物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

# 基于Bell态粒子和单光子混合的量子安全直接通信方案

曹正文　赵光　张爽浩　冯晓毅　彭进业

# Quantum secure direct communication protocol based on the mixture of Bell state particles and single photons

Cao Zheng-Wen　Zhao Guang　Zhang Shuang-Hao　Feng Xiao-Yi　Peng Jin-Ye

引用信息 Citation: Acta Physica Sinica, 65, 230301 (2016)　DOI: 10.7498/aps.65.230301
在线阅读 View online: http://dx.doi.org/10.7498/aps.65.230301
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2016/V65/I23

---

# 基于Bell态粒子和单光子混合的量子安全直接通信方案*

曹正文[1)2)†] 赵光[1)] 张爽浩[1)] 冯晓毅[2)] 彭进业[1)]

1) (西北大学信息科学与技术学院, 西安 710127)

2) (西北工业大学电子信息学院, 西安 710072)

( 2016 年 5 月 28 日收到; 2016 年 8 月 30 日收到修改稿 )

为了提高量子安全直接通信的效率, 本文提出了一种基于 Bell 态粒子和单光子混合的量子安全直接通信方案. 该方案中 Alice 将所有 Bell 态粒子划分为两个序列 $S_{\rm A}$ 和 $S_{\rm B}$, 先将 $S_{\rm B}$ 发给 Bob 进行第一次窃听检测, 检测结果表示量子信道安全后再将信息序列编码在序列 $S_{\rm A}$ 和单光子序列 $S_{\rm S}$ 混合的量子态序列上; 然后将已编码序列经过顺序重排和添加单光子检测粒子后发给合法接收方 Bob. 该方案避免了复杂的 U 变换, 简化了方案的实现过程. 同时顺序重排和检测粒子的结合保证了方案的安全性. 另外 3 bits 经典信息加载在一个态上的编码规则大大提高了编码容量, 从而使信息传输效率也得到提高.

**关键词**: 单光子, Bell 态, 量子安全直接通信, 传输效率

**PACS:** 03.67.Hk, 03.67.Dd **DOI:** 10.7498/aps.65.230301

## 1 引 言

近 30 年量子通信作为量子理论和信息论相结合的成果已成为一个热门的研究领域. 量子通信是应用量子力学基本原理或量子特性进行信息传输的一种新型通信方式. 量子通信主要包括基于量子密钥分发的量子保密通信 [1−3]、应用量子隐形传态和量子密集编码方法的量子间接通信和量子安全直接通信 [4−16] 等模式. 由于量子通信具有绝对安全、高信道容量、可利用量子物理纠缠资源和高效率等特点, 因此受到了人们的重视.

量子安全直接通信是利用量子力学的基本原理或量子特性通过量子信道, 在通信双方之间安全、无泄露地直接传输机密信息. 量子密钥分发与量子安全直接通信的区别是: 首先, 量子密钥分发传输的是密钥, 量子安全直接通信在量子信道中无需建立密钥直接安全传输秘密信息本身; 其次, 当发现窃听时, 前者直接丢弃此次密钥重新开始通信, 而后者由于发送的是信息本身不能像前者那样直接丢弃已发送的信息, 所以需要提前采用一些技术或者编码方法使窃听者得到的只是一些随机值, 防止窃听者窃听到有用信息. 因此量子安全直接通信的安全性要求比量子密钥分发更高. 量子安全直接通信的安全性基于量子不可克隆原理、量子测不准原理以及纠缠粒子的关联性和非定域等.

对量子安全直接通信的深入研究和探讨促进了其快速的发展. 2002 年, Long 和 Liu [4] 提出了最早的安全的量子安全直接通信方案——高效两步量子安全直接通信方案. Beige 等 [5] 首次提出基于单光子的 QSDC (quantum secure direct communication) 方案, 由于需要辅助经典信息, 故不是真正的安全直接通信. Bostrom 和 Felbinger [6] 借鉴量子密集编码的思想提出基于 EPR 纠缠粒子的 QSDC 方案, 即 Ping-Pong 方案, 但该方案仅仅为准安全. 2004 年, Cai 和 Li [7] 在其论文中证明了当存在窃听时, Ping-Pong 方案容易受到拒绝服务攻

* 陕西省自然科学基金 (批准号: 2013JM8036) 资助的课题.

