第14卷 第8期 2014年3月
1671—1815(2014)08-0019-04

科 学 技 术 与 工 程
Science Technology and Engineering

Vol. 14 No. 8 Mar. 2014

通信技术

基于纠缠交换的量子密钥分发

李文骞
(南京森林警察学院,南京 210023)

摘 要 为了提高量子密钥分发的效率,提出了一种基于纠缠交换的密钥分配方案。该方案无需交换经典信息且不要进行任何酉操作,通信双方通过纠缠交换并利用贝尔测量即可生成密钥;除去少量用于检测量子信道安全的量子位,其余量子位都可以用来生成密钥,且每两对纠缠粒子就可以生成密钥的两个比特位。利用 Stinespring Dilation 定理证明了该方案的安全性并给出了效率分析。

关键词 量子通信 量子密钥分发 纠缠交换 贝尔测量
中图法分类号 TN918.1; **文献标志码** A

基于量子机制的量子密钥分配,允许相距遥远的通信双方通过传输量子信号生成共享密钥,加密传送信息。在量子密钥分配协议中,通信双方均利用量子作为信息载体来生成密钥,量子力学的基本原理保证了密钥的安全性,防止被非法用户获取。自 1984 年 Bennett 和 Brassard[1] 提出了标准的 BB84 量子密钥分配协议后,许多研究者开始对量子密钥分配进行研究,提出了若干量子密钥分配方案,这些协议大致可分为两类,一类是基于"非正交"单粒子状态的,如文献[1—3];另一类是基于纠缠状态的,如文献[4—8]。上述各量子密钥分发方案的通信双方需交换经典信息或进行酉操作来生成密钥。

本文提出一种基于纠缠交换[9—12]的量子密钥分配方案,通信双方无需交换经典信息且不需要进行酉操作,只需进行贝尔测量就可以生成密钥。该方案的高效性在于除去少量用于检测的量子位,其余量子位都可以用来生成密钥,且每两对纠缠粒子就可以生成密钥的两个比特位。文中详细证明了该方案的安全性。

1 纠缠交换的基本原理

纠缠交换(entanglement swapping)使原本没有直接相互作用的两个量子系统产生纠缠,使得远距离分布纠缠状态成为可能。由于其特殊的性质,在量子信息中起着非常重要的作用。EPR 对是处于最大纠缠态的双量子系统,它处于下列四种状态中的任一种,

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{1}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{2}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{3}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{4}$$

每种状态均称为贝尔态,显然$\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$构成双量子位系统的一个完备正交基,以这组基来测量双量子比特系统的状态称为贝尔测量。

假设通信双方 Alice 和 Bob 共享两个贝尔态$|\Phi^+{}_{1,2}\rangle$和$|\Phi^+_{3,4}\rangle$,其中 Alice 拥有粒子 1 和 4,Bob 拥有粒子 2 和 3。$|\Phi^+_{1,2}\rangle$和$|\Phi^+_{3,4}\rangle$的张量积态可以表示为

$$|\Phi^+_{1,2}\rangle\otimes|\Phi^+_{3,4}\rangle = \frac{1}{2}(|\Phi^+_{1,4}\rangle|\Phi^+_{2,3}\rangle + |\Phi^-_{1,4}\rangle|\Phi^-_{2,3}\rangle + |\Psi^+_{1,4}\rangle|\Psi^+_{2,3}\rangle + |\Psi^-_{1,4}\rangle|\Psi^-_{2,3}\rangle) \tag{5}$$

如果 Alice 对粒子 1 和 4 进行贝尔测量,则她以等概率得到$|\Phi^+_{1,4}\rangle$, $|\Phi^-_{1,4}\rangle$, $|\Psi^+_{1,4}\rangle$或$|\Psi^-_{1,4}\rangle$,那么 Bob 对粒子 2 和 3 进行贝尔测量将获得和 Alice 相同的结果,使得原本不纠缠的粒子对(1,4)、(2,3)之间分别产生纠缠。

2 基于纠缠交换的密钥分配方案

假设通信双方 Alice 和 Bob 要生成一个 $2(N-M)$ 比特的密钥,其中 N 表示 Alice 和 Bob 分别拥有的$|\Phi^+\rangle$的数目,M 表示用于检测信道安全性时 Al-

