠缠对的量子机密共享方案(不妨称为 N-ordered Entangled Pairs QSS),并对其安全性进行分析.

1 量子力学相关知识——测量基

以偏振单光子为例对测量基做简要说明.

测量基分为水平垂直基(用⊕表示)和 45°与 135°基(用⊗表示).用⊕基去测水平和垂直偏振的光子能够得到一个完全确定的结果,水平偏振的光子通过后不发生偏转,垂直偏振的光子通过后发生偏转;用⊗基去测 45°方向与 135°方向偏振的光子

基金项目:国家自然科学基金(No. 11005003、No. 11005002、No. 11047108)资助
第一作者:袁素真(1982—),女,助教,硕士,主要从事量子光学及量子信息方面的研究. Email:yusuzh@aynu.edu.cn
收稿日期:2011-01-04;**修回日期**:2011-06-29

能够得到一个完全确定的结果(45°方向偏振的光子通过后不发生偏转，135°方向偏振的光子通过后发生偏转). 用⊕基去测量 45°或 135°方向偏振的光子，或用⊗基去测量水平或垂直方向偏振的光子均无法事先得到确定的结果，即是否偏转是完全随机的.

用⊕基制备的 2 个量子态分别为水平方向偏振的$|H\rangle$和垂直方向偏振的$|V\rangle$，用⊗基制备的 2 个量子态分别为 45°方向偏振的$|L\rangle$和 135°方向偏振的$|R\rangle$，用量子力学语言来描述为

$$|H\rangle=|0\rangle,|V\rangle=|1\rangle,$$

$$|R\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle),|L\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \quad (1)$$

将水平方向$|H\rangle$和 45°方向$|L\rangle$偏振的光子量子态编码为二进制的“0”，把垂直方向$|V\rangle$和 135°方向$|R\rangle$偏振的光子量子态编码为“1”，如果选择⊕基进行单光子制备，然后随机选择⊕基和⊗基进行单光子测量，结果如表 1. 同理，选择⊗基进行单光子制备时情况类似.

表 1　用⊕基单光子制备，随机选择⊕和⊗基进行单光子测量结果

Table 1　Single photons prepared with ⊕ base and measured with random selection of ⊕ and ⊗ base

Preparation bases	Polarized states	Measurement bases	Measurement results	Appearance probability
⊕	→	⊕	→	100%
⊕	↑	⊕	↑	100%
⊕	→	⊗	↗	50%
⊕	→	⊗	↖	50%
⊕	↑	⊗	↗	50%
⊕	↑	⊗	↖	50%

2　基于 *N* 个有序纠缠对的量子机密共享方案(*N*-ordered Entangled Pairs-QSS)

图 1 给出了 *N*-ordered Entangled Pairs QSS 的原理，Alice 制备一组由处于最大纠缠态(Einstein-Podolsky-Rosen，EPR)的光子对组成的量子信号，

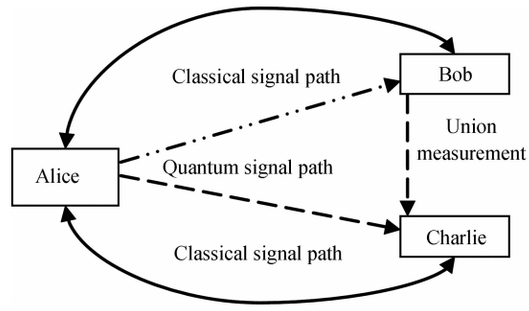

图 1　*N* 个有序纠缠对的量子机密共享方案

Fig. 1　*N*-ordered entangled pairs-QSS scheme

即 *N* 个有序纠缠光子对，用符号标记为$\{(P_1(B),P_1(C)),(P_2(B),P_2(C)),\cdots,(P_i(B),P_i(C)),\cdots,(P_N(B),P_N(C))\}$，其中，$i$ 代表第 $i(i=1,2,\cdots,N)$对 EPR 对，B 和 C 分别表示一个 EPR 对中的两个光子，并把它们制备在相同的量子态下，此量子态可以是四个 Bell 基态之一，四个 Bell 基态分别为

$$|\Psi^-\rangle=\frac{1}{\sqrt{2}}(|0\rangle_B|1\rangle_C-|1\rangle_B|0\rangle_C)$$

$$|\Psi^+\rangle=\frac{1}{\sqrt{2}}(|0\rangle_B|1\rangle_C+|1\rangle_B|0\rangle_C)$$

$$|\phi^-\rangle=\frac{1}{\sqrt{2}}(|0\rangle_B|0\rangle_C-|1\rangle_B|1\rangle_C)$$

$$|\phi^+\rangle=\frac{1}{\sqrt{2}}(|0\rangle_B|0\rangle_C+|1\rangle_B|1\rangle_C) \quad (2)$$