† 通信作者. E-mail: caozhw@nwu.edu.cn

 

击和具有不可见光子的联合木马攻击, 因此 Ping-Pong 方案是不安全的. 2003 年, Deng 等[8] 利用量子密集编码和块传输的思想, 提出了基于纠缠对的 Two-Step QSDC 方案. 2004 年, Deng 和 Long[9] 提出基于单光子的一次一密 (one-time-pad) QSDC 方案. 2005 年, Wang[10] 提出基于量子密集编码的高维度 QSDC 方案, 该方案利用高位粒子进行密集编码, 从而每个粒子携带一个比特的经典信息. 2006 年, Wang 等[11] 提出基于单光子顺序重排的量子直接安全通信方案, 这个方案利用单光子双向传输来实现, 这个方案的安全性是基于量子无法克隆理论和单光子的秘密发送顺序, 虽采用顺序重排, 但仍然不能克服木马攻击. 2007 年, 王剑等[12,13] 提出基于纠缠交换的量子安全通信方案和多方控制的量子直接安全通信方案. 2008 年, 王天银等[14] 针对王剑的多方控制的 QSDC 方案的不足, 提出一种改进的多方控制的 QSDC 方案, 并分析表明该方案可以抵抗一种新的伪信号替换攻击. 2010 年, 权东晓等[15] 提出基于单光子的单向量子安全直接通信方案. 2012 年, 李凯等[16] 提出一种基于 EPR 序列的量子安全直接通信方案.

为避免复杂的 U 变换, 简化方案, 提高信息传输效率, 本文提出了基于 Bell 态粒子和单光子混合的量子安全直接通信方案. 首先, 介绍该方案的具体实现过程; 然后, 分别从量子力学理论和信息论角度分析安全性; 最后, 计算本方案的通信传输效率和量子比特利用率.

## 2 方案描述

假定 Alice 和 Bob 为量子通信过程中合法的发送方和接收方. 本方案执行的具体步骤如下.

1) Alice 制备一串单光子序列和一串 Bell 态序列即 EPR 纠缠粒子对. 每个单光子随机地处于 $|H\rangle$, $|V\rangle$, $|L\rangle$, $|R\rangle$ 四个态中的其中一个. 每对 Bell 态随机地处于 $|\varphi^-\rangle$, $|\psi^+\rangle$, $|\psi^-\rangle$, $|\varphi^+\rangle$ 四个态中的其中一个, 抽取所有 Bell 态中的第一个粒子可构成序列 $S_{\rm A}$, 所有剩余的第二个粒子构成序列 $S_{\rm B}$.

2) Alice 将 $S_{\rm B}$ 发给 Bob 而将 $S_{\rm A}$ 本地保留. Bob 收到序列 $S_{\rm B}$ 后随机地选取部分粒子进行单光子测量, 即 Bob 随机选取 $Z$ 基 $\{|0\rangle, |1\rangle\}$ 或 $X$ 基 $\{|+\rangle, |-\rangle\}$ 对抽样粒子进行测量, 并将自己测量完后的结果、位置及其测量基信息通过不能被篡改的经典信道发给 Alice.

3) Alice 收到 Bob 发送的信息后, 利用和 Bob 相同的测量基在 $S_{\rm A}$ 中对与 Bob 抽样粒子对应位置上的粒子进行单光子测量, 并将自己的测量结果与 Bob 发送过来的测量结果作对比, 分析错误率. Alice 根据错误率判断量子信道是否存在 Eve 的窃听. 若错误率高于初期定好的可容忍的阈值, 放弃已接收序列且终止通信, 如果低于初期定好的可容忍的阈值则说明量子信道中不存在窃听者 Eve, 可以进行下一步通信.

4) Alice 按照之前约定好的编码规则, 将信息序列 $M$ 编码在序列 $S_{\rm A}$ (去除用于安全检测的粒子) 和单光子序列 $S_{\rm S}$ 上, 形成混合量子态编码序列 $S_{\rm A\text{-}S}$. 编码规则如表 1 所示.

5) Alice 先将已编码序列 $S_{\rm A\text{-}S}$ 顺序重排构成新序列 $S_1$, 再加入部分用于窃听检测的单光子构成发送序列 $S_2$ 发给 Bob.

6) Bob 收到序列 $S_2$ 后利用光纤中的光延时对其进行延迟, 以防公布位置后部分量子态未发送完导致信息泄露. Alice 公布检测粒子的位置信息, Bob 对这些检测粒子进行单光子测量, 如同步骤 2. Alice 利用 Bob 告知的测量基信息对序列 $S_2$ 中的检测粒子进行测量, 并将测量结果与 Bob 告知的测量结果作对比, 分析错误率, 如同步骤 3.