2013 年 10 月 21 日收到,10 月 30 日修改 中央高校基本科研业务费专项资金项目(LGYB201312)资助
第一作者简介:李文骞(1979—),男,讲师,研究方向:量子信息与量子信息。E-mail:zxhflwq@sina.com。

ice 和 Bob 分别消耗的$|\Phi^+\rangle$的数目。以下是本文提出的密钥分配方案：

(1)Alice 和 Bob 各自准备 N 个贝尔态 $|\Phi^+\rangle$，并分别记为 $|\Phi^+_{1,2}\rangle$ 和 $|\Phi^+_{3,4}\rangle$。Alice 将 N 个 $|\Phi^+_{1,2}\rangle$ 中所有的 1 和 2 粒子分别组成粒子序列 S_1、S_2，Bob 将 N 个 $|\Phi^+_{3,4}\rangle$ 中所有的 3 和 4 粒子分别组成粒子序列 S_3、S_4。

(2)Alice 保留粒子序列 S_1 并将 S_2 传送给 Bob，并将这一事实告知 Bob。Bob 向 Alice 确认收到粒子序列 S_2。

(3)Bob 保留粒子序列 S_3 并将 S_4 传送给 Alice，并将这一事实告知 Alice。Alice 向 Bob 确认收到粒子序列 S_4。

(4)Bob 随机选择 S_2 中 M 个粒子作为检测粒子，并告知 Alice 所选择的 M 个粒子的位置，然后随机选择 Z 基($|0\rangle$，$|1\rangle$)或 X 基($|+\rangle$，$|-\rangle$)[其中 $|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$，$|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$]对检测粒子进行测量。测量完成后，Bob 告知 Alice 对每个检测粒子进行测量所选择的测量基及测量结果。Alice 采用相同的测量基对序列 S_1 中相应位置的粒子进行测量，并将测量结果和 Bob 公布的结果进行比较。由于，

$$|\Phi^+{}_{1,2}\rangle=\frac{1}{\sqrt{2}}(|0_1 0_2\rangle+|1_1 1_2\rangle)=\frac{1}{\sqrt{2}}(|+_1+_2\rangle+|-_1-_2\rangle) \tag{6}$$

可知理想情况下，测量粒子中 Alice 的粒子 1 和 Bob 粒子 2 的测量结果应该相同。据此，若存在信道噪声或窃听者采用“测量—转发”进行信息窃取，则 Alice 和 Bob 可以检测出传输粒子序列 S_2 的错误率。Alice 和 Bob 用相同的方法检测传输序列 S_4 中相同位置的粒子，得出传输序列 S_4 的错误率。如果 S_2 或 S_4 错误率超过某个阈值，通信双方放弃本次通信，否则继续执行下一步。

(5)设去掉检测粒子后的 S_1、S_2、S_3 和 S_4 序列为 S_1'、S_2'、S_3' 和 S_4'，$S_j'(i)$ 为序列 S_j' 中第 i 个粒子。Alice 对 $S_1'(i)$ 和 $S_4'(i)$ 进行贝尔测量，Bob 对 $S_2'(i)$ 和 $S_3'(i)$ 进行贝尔测量，并分别保密各自的结果。Alice 和 Bob 约定根据测量结果生成密钥的规则，一种密钥生成规则如下：

$$|\Phi^+\rangle\rightarrow 00,\ |\Phi^-\rangle\rightarrow 01,\ |\Psi^+\rangle\rightarrow 10,\ |\Psi^-\rangle\rightarrow 11 \tag{7}$$

(6)生成初始密钥之后，Alice 和 Bob 对所生成的密钥进行信息调和和保密增强得到安全的私钥。

从上述方案可知，在无噪声量子信道和无窃听者的情况下，Alice 和 Bob 无需交换经典信息且不要进行任何酉操作，通过纠缠交换并利用贝尔测量即可生成密钥；除去少量用于检测量子信道安全的量子位，其余量子位都可以用来生成密钥，且根据密码生成规则可知每两对纠缠粒子可以生成密钥的两个比特位。