式中$|0\rangle$和$|1\rangle$是两状态系统的特征向量，例如，对于 z 方向极化的光子，它们是 Pauli 算符 σ_z 的特征向量. 不妨设 Alice 制备的 *N* 个有序 EPR 对都处于量子态$|\Psi^-\rangle=\frac{1}{\sqrt{2}}(|0\rangle_B|1\rangle_C-|1\rangle_B|0\rangle_C)$. 然后 Alice 将这 *N* 个 EPR 对分成两个序列，即从每一个 *EPR* 对中拿出一个光子按顺序组成一个序列，可以记为序列 $S_B=[P_1(B),P_2(B),\ldots,P_i(B),\ldots,P_N(B)]$；另一个光子顺序组成另一个相应的序列，可记为 $S_C=[P_1(C),P_2(C),\ldots,P_i(C),\ldots,P_N(C)]$，见图 2，其中直线所连接的两个黑球为一对纠缠光子.

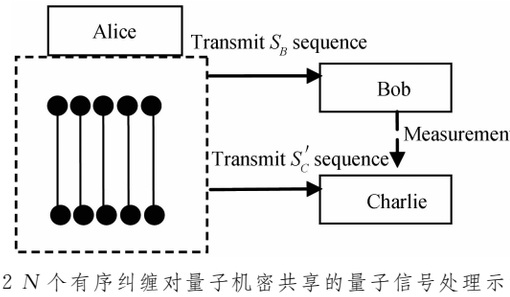

图 2 *N* 个有序纠缠对量子机密共享的量子信号处理示意图

Fig. 2　Schematic diagram of the quantum signal processing of *N*-ordered entangled pairs-QSS

Alice 将 S_B 序列发送给合作者 Bob，但她仍然控制着 S_C 序列. Bob 接收到光子序列 S_B 后，从中随机抽取适量的光子，并对其进行单光子测量，Bob 随机选择两组测量基⊕和⊗中的一组来对每一个抽样光子进行测量并记录测量基信息和结果，并通过经典信道通知 Alice. Alice 根据 Bob 所告知的所有信息，在 S_C 中重复 Bob 的操作，并记录测量结果. Alice 将自己的测量结果与 Bob 所告知的测量结果进行比对并进行出错率分析；如果出错率在阈值范围内，则表明 S_B 序列的传输是安全的；否则，Alice 和 Bob 放弃已经得到的传输结果.

如果已经确定 S_B 序列的传输是安全的，Alice 根据自己所需传输的信息，选择 4 个幺正操作 $\{U_0、U_1、U_2、U_3\}$ 中的一个来对序列 S_C'（在 S_C 中扣除用于安全检测后的所有光子）中的每一个光子依次做相应的幺正操作，从而完成对量子态的机密编码过程. 在编码过程中，Alice 需要在随机的位置进行适量的安全检测编码，即加入一些为安全检测服务的随机编码. 四个量子幺正操作为

$$U_0=I_2\otimes I_2=\begin{pmatrix} I_2 & 0\\ 0 & I_2\end{pmatrix}=\begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1\end{pmatrix} \tag{3}$$

$$U_1=I_2\otimes\sigma_x=\begin{pmatrix} \sigma_x & 0\\ 0 & \sigma_x\end{pmatrix}=\begin{pmatrix} 0&1&0&0\\ 1&0&0&0\\ 0&0&0&1\\ 0&0&1&0\end{pmatrix} \tag{4}$$

$$U_2=I_2\otimes(-\mathrm{i}\sigma_y)=\begin{pmatrix} -\mathrm{i}\sigma_y & 0\\ 0 & -\mathrm{i}\sigma_y\end{pmatrix}=\begin{pmatrix} 0&-1&0&0\\ 1&0&0&0\\ 0&0&0&-1\\ 0&0&1&0\end{pmatrix} \tag{5}$$

$$U_3=I_2\otimes\sigma_z=\begin{pmatrix} \sigma_z & 0\\ 0 & \sigma_z\end{pmatrix}=\begin{pmatrix} 1&0&0&0\\ 0&-1&0&0\\ 0&0&1&0\\ 0&0&0&-1\end{pmatrix} \tag{6}$$