7) Alice 将序列 $S_1$ 原来的顺序、位置和测量基信息发给 Bob. Bob 按照 Alice 告知的信息恢复原编码序列 $S_{\rm A\text{-}S}$ 并对其进行相应的 $Z$ 基 $\{|0\rangle, |1\rangle\}$ 测量或 $X$ 基 $\{|+\rangle, |-\rangle\}$ 测量或 Bell 基联合测量, 将测量结果结合编码规则进行译码, 最终得到原信息序列 $M$.

表 1 本协议编码方案

Table 1. The code scheme of this protocol.

| 信息序列 | 量子态 | 信息序列 | 量子态 |
|---|---|---|---|
| 000 | $\|H\rangle$ | 100 | $\|\varphi^+\rangle$ |
| 001 | $\|V\rangle$ | 101 | $\|\varphi^-\rangle$ |
| 010 | $\|L\rangle$ | 110 | $\|\psi^+\rangle$ |
| 011 | $\|R\rangle$ | 111 | $\|\psi^-\rangle$ |

光源使用 Bell 态粒子和单光子的混合, 是为了达到更高的编码容量, 即一个量子态可以加载 3 bits 的经典信息, 从而可以提高信道容量和通信传输效率. 第一次的安全性检测目的是确保信道的安全, Bob 获得的 $S_{\rm B}$ 可信. 若 Eve 采取测量重发或截获重发攻击, 则在第一次安全性检测中就可以被发现; 若 Eve 采取辅助粒子攻击, 即使 Eve 逃过

第一次检测, 但因不能对 Bell 态划分的两个序列中对应粒子进行 Bell 基联合测量, 所以最终无法获取合法通信者的秘密信息. 第二次安全性检测目的是为了判断编码序列传输过程中是否存在窃听者恶意破坏纠缠量子态的关联性, 从而判断有没有必要对已传输的结果做纠错等数据后处理.

综合上序步骤, 用流程图描述一下本方案. 具体实现过程如图 1 所示.

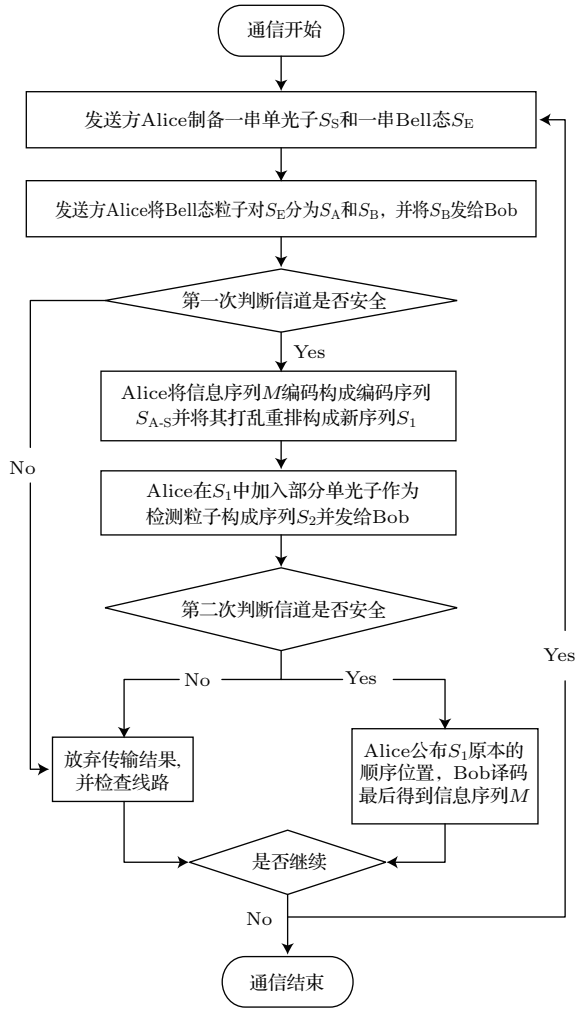


图 1 协议流程图

Fig. 1. The flow chat of this protocol.

从流程图可归纳出本文方案的步骤主要包括: Alice 的制备过程, Alice 的编码过程, Alice 形成新序列过程, 窃听检测过程, Bob 译码获取信息序列过程.

## 3 安全性分析

量子安全直接通信的安全性是指没有 Eve 窃听或者即使 Eve 窃听也得不到有用信息. 本方案的安全性基于量子不可克隆定理和编码光子序列的秘密传输顺序. 下面从几种典型攻击模式和信息论的角度分析本方案的安全性.