3 安全性分析

协议的安全性主要基于量子信道的安全性，也就是说如果量子信道是安全的则生成的密钥也是安全的。窃听者(Eve)只能访问 S_2 序列和 S_4 序列，不失一般性，分析 Eve 窃听 S_2 序列情况，对于 Eve 窃听 S_4 的情况与此类似。对于 2 粒子，其状态系统的密度算子为 $\rho_2=tr_1(|\Phi^+_{1,2}\rangle\langle\Phi^+_{1,2}|)=\frac{1}{2}I$，处于完全混合态，其状态是不可区分的。根据 Stinespring Dilation 定理[13]，Eve 的窃听操作可以通过作用在更大的希尔伯特(Hilbert)空间上的酉操作实现，即将酉算子 $\hat{E}$ 作用于 S_2 序列中的粒子和辅助粒子 E 上。因此 Eve 窃听之后，Alice、Bob 和 Eve 的系统状态可表示为，

$$\hat{E}|\Phi^+_{1,2}\rangle|E\rangle=a_{00}|00\rangle_{1,2}|\varepsilon_{00}\rangle+a_{01}|01\rangle_{1,2}|\varepsilon_{01}\rangle+a_{10}|10\rangle_{1,2}|\varepsilon_{10}\rangle+a_{11}|11\rangle_{1,2}|\varepsilon_{11}\rangle \tag{8}$$

式(8)中 $|\varepsilon_{ij}\rangle$ 为 Eve 引入的辅助粒子的状态，由归一化条件可得，

$$\sum_{i,j\in\{0,1\}}a_{ij}a_{ij}^*=1 \tag{9}$$

在 Alice 和 Bob 检测信道安全性的过程中，Bob 随机使用 Z 基或 X 基对检测粒子进行测量。若采用 Z 基测量检测粒子，由于 1 和 2 粒子的初始状态为 $|\Phi^+\rangle$，根据公式(6)要使窃听不被发现，则公式(8)中出现 $|01\rangle$ 和 $|10\rangle$ 的概率为 0，即有，

$$a_{01}=a_{10}=0 \tag{10}$$

由 $|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)$，公式(8)可以重新写成如下形式：

$$\begin{aligned}\hat{E}|\Phi^+_{1,2}\rangle|E\rangle=\frac{1}{2}[&(a_{00}|\varepsilon_{00}\rangle+a_{01}|\varepsilon_{01}\rangle+a_{10}|\varepsilon_{10}\rangle+a_{11}|\varepsilon_{11}\rangle)|++\rangle_{1,2}+\\&(a_{00}|\varepsilon_{00}\rangle-a_{01}|\varepsilon_{01}\rangle-a_{10}|\varepsilon_{10}\rangle+a_{11}|\varepsilon_{11}\rangle)|--\rangle_{1,2}+\\&(a_{00}|\varepsilon_{00}\rangle-a_{01}|\varepsilon_{01}\rangle+a_{10}|\varepsilon_{10}\rangle-a_{11}|\varepsilon_{11}\rangle)|+-\rangle_{1,2}+\\&(a_{00}|\varepsilon_{00}\rangle+a_{01}|\varepsilon_{01}\rangle-a_{10}|\varepsilon_{10}\rangle-a_{11}|\varepsilon_{11}\rangle)|-+\rangle_{1,2}]\end{aligned} \tag{11}$$

如果采用 X 基测量检测粒子，根据公式(6)要保证窃听不被发现，则公式(11)中出现 $|+-\rangle$ 和 $|-+\rangle$ 的概率为 0，即有，

$$\begin{cases} a_{00}\mid \varepsilon_{00}\rangle - a_{01}\mid \varepsilon_{01}\rangle + a_{10}\mid \varepsilon_{10}\rangle - a_{11}\mid \varepsilon_{11}\rangle = 0 \\ a_{00}\mid \varepsilon_{00}\rangle + a_{01}\mid \varepsilon_{01}\rangle - a_{10}\mid \varepsilon_{10}\rangle - a_{11}\mid \varepsilon_{11}\rangle = 0 \end{cases} \tag{12}$$

从而可知,

$$a_{00}\mid \varepsilon_{00}\rangle - a_{11}\mid \varepsilon_{11}\rangle = 0, a_{01}\mid \varepsilon_{01}\rangle - a_{10}\mid \varepsilon_{10}\rangle = 0 \tag{13}$$