它们分别代表编码 00，01，10 和 11，这四种幺正操作可以实现 Bell 基态 $\{|\psi^-\rangle_{BC}, |\psi^+\rangle_{BC}, |\varphi^-\rangle_{BC}, |\varphi^+\rangle_{BC}\}$ 之间的相互转换，转换情况如表 2. Alice 将编码后的 S_C' 序列发送给 Charlie，此时，Charlie 和 Bob 合作对 S_C' 序列和 S_B' 序列（S_B 中扣除用于安全性检测后的所有光子）中对应的纠缠光子对做 Bell 基联合测量，从而读出 Alice 所做的操作信息，即 Alice 对光子序列中的每一个光子分别采用了什么幺正操作，也就得到了 Alice 所需传输的机密信息序列.

表 2 幺正操作下 BELL 基态转换

Table 2 The coversion of Bell base under unitary operation

Operations	U_0	U_1	U_2	U_3
Objects	$\psi^-\psi^+$	$\psi^-\psi^+$	$\psi^-\psi^+$	$\psi^-\psi^+$
	$\varphi^-\varphi^+$	$\varphi^-\varphi^+$	$\varphi^-\varphi^+$	$\varphi^-\varphi^+$
Results	$\psi^-\psi^+$	$\varphi^-\varphi^+$	$\varphi^+\varphi^-$	$\psi^+\psi^-$
	$\varphi^-\varphi^+$	$\psi^-\psi^+$	$\psi^+\psi^-$	$\varphi^+\varphi^-$

3 安全性分析

本方案涉及到两个信息的传输过程，第一个过程为：Alice 将信息序列 S_B 发送给 Bob，第二个过程为：Alice 将编码后的 S_C' 序列发送给 Charlie.

过程一的安全性是由单光子测量保证的，Bob 接收到光子序列 S_B 后，从中随机抽取适量的光子，选择两组测量基⊕和⊗中的一组进行单光子测量，根据量子力学原理，测量后光子的状态坍缩到测量基的本征态上. Alice 在 S_C 中用相同于 Bob 的测量基，对与 Bob 的抽样光子对应位置的光子进行单光子测量，并记录测量结果. Alice 对以下三个方面的信息进行比对：Alice 所制备的原始纠缠态；Alice 的测量结果；Bob 所告知的测量基和测量结果. 比对结果在没有窃听行为的理想状态下如表 3. 假设此过程有 Charlie 全程窃听，则由于 Charlie 窃听时会随机选择测量基⊕和⊗，则会有 50% 的几率与 Bob 所选测量基相同，这部分不会引入错误，而其余 50% 几率所选的测量基不同，由此会引入 25% 的错误几率. 总体而言，假设有第三者窃听，很容易因为出错率超过 25%（加上噪音等其他因素引起的错误率）而被发现. Charlie 进行窃听时，Alice 的单光子测量结果如表 4.

表 3 理想状态下 Alice 和 Bob 的测量结果

Table 3 Measurement results of Alice and Bob under ideal circumstance

Alice's EPR photons	ψ^-	ψ^-	ψ^-	ψ^-
Bob's measurement base	⊕	⊕	⊗	⊗
	↑	→	↗	↖
Bob's measurement result	1	0	0	1
Alice's measurement base	⊕	⊕	⊗	⊗
	→	↑	↖	↗
Alice's measurement result	0	1	1	0
Raw key	0	1	1	0

表 4　Charlie 窃听时 Alice 和 Bob 的测量结果

Table 4　Measurement results of Alice and Bob under Charlie′s eavesdropping

Alice′s EPR photons	ψ^-	ψ^-	ψ^-	ψ^-	ψ^-	ψ^-	ψ^-	ψ^-	ψ^-	ψ^-	ψ^-	ψ^-
Charlie′s measurement base	⊕	⊕	⊗	⊗	⊕	⊕	⊕	⊕	⊗	⊗	⊗	⊗
	↑	→	↗	↖	↑	↑	→	→	↗	↖	↗	↖
Charlie′s measurement base	1	0	0	1	1	1	0	0	0	1	0	1
Bob′s measurement base	⊕	⊕	⊗	⊗	⊗	⊗	⊗	⊗	⊕	⊕	⊕	⊕
	↑	→	↗	↖	↗	↖	↗	↖	↑	↑	→	→
Bob′s measurement base	1	0	0	1	0	1	0	1	1	1	0	0
Alice′s measurement base	⊕	⊕	⊗	⊗	⊗	⊗	⊗	⊗	⊕	⊕	⊕	⊕
	→	↑	↖	↗	↗	↗	↖	↖	↑	→	↑	→
Alice′s measurement base	0	1	1	0	0	0	1	1	1	0	1	0
Raw key	0	1	1	0		0	1			0	1	