### 3.1 典型攻击模式下的安全性分析

测量重发和截获重发攻击: 测量重发攻击是指在 Alice 编码发送序列发给 Bob 的过程中, 窃听者 Eve 俘获 Alice 的发送序列, 然后随机选取测量基 $Z$ 基 $\{|0\rangle, |1\rangle\}$ 或 $X$ 基 $\{|+\rangle, |-\rangle\}$ 或者 Bell 基进行单光子测量或 Bell 基测量, 并将测量后的序列发给 Bob. 我们的信息序列编码后顺序重排又添加部分检测粒子, 就算 Eve 捕获一部分光子并选对测量基, 但由于不知编码序列的顺序、位置的信息, 故 Eve 得不到有用信息且由于窃听检测测量重发攻击不可能不被发现. 截获重发攻击是指在 Alice 发送序列给 Bob 的过程中, 窃听者 Eve 截获部分发送序列, 并将自己准备好的一串粒子重新发给 Bob. 没有原序列的顺序和随机序列数值, Eve 只获得了一批毫无意义的随机数, 且 Eve 的攻击将会在窃听检测中被发现.

辅助粒子攻击: 窃听者 Eve 提前制备好辅助粒子, 然后截获 Alice 发给 Bob 的粒子. 然后用自己的辅助粒子对截获粒子进行纠缠, 即对两个粒子执行一个幺正变换, 根据海森堡测不准原理和不可克隆原理, Eve 不可能在不引起任何错误的情况下通过辅助粒子来获取有用信息.

拒绝服务攻击: Eve 对俘获到的光子只采取随机的操作来破坏量子信道传输的信息, 自己不试图获取任何有用信息, 但是随机的操作肯定会引起光子状态的改变, 肯定会通过窃听检测被发现 [15].

木马攻击: 存在于双向通信方案中, 主要包括不可见光子木马攻击 [17] 和时间延迟攻击 [18]. 本方案是单向通信从而可以避免木马攻击. 2006 年, Wang 等 [11] 提出基于单光子顺序重排的量子直接安全通信方案, 这个方案利用单光子双向传输来实现, 故不能克服木马攻击. 如果对序列只采取 I 或者 Y 操作, Eve 可以通过截获重发攻击 (intercept-resend attack) 获得控制有用信息.

### 3.2 基于信息论的安全性分析

从信息论的角度分析方案的安全性, 可以更加清楚地说明 Eve 的窃听行为无法逃脱通信双方的窃听检测. 测量重发是 Eve 随机选取测量基对俘

获粒子进行测量, 并将测量后的量子态发给Bob. 测量单光子或 Bell 态粒子并重发引起的检测粒子错误率为 1/4. 若含有 $n$ 个俘获粒子则窃听被检测到的概率为 $(1/4)^n$. 显然 $n$ 越小, 窃听被检测到的概率就越大. 截获重发是 Eve 俘获部分粒子, 然后将自己提前准备好的量子态发给 Bob. 截获单光子并重发引起的检测粒子错误率为 3/4. 若含有 $n$ 个俘获粒子则窃听被检测到的概率为 $(3/4)^n$. 截获 Bell 态粒子并重发引起的检测粒子错误率为 1/4. 若含有 $n$ 个俘获粒子则窃听被检测到的概率为 $(1/4)^n$.

辅助粒子攻击是 Eve 借助辅助粒子对俘获粒子进行纠缠, 即 Eve 对窃听系统和发送量子态组成的一个更大的希尔伯特空间(复合系统)做幺正操作. 测量重发和截获重发攻击都没有进行幺正操作. Eve 的这个幺正操作会引起一定的错误率以及辅助粒子和俘获粒子的纠缠. 所以论文对于 Eve 的幺正操作所引起的错误率(窃听被检测到的概率)和纠缠后 Eve 的系统状态进行具体分析. 基本思想是首先计算 Eve 窃听攻击被检测到的概率, 然后计算 Eve 可访问的最大信息量 $I_{\rm E}$, 根据该信息量可以判定方案的安全性. 本方案中加载信息的量子比特包括 Bell 态粒子和单光子, 所以计算 Eve 窃听攻击被检测到的概率时分为攻击单光子和 Bell 态纠缠粒子两种情况.