综合公式(8)、式(10)、式(13)可得 $\hat{E}\mid \Phi^{+}_{1,2}\rangle\mid \times E\rangle = 2a_{00}(\mid 00\rangle_{1,2} + \mid 11\rangle_{1,2})\mid \varepsilon_{00}\rangle = \sqrt{2}a_{00}\mid \Phi^{+}_{1,2}\rangle\mid \varepsilon_{00}\rangle$,由归一化条件可知,$a_{00} = \frac{1}{\sqrt{2}}$。即有 $\hat{E}\mid \Phi^{+}_{1,2}\rangle\mid E\rangle = \mid \Phi^{+}{}_{1,2}\rangle\mid \varepsilon_{00}\rangle$,即 Eve 的附加粒子与粒子 1 和 2 组成的状态空间可表示成张量积关系。此时,Eve 引入的辅助粒子状态空间的密度算子为 $\rho_e = tr_{12}(\mid \Phi^{+}{}_{1,2}\rangle\mid \varepsilon_{00}\rangle\langle \varepsilon_{00}\mid \langle \Phi^{+}_{1,2}\mid) = \mid \varepsilon_{00}\rangle\langle \varepsilon_{00}\mid$。可知 von Neumann 熵 $S(\rho_e) = 0$,即如果 Eve 的窃听不被发现,那么 Eve 不可获得任何信息。综上说明 Eve 对量子信道进行窃听或被发现,否则不能获取任何有效的信息。可知文中所提方案是安全的。

4　效率分析

2000 年,Cabello[14] 根据信息论的观点,提出 QKD 方案的效率计算公式,

$$\varepsilon = \frac{b_s}{q_t + b_t} \tag{14}$$

式(14)中,b_s 为 Bob 收到的秘密信息总比特数,q_t、b_t 分别为在生成密钥过程中,Alice 和 Bob 互换的总量子比特数量和总经典比特数,但不包含用于检测量子信道安全而交换的量子比特和经典比特位。由于经检测信道安全后,密钥的生成不需要交换任何经典信息,$b_s = 2$, $q_t = 2$, $b_t = 0$,可知文中所提方案的效率 $\varepsilon = 100\%$。

事实上,传送纠缠粒子中的一个粒子与传送一个单粒子是不同的,Li 等人[15] 引入一个改进的效率计算公式,

$$\eta_t = \frac{b_s}{q_t' + b_t} \tag{15}$$

式(15)中,q_t' 为除用于检测量子信道安全消耗的量子外总耗费的量子数而不像 Cabello 定义的只考虑传输的量子。由于 $b_s = 2$, $q_t' = 4$, $b_t = 0$ 可知总的效率为 50%。

除用于检测量子信道安全消耗的量子外,其余量子均对生成密钥有贡献,该方案的量子比特效率 η_q 为 100%。这里,

$$\eta_q = \frac{q_u}{q_t'} \tag{16}$$

式(16)中,q_u 为生成量子密钥有贡献的量子数。

5　结束语

基于量子纠缠交换,提出了一种量子密钥分配方案。在该方案中通信双方各自准备一种贝尔纠缠态资源,并分别传送贝尔态的一半粒子给对方,利用纠缠交换和贝尔测量使原本没有相互作用的两个量子系统关联起来,并利用这种关联使每两对纠缠粒子生成两比特的密钥。文中证明只要保证传输信道的安全,则该方案是安全的,能得到安全的密钥。该方案无需交换任何经典信息且不要进行任何酉操作,只需双方各一次量子信道上的传输,且除去少量用于检测的量子位,其余量子位都可以通过贝尔测量生成密钥。根据 Cabello 定义的 QKD 方案的效率计算公式效率为 100%,而根据 Li 等人引入的改进的效率计算公式为 50%,同时该方案的量子比特效率为 100%,可知本文提出的 QKD 方案具有较高效率。

参　考　文　献

1　Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. IEEE International Conference on Computers, Systems & Signal Processing, Bangalore, India: IEEE Press, 1984:175—179