过程二是在保证过程一安全的前提下进行的. 过程二的安全性是由 Alice 在进行机密编码过程中加入安全检测编码所保证的. 当 Charlie 接收到携带机密信息 S_C' 后，Alice 要求 Bob 和 Charlie 在 Alice 加入安全检测编码位置处的光子进行 Bell 基联合测量，然后 Bob 和 Charlie 通过经典信道将测量结果反馈给 Alice，从而 Alice 可以根据自己所做的幺正操作和反馈信息做出错率分析. 如果有窃听者窃听，就会将 Charlie 手中光子序列与 Bob 手中光子序列的关联性破坏，从而在进行联合测量时得不到预期的结果.

如果经过以上两个安全性分析，出错率都在阈值以内，说明管理者 Alice 成功将密钥传给了合作者 Bob 和 Charlie，从而 Alice、Bob 和 Charlie 就可以完成安全的量子密钥共享，Bob 和 Charlie 对除去两次安全检测的纠缠光子序列进行联合测量就可以得到 Alice 所加到纠缠光子对上的密钥信息.

N-ordered Entangled Pairs-QSS 方案的一个优点是：高容量. 每一个 EPR 对携带 2 比特信息，*N* 个 EPR 对载荷 2*N* 个比特信息；Alice、Bob 和 Charlie 只需要对抽样的量子数据进行经典信息交换，对其它量子数据不需要交换经典信息，而抽样数据对整个数据而言是很少的一部分，这样 *N*-ordered Entangled Pairs-QSS 方案的总信息传输效率高，传输效率的定义及计算见文献[23]. 它的缺点是：需要克制退相干作用；另一个缺点是一个粒子序列需要等待另一个粒子序列传输完后才能传输，所以需要对量子态进行保存，这方面的技术尚不成熟.

4　结论

本文介绍了一种新的量子机密共享方案，采用 *N* 个有序的纠缠光子对作为信息载体，任何窃听者的窃听行为都能通过安全分析检测出来，即便是合作者本身的窃听行为也能被识别，并且，本方案只需要线性光学元件和简单的双光子纠缠源，在现有的技术条件下在实验上很容易实现.

参考文献

[1] WEN Hao, HAN Zheng-fu, ZHAO Yi-bo, *et al*. Multiple stochastic paths scheme on partially-trusted relay quantum key distribution network[J]. *Science in China* (*Series F*),,2009,**52**(1):18-22.

[2] HAN Zheng-fu, MO Xiao-fan, GUI You-zhen, *et al*. Stability of phase-modulated quantum key distribution system[J]. *Applied Physics Letters*, 2005, **86**(22): 1103-1105.

[3] LI Xi-han, DENG Fu-guo, ZHOU Hong-yu. Efficient quantum key distribution over a collective noise channel[J]. *Physical Review A*, 2008, **78**(2): 2321-2326.

[4] XIAO L, LONG G L, DENG F G, *et al*. Efficient multiparty quantum-secret-sharing schmes[J]. *Physical Review A*, 2004, **69**(5): 2307-2311.

[5] LONG G L, LIU X S. Theoretically efficient high-capacity quantum-key-distribution schemes[J]. *Physical Review A*, 2002, **65**(3): 2302-2304.

[6] BLAKLEY G R. In proceedings of American federation of information processing 1979 national computer congerence [C]. American Federantion of Information Processing, Arlington, VA. 1979(48):313-317.

[7] SHAMIR A. How to share a secret[J]. *Communication of the ACM*, 1979, **22**(11):612-613.

[8] HILLEY M, BUŽEK V, BERTHIAUME A. Quantum secret sharing[J]. *Physical Review A*, 1999, **59**(3):1829-1834.

[9] KARLSSON A, KOASHI M, IMOTO N. Quantum entanglement for secret sharing and secret splitting [J]. *Physical Review A*, 1999, **59**(1):162-168.