1) 当 Eve 借助辅助粒子 $|e\rangle$ 对俘获的单光子进行识别时, 假设并没有改变单光子的状态.

$$\hat{E}\otimes|0e\rangle = a|0e_{00}\rangle + b|1e_{01}\rangle, \tag{1}$$

$$\hat{E}\otimes|1e\rangle = b'|0e_{10}\rangle + a'|1e_{11}\rangle, \tag{2}$$

$$\begin{aligned}&\hat{E}\otimes|+e\rangle\\ &= \frac{1}{\sqrt{2}}\left(a|0e_{00}\rangle + b|1e_{01}\rangle + b'|1e_{10}\rangle + a'|1e_{11}\rangle\right)\\ &= \frac{1}{2}[|+\rangle\left(a|e_{00}\rangle + b|e_{01}\rangle + b'|e_{10}\rangle + a'|e_{11}\rangle\right)\\ &\quad + |-\rangle\left(a|e_{00}\rangle - b|e_{01}\rangle + b'|e_{10}\rangle - a'|e_{11}\rangle\right)], \end{aligned}\tag{3}$$

$$\begin{aligned}&\hat{E}\otimes|-e\rangle\\ &= \frac{1}{\sqrt{2}}\left(a|0e_{00}\rangle + b|1e_{01}\rangle - b'|1e_{10}\rangle - a'|1e_{11}\rangle\right)\\ &= \frac{1}{2}[|+\rangle\left(a|e_{00}\rangle + b|e_{01}\rangle - b'|e_{10}\rangle - a'|e_{11}\rangle\right)\\ &\quad + |-\rangle\left(a|e_{00}\rangle - b|e_{01}\rangle - b'|e_{10}\rangle + a'|e_{11}\rangle\right)], \end{aligned}\tag{4}$$

其中, $\{e_{00}, e_{01}, e_{10}, e_{11}\}$ 为算符 $\hat{E}$ 所决定的四个纯态, 满足归一化条件:

$$\sum_{\alpha,\beta\in\{0,1\}}\langle e_{\alpha,\beta}|e_{\alpha,\beta}\rangle = 1. \tag{5}$$

Eve 的幺正操作 $\hat{\boldsymbol{E}}$ 的矩阵形式可表示为

$$\hat{\boldsymbol{E}} = \begin{pmatrix} a & b' \\ b & a' \end{pmatrix}. \tag{6}$$

由于 $\hat{\boldsymbol{E}}\hat{\boldsymbol{E}}^* = \boldsymbol{I}$, 所以 $a$, $b$, $a'$ 和 $b'$ 满足以下关系:

$$\begin{aligned} |a|^2 + |b|^2 &= 1,\\ |a'|^2 + |b'|^2 &= 1,\\ ab^* &= (a')^* b'. \end{aligned}\tag{7}$$

进而得出

$$|a|^2 = |a'|^2, \quad |b|^2 = |b'|^2. \tag{8}$$

在安全检测的时, Eve 的窃听被检测到的概率, 即 Eve 引起的错误率为

$$P_{\rm error} = |b|^2 = 1 - |a|^2 = |b'|^2 = 1 - |a'|^2. \tag{9}$$

2) 如果 Eve 俘获 Bell 态纠缠粒子并对其进行窃听攻击即对量子信道中的量子态进行幺正操作 $\hat{E}$, 攻击之后粒子状态 $|0\rangle$ 和 $|1\rangle$ 分别变为

$$\hat{E}\otimes|0e\rangle = a|0e_{00}\rangle + b|1e_{01}\rangle, \tag{10}$$

$$\hat{E}\otimes|1e\rangle = b'|0e_{10}\rangle + a'|1e_{11}\rangle. \tag{11}$$

假设 Eve 攻击了EPR纠缠粒子中的 $|\varphi^+\rangle$ 态之后整个系统的状态变为

$$\begin{aligned}|\varphi\rangle_{\rm Eve} &= E\otimes\frac{|0e\rangle\otimes|0\rangle + |1e\rangle\otimes|1\rangle}{\sqrt{2}}\\ &= \frac{1}{\sqrt{2}}\big[\left(a|0e_{00}\rangle + b|1e_{01}\rangle\right)\otimes|0\rangle\\ &\quad + \left(b'|0e_{10}\rangle + a'|1e_{11}\rangle\right)\otimes|1\rangle\big]\\ &= \frac{1}{\sqrt{2}}\big(a|0e_{00}0\rangle + b|1e_{01}0\rangle\\ &\quad + b'|0e_{10}1\rangle + a'|1e_{11}1\rangle\big). \end{aligned}\tag{12}$$

Alice 对 $|\varphi^+\rangle$ 的检测粒子做测量时, 当且仅当 $|a| = |a'|$ 时, 没有窃听的概率是

$$P_{\rm Eve} = \frac{|a|^2 + |a'|^2}{2} = |a|^2, \tag{13}$$

故窃听被检测到的概率, 即 Eve 引起的错误率为

$$P_{\rm error} = 1 - P_{\rm Eve} = 1 - |a|^2 = 1 - |a'|^2. \tag{14}$$

所以在辅助粒子攻击下, Eve为识别俘获粒子的状态, 肯定会干扰其状态的改变, 必然会在稍后的窃听检测过程中被合法通信方发现.