2　Bennett C H. Quantum cryptography using any two nonorthogonal states. Physical Review Letters, 1992; 68(21): 3121—3124

3　BruB D. Optimal eavesdropping in quantum cryptography with six states. Physical Review Letters, 1998; 81(14): 3018—3021

4　Ekert A K. Quantum cryptography based on Bell's theorem. Physical Review Letters, 1991; 67(6): 661—663

5　Bennett C H, Brassard G Mermin N D. Quantum cryptography without bell´s theorem. Physical Review Letters, 1992, 68(5): 557—559

6　Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. Physical Review A, 2002; 65(3): 032302(1)—032302(3)

7　GUO Ying, ZENG Gui-Hua. Deterministic quantum key distribution using two non-orthogonal entangled states. Communications in Theoretical Physics, 2007; 47(3): 459—463

8　Zhang X L, Zhang Y X, Gao K L. Quantum key distribution scheme based on dense encoding in entangled states. Communications in Theoretical Physics, 2005; 43(4): 627—630

9　Zukowski M, Zeilinger A, Horne M A, *et al.* Event-ready-detectors bell experiment via entanglement swapping. Physical Review Letters, 1993; 71(26): 4287—4290

10　Li C, Song H S, Zhou L, *et al.* A random quantum key distribution achieved by using bell states. Journal of Optics B: Quantum and Semiclassical Optics, 2003; 5(2): 155—157

11　许新山,张　军,陈汉武. 基于纠缠交换的第三方密钥分配. 南京邮电大学学报(自然科学版), 2011; 31(02): 59—63

12　刘林曜,胡孟军,吕洪君,等. 基于任意 bell 态的量子密钥分配.

量子电子学报, 2013; 39(04): 439—444
13 Kim B, Timo F. Deterministic secure direct communication using entanglement. Physical Review Letters, 2002; 89(18): 187902(1)—187902(4)
14 Cabello A. Quantum key distribution in the holevo limit. Physical Review Letters, 2000; 85(26): 5635—5638
15 Li X H, Deng F G, Li C Y, *et al*. Deterministic secure quantum communication without maximally entangled states. Journal of the Korean Physical Society, 2006; 49(4): 1354—1359

Quantum Key Distribution Based on Entanglement Swapping

LI Wen-qian
(Nanjing Forest Police College, Nanjing 210023, P. R. China)

[**Abstract**] In order to enhance the efficiency of quantum key distribution (QKD), a protocol based on entanglement swapping is proposed. Without classical information exchange or unitary operations, the two communication parts can securely share a session key by entanglement swapping and Bell measurement. Almost all qubits, except a few which are used to check the security of quantum channel, can produce the private key, and two pairs of entangled particles can generate two bits private key. The protocol is proved to secure using Stinespring Dilation Theorem and the efficiency analysis is presented.

[**Key words**] quantum communication quantum key distribution entanglement swapping Bell measurement

(上接第 14 页)

7 郭东道. 特征轨迹设计技术及 MATLAB 实现. 西安联合大学学报,2002;5(2):55—59
8 胡庆婉. 常微分方程初值问题的数值求解及 MATLAB 实现. 科技信息,2007;7:34—35
9 云 磊. 牛顿迭代法的 MATLAB 实现. 信息通信,2001;6:20,22

Research on Evaluation Method of Grapeshot Impact Points Distribution Uniformity

DU Ye-hong[1,2], LI Guo-fu[1], ZHAO Jing[1], HUANG Ke-wei[2]
(Ordnance Test Center[1], Baicheng 137001, P. R. China;
School of Mechatronic Engineering, Beijing Institute of Technology[2], Beijing 100081, P. R. China)

[**Abstract**] To evaluation methodological question of tactical and technical quality index raised in grapeshot type testing for impact points uniformity, two-dimensional uniformity distribution within one circle is divided into one-dimensional radial uniformity distribution and one-dimensional circumferential uniformity distribution to evaluate respectively. MATLAB is applied to achieve a method of compatibility test critical values calculation of one-dimensional uniformity distribution and compatibility test critical values of each sample size are calculated under different confidence level with the method. Sample size of compatibility test critical values is extended to meet practical requirements that pellets quantities of some types grapeshot are large.

[**Key words**] uniform distribution compatibility testing critical values MATLAB