[10] BANDYPADHYAY S. Teleportation and secret sharing with pure entangled state[J]. *Physical Review A*, 2000, **62**(1): 2308-2320.

[11] NASCIMENTO ACA, MUELLER-QUADE J, IMAI H. Improving quantum secret sharing schemes [J]. *Physical Review A*, 2001, **64**(4):2311.

[12] XIONG Xue-shi, FU Jie, SHEN Ke. Controlled teleportation of an unkbown two-particle partly entangled state[J]. *Acta Photonica Sinica*, 2006 , **35**(5):780-782.
熊学仕，付洁，沈柯. 二粒子部分纠缠未知态的量子受控传递

[J]. 光子学报,2006 , **35**(5):780-782.

[13] KARIMIPOUR V, BAHRAMINASAB A, BAGHERINEZHAD S. Entanglement swapping of generalized cat states and secret sharing[J]. *Physical Review A*, 2002, **65**(4): 2320.

[14] DENG Xiao-ran, YANG Shuai, YAN Feng-li. Quantum secret sharing with *N*-particle entangled state[J]. *Acta Photonica Sinica*, 2010, **39**(11):2083-2087.
邓晓冉,杨帅,闫凤利. 利用 *N* 粒子纠缠态的量子秘密共享[J]. 光子学报,2010, **39**(11):2083-2087.

[15] GAO Gan. Eavesdropping on the improved three-party quantum secret sharing protocol[J]. *Optics Communications*, 2011, **284**(3):902-904.

[16] SHI Run-hua, HUANG Liu-sheng, YANG Wei, *et al*. Multiparty quantum secret sharing with bell states and bell measurements[J]. *Optics Communications*, 2010, **283**(11): 2476-2480.

[17] DONG Li, XIU Xiao-ming, GAO Ya-jun, *et al*. An arbitrary two-particle state probabilistic teleportation scheme [J]. *Acta Photonica Sinica*, 2008 , **37**(4):825-828.
董莉,修晓明,高亚军,等. 一种两粒子任意态的概率传送方案[J]. 光子学报,2008 , **37**(4):825-828.

[18] YANG Yu-guang, CAO Wei-feng , WEN Qiao-yan. Three-party quantum secret sharing of secure direct communication based on x-type entangled states[J]. *Chinese Phys B*, 2010, **19**:050306.

[19] ZHOU Ping, DENG Fu-Guo, ZHOU Hong-Yu. Probabilisticquantum entanglement swapping and quantum secret sharing with high-dimensional pure entangled systems [J]. *Phys Scr*, 2009, **79**(3):5005-5009.

[20] LI Y M, ZHANG K S, PENG K C. Multiparty secret sharing of quantum information based on entanglement swapping[J]. *Physics Letters A*, 2004, **324**(5):420-424.

[21] DENG F G, LI C Y, LI Y S. Symmetric multiparty - controlled teleportation of an arbitrary two-particle entanglement[J]. *Physical Review A*, 2005, **72**(5):022338.

[22] DENG Fu-Guo, LI Xi-Han, LI Chun-Yan, *et al*. Multiparty quantum-state sharing of an arbitrary two-particle state with Einsten-Podolsky-Rosen pairs[J]. *Physical Review A*, 2005, **72**(4):4301-4304.

[23] CABELLO A. Quantum key distribution in the Holevo limit [J]. *Physical Review Letters*, 2000, **86**(26):5635-5638.

Quantum Secret Sharing Scheme with *N*-ordered Entangled Photon pairs

YUAN Su-zhen, SUN Zhi-fu, TIAN Jun-long

(*School of Physics and Electrical Engineering, Anyang Normal University, Anyang, Henan* 455002, *China*)

Abstract: A new quantum secret sharing scheme is proposed, based on *N*-ordered entangled photon pairs. Entangled photons are used as information carrier. Alice, the private key administrator, will divide the entangled photons into two sequences. One of the sequences will be sent to one of the partners Bob directly. After the safety of the first sequence ensured, the second sequence will be encoded and sent to another partner Charlie. Bob and Charlie will make Bell-based joint measurements with what they have received respectively, thus they obtain keys that Alice released. It needs the administrator and all the partners′ collaboration to get the whole information. Relative to there-particle entangled state, this scheme adopts two bodies entanglement, and can be experimentally realized easier. It only needs linear optical elements and simple entanglement source.

Key words: Quantum secret sharing; Entangled photon pairs; Unitary operation; Single photon measurement