每一个光子的约化密度矩阵为

$$\boldsymbol{\rho} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{15}$$

从中可以看出 Eve 对光子的测量会以相等的概率 0.5 得到 $|0\rangle$ 或者 $|1\rangle$. 如果 Alice 的粒子量子态是 $|0\rangle$, 则 Eve 进行攻击后状态是

$$|\psi\rangle_{\mathrm{Eve}} = \hat{E} \otimes |0e\rangle = a|0e_{00}\rangle + b|1e_{01}\rangle. \tag{16}$$

以 $|0e_{00}\rangle$, $|1e_{01}\rangle$ 为基, 且 $aa^* = |a|^2$, $bb^* = |b|^2$, 则有

$$\begin{aligned} \rho' &= |\psi\rangle_{\mathrm{Eve}}\langle\psi|_{\mathrm{Eve}} \\ &= |a|^2|0e_{00}\rangle\langle 0e_{00}| + |b|^2|1e_{01}\rangle\langle 1e_{01}| \\ &\quad + ab^*|0e_{00}\rangle\langle 1e_{01}| + a^*b|1e_{01}\rangle\langle 0e_{00}|, \end{aligned} \tag{17}$$

用矩阵表示为

$$\boldsymbol{\rho}' = \begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix}. \tag{18}$$

求解密度算子 $\rho'$ 的特征值 $\lambda$

$$\det\begin{bmatrix} |a|^2 - \lambda & ab^* \\ a^*b & |b|^2 - \lambda \end{bmatrix} = 0, \tag{19}$$

特征方程为

$$(|a|^2 - \lambda) \times (|b|^2 - \lambda) - ab^* \times a^*b = 0. \tag{20}$$

解方程得到 $\rho'$ 的两个特征值, 是常数, $\lambda_0 = 0$, $\lambda_1 = 1$. 因此 Eve 的 Von-Neumann 熵为

$$I_{\mathrm{E}} = \chi(\rho') = -\sum_{i=0}^{1}\lambda_i \log_2 \lambda_i = 0. \tag{21}$$

由 (21) 式可以看出, 即使 Eve 采用 U 操作对发送中的量子态进行窃听, 获得的平均互信息仍为 0.

根据信息论可知, Eve 在量子系统中可访问的最大信息量受限于 Holevo 限:

$$\chi(\rho) = S(\rho) - \sum_{i=1}^{8} p_i S(\rho_i), \tag{22}$$

其中, $S(\rho)$ 为态 $\rho$ 的 Von-Neumann 熵, $\rho = \sum_{i=1}^{8} p_i\rho_i$, $\rho_i$ 是通信以概率 $p_i$ 制备的量子态, 如果通信发送方 Alice 以 1/8 的概率发送信息 “000”, “001”, “010”, “011”, “100”, “101”, “110”, “111”, 那么发送的信息熵为

$$\begin{aligned} H(p) = & -p_{000}\log_2 p_{000} - p_{001}\log_2 p_{001} \\ & - p_{010}\log_2 p_{010} - p_{011}\log_2 p_{011} \\ & - p_{100}\log_2 p_{100} - p_{101}\log_2 p_{101} \\ & - p_{110}\log_2 p_{110} - p_{111}\log_2 p_{111} \\ = & \ 3, \end{aligned} \tag{23}$$

因此,

$$I_{\mathrm{E}} = \chi(\rho') = S(\rho') - \sum_{i=1}^{8} p_i S(\rho_i') < H(p). \tag{24}$$

由此可知, Eve 所得到的信息 $I_{\mathrm{E}} = 0$, 且 Alice 和 Bob 之间的互信息为 3, 说明基于我们的方案量子信道中不存在窃听者 Eve.

## 4 效率和编码容量分析

从信息论角度定义量子密码方案的效率为

$$\xi = \frac{b_s}{q_{\mathrm{t}} + b_{\mathrm{t}}}, \tag{25}$$

其中, $b_s$ 为通信双方在通信中交换的有用信息比特数, $q_{\mathrm{t}}$ 为通信过程中的量子比特数, $b_{\mathrm{t}}$ 为通信过程中的经典比特数 [19]. 计算传输效率时不考虑与窃听检测有关的经典比特、测量基及位置信息. 由传输效率公式可知本方案的传输效率提高到

$$\xi = \frac{b_s}{q_{\mathrm{t}} + b_{\mathrm{t}}} = \frac{n}{n/3 + n/6} = 2\text{倍}.$$

量子比特利用率被定义为

$$\eta = \frac{q_{\mathrm{u}}}{q_{\mathrm{t}}}, \tag{26}$$

其中, $q_{\mathrm{u}}$ 为携带信息的有用量子比特, $q_{\mathrm{t}}$ 为传输的总量子比特 [19]. 由量子比特利用率公式可知, 本方案的量子比特利用率为 $\eta = q_{\mathrm{u}}/q_{\mathrm{t}} = 1$.

Bostrom 与 Felbinger 提出的基于 EPR 纠缠粒子的 QSDC 方案, 即 Ping-Pong 方案, 假设 Alice 每发送一个经典比特的信息均需要进行一次控制模式, 这里的控制模式相当于窃听模式, 通信的效率为 $\xi = b_s/(q_{\mathrm{t}} + b_{\mathrm{t}}) = n/3n \approx 0.33$, 量子比特利用率为 $\eta = q_{\mathrm{u}}/q_{\mathrm{t}} \approx 0.33$. 按照本方案定义的公式, 分析文献中具有代表性的方案并计算其量子通信传输效率、量子比特利用率. 将他们与本方案的量子通信传输效率、量子比特利用率作为对比, 结果如表 2 所列.

表 2 参数对比

Table 2. Comparison on parameters.

| 协议 | 传输效率 $\xi$ | 量子比特率 $\eta$ | 编码容量 |
|---|---|---|---|
| Ping-Pong 协议 | 0.33 | 0.33 | 一个态: 1 bit |
| 邓富国 Two-Step QSDC 协议 | 1 | 1 | 一个态: 2 bits |
| 邓富国 One-Pad-Time QSDC 协议 | 1 | 1 | 一个态: 1 bit |
| 王剑基于纠缠交换的 QSDC 协议 | 1 | 1 | 一个态: 2 bits |
| 权东晓基于单光子的单向 QSDC 协议 | 0.5 | 1 | 一个态: 1 bit |
| 本协议 | 2 | 1 | 一个态: 3 bits |

从表 2 中可明显看出本方案的优势: 一个量子态可以表示 3 bits 的经典信息, 较高的编码容量使得量子通信的传输效率大大提高.

## 5 结 论

本文基于 Bell 态粒子和单光子提出一种新的量子安全直接通信方案. 本方案利用两次窃听检测和顺序重排保证了通信信道和编码序列的安全, 并分别从量子力学基本原理和量子信息论的角度证明了方案的安全性. 与以往方案相比, 本方案优点是避免了复杂的 U 操作, 简化了通信过程; Bell 态粒子和单光子混合的编码规则保证了较高的编码容量, 从而提高了通信效率. 本方案主要是理论研究, 实际应用仍存在一定的难度. 与基于单光子的 QSDC 方案相比较, 本方案不仅需要制备和测量单光子, 还需要制备和联合测量 Bell 态, 并需要利用量子态存储技术. 单光子的制备和测量可利用单光子源、单光子检测器和一些线性光学器件来实现, 量子态的存储技术在实际应用中还不成熟, 考虑采用光学延迟方式实现. 基于现有的技术条件, Bell 态的制备与测量以及如何将 Bell 态和单光子混合还存在一定的实现难度, 有待于以后量子实用技术的发展与突破.

## 参考文献


[1] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (New York: IEEE Press) p175

[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[3] Wang X B 2005 *Phys. Rev. A* **72** 012322

[4] Long G L, Liu X S 2002 *Phys. Rev. A* **65** 032302

[5] Beige A, Englert B G, Kurtsiefer C 2002 *J. Phys. A: Math. Gen.* **35** L407

[6] Bostrom K, Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

[7] Cai Q Y, Li B W 2004 *Phys. Rev. A* **69** 054301

[8] Deng F G, Long G L, Liu X S 2003 *Phys. Rev. A* **68** 042317

[9] Deng F G, Long G L 2004 *Phys. Rev. A* **69** 052319

[10] Wang C, Deng F G, Li Y S 2005 *Phys. Rev. A* **71** 044305

[11] Wang J, Zhang Q, Tang C J 2006 *Phys. Lett. A* **358** 256

[12] Wang J, Chen H Q, Zhang Q, Tang C J 2007 *Journal of National University of Defense Technology* **29** 56 (in Chinese) [王剑, 陈皇卿, 张权等, 唐朝京 2007 国防科技大学学报 **29** 56]

[13] Wang J, Chen H Q, Zhang Q, Tang C J 2007 *Acta Phys. Sin.* **56** 673 (in Chinese) [王剑, 陈皇卿, 张权, 唐朝京 2007 物理学报 **56** 673]

[14] Wang T Y, Qin H J, Wen Q Y, Zhu P C 2008 *Acta Phys. Sin.* **57** 7452 (in Chinese) [王天银, 秦海娟, 温巧燕, 朱甫臣 2008 物理学报 **57** 7452]

[15] Quan D X, Pei C X, Liu D, Zhao N 2010 *Acta Phys. Sin.* **59** 2493 (in Chinese) [权东晓, 裴昌辛, 刘丹, 赵楠 2010 物理学报 **59** 2493]

[16] Li K, Huang X Y, Teng J H, Li Z H 2012 *Journal of Electronics Information Technology* **34** 1917 (in Chinese) [李凯, 黄晓英, 滕吉红, 李振华 2012 电子与信息学报 **34** 1917]

[17] Li X H, Deng F G, Zhou H Y 2006 *Phys. Rev. A* **74** 054302

[18] Cai Q Y 2006 *Phys. Lett. A* **351** 23

[19] Wang J, Zhang S, Zhang Q, Zhang S L 2009 *Journal of National University of Defense Technology* **31** 51 (in Chinese) [王剑, 张盛, 张权, 张盛林 2009 国防科技大学学报 **31** 51]

# Quantum secure direct communication protocol based on the mixture of Bell state particles and single photons*

Cao Zheng-Wen[1)2)†] Zhao Guang[1)] Zhang Shuang-Hao[1)] Feng Xiao-Yi[2)] Peng Jin-Ye[1)]

1) (*School of Information Science and Technology, Northwest University, Xi'an 710127, China*)

2) (*School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710072, China*)

( Received 28 May 2016; revised manuscript received 30 August 2016 )

**Abstract**

By studying the properties of the mixture of Bell state particles and single photons, in the paper we design a quantum code scheme with high coding capacity, and propose a novel quantum secure direct communication protocol with high transmission efficiency. Alice prepares Bell state particles and single photons, and divides Bell state particles into two sequences $S_{\rm A}$ and $S_{\rm B}$. $S_{\rm B}$ is sent to Bob for the first security check through using quantum correlation properties of particles. When the check result shows that the quantum channel is safe, by using the designed quantum code scheme, Alice encodes her classical message on the mixed quantum state sequence of Bell sequence $S_{\rm A}$ and single photon sequence $S_{\rm S}$. Then, some single photons that are used for security check are re-inserted randomly into the encoded sequence, and the order of particles is rearranged to ensure checking Eve's attack. Alice sends the new sequence to Bob. Bob delays and receives it. And then, the quantum channel conducts the second-time security check. The transmission error rate is calculated, and if the error rate is lower than the tolerance threshold, the channel is safe. Bob decodes and reads Alice's message. The first security check is to determine whether quantum channel is safe. The second security check is to test whether there are eavesdroppers during information transmission. Safety analysis is done by applying the quantum information theory for the proposed protocol. The error rate introduced by Eve and the amount of information by Eve are calculated. It is shown that this pro-tocol can effectively resist measurement-resend attack, intercept-resend attack, auxiliary particle attack, denial of service attack and Trojan attack. Among them, auxiliary particle attack is analyzed in detail. The transmission efficiency and coding capacity are also analyzed. The transmission efficiency is 2, the quantum bit rate is 1, and the coding capacity is that a quantum state can encode three bits of classical messages. We also compare the proposed protocol with many existing popular protocols in the sense of efficiency, e.g., Ping-Pong protocol, Deng F G *et al.*'s two-step and one-pad-time quantum secure direct communication protocol, Wang J *et al.*'s quantum secure direct communication protocol based on entanglement swapping and Quan D X *et al.*'s one-way quantum secure direct communication protocol based on single photon. It is proved that this proposed protocol has higher transmission efficiency. In addition, neither complex U operation nor entanglement swapping is used, and implementation process is simplified. However, this protocol is devoted to theoretical research of quantum secure direct communication. There are still some difficulties in the practical application. For example, the storage technology of quantum states is not mature at present. It is not easy to prepare and measure Bell state particles nor to combine them with single photons, and so on. The implementation of this protocol depends on the development of quantum technology in the future.

**Keywords:** single photon, Bell state, quantum secure direct communication, transmission efficiency

**PACS:** 03.67.Hk, 03.67.Dd **DOI:** 10.7498/aps.65.230301

* Project supported by the Natural Science Foundation of Shaanxi Province,China (Grant No. 2013JM8036).

† Corresponding author. E-mail: caozhw@nwu.edu.cn