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

基于单光子的高效量子安全直接通信方案

赵宁　江英华　周贤韬

Efficient quantum secure direct communication scheme based on single photons

Zhao Ning　Jiang Ying-Hua　Zhou Xian-Tao

引用信息 Citation: Acta Physica Sinica, 71, 150304 (2022)　DOI: 10.7498/aps.71.20220202
在线阅读 View online: https://doi.org/10.7498/aps.71.20220202
当期内容 View table of contents: http://wulixb.iphy.ac.cn

您可能感兴趣的其他文章
Articles you may be interested in

基于单光子双量子态的确定性安全量子通信
Deterministic secure quantum communication with double-encoded single photons
物理学报. 2022, 71(5): 050302　https://doi.org/10.7498/aps.71.20210907

基于高维单粒子态的双向半量子安全直接通信协议
Bi-directional semi-quantum secure direct communication protocol based on high-dimensional single-particle states
物理学报. 2022, 71(13): 130304　https://doi.org/10.7498/aps.71.20211702

半导体自组织量子点量子发光机理与器件
Physics and devices of quanutm light emission from semicoductor self-assembled quantum Dots
物理学报. 2018, 67(22): 227801　https://doi.org/10.7498/aps.67.20180594

半导体上转换单光子探测技术研究进展
Research progress of semiconductor up-conversion single photon detection technology
物理学报. 2018, 67(22): 221401　https://doi.org/10.7498/aps.67.20180618

单光子激光测距的漂移误差理论模型及补偿方法
Theoretical model and correction method of range walk error for single-photon laser ranging
物理学报. 2018, 67(6): 064205　https://doi.org/10.7498/aps.67.20172228

基于Cayley图上量子漫步的匿名通信方案
Anonymous communication scheme based on quantum walk on Cayley graph
物理学报. 2020, 69(16): 160301　https://doi.org/10.7498/aps.69.20200333

基于单光子的高效量子安全直接通信方案

赵宁† 江英华 周贤韬

(西藏民族大学信息工程学院, 咸阳 712000)

(2022 年 1 月 28 日收到; 2022 年 3 月 28 日收到修改稿)

首先介绍了单次发送单光子的量子安全直接通信方案的具体步骤. 基于该方案的基本步骤, 逐步扩展到分两次和分四次发送单光子序列的量子安全直接通信方案, 重点介绍各方案对应的编码规则. 分析上述方案的效率可以看出, 发送次数的增加可以增加单光子的分类, 大大提高每个单光子的编码容量和整个通信中量子态的传输效率. 最后提出有通用性的分 n (n 为 2 的整数次幂) 次发送单光子来进行量子安全直接通信的方案及其编码规则, 经过安全性分析证明方案安全可行. 通过效率分析, 该方案比现有方案的通信效率更高, 而且该方案的实施只用到单光子, 不涉及量子纠缠, 实现难度更小.

关键词: 单光子, 多次发送, 编码规则, 效率分析

PACS: 03.67.Hk, 03.67.Dd **DOI**: 10.7498/aps.71.20220202

1 引 言

量子通信是近半个世纪提出的一种新型的交叉性学科, 主要依据量子力学的一些基础性原理与性质 [1]. 学者们在对量子领域的研究中发现了其存在的通信价值, 并尝试将其引入通信领域, 加入信息学等诸多领域的知识形成了现在的量子通信 [2]. 量子通信相较于传统的通信方式有着极大的优势, 理论上可以使通信达到绝对的安全 [3], 在发现量子通信存在的潜力后, 诸多专家努力对该领域进行更加深入的研究. 近几年越来越多关于量子领域的通信协议被提出, 目的是形成更加高效安全 [4] 的量子通信方案.

目前在量子通信领域, 中国走在世界领先位置, 墨子号量子卫星 [5] 的成功发射, 更是该领域能够应用于实践的一个有力证明. 在新时代科技强国的背景下, 我国在新的五年计划中也提到要更加重视量子通信的发展. 不仅中国, 美国、欧盟、日本等世界领先的发达经济体都提出要在该领域进行大笔投入, 将量子通信作为重点发展战略之一.

在量子通信协议的研究中, 包括量子安全直接通信 (QSDC)[6–9], 如邓富国的 Two-Step QSDC 协议 [10,11], 权东晓等 [12] 基于单光子的单向 QSDC 协议. 近几年相继提出的单光子与 Bell 态结合 [13–15], 单光子与 GHZ 态结合的 QSDC 协议 [16,17], 在研究了这些基于单光子与纠缠态粒子结合的混合态量子安全直接通信协议后, 发现对于此类协议, 纠缠态粒子在通信效率方面表现得并没有单光子高效, 纠缠态粒子的使用会造成协议中传输效率和编码容量降低. 针对这个发现, 尝试仅利用单光子完成 QSDC 通信, 以达到更高的通信效率. 因此需要对发送的单光子进行分类, 本文提出利用多次发送的方式将单光子分类, 在传输效率和编码效率上要高于单光子与其他纠缠态粒子混合的量子安全直接通信方案, 且此方案的应用难度更小.

2 方案描述

在制定编码规则时, 要确保单次发送单光子序

† 通信作者. E-mail: 1720277914@qq.com

© 2022 中国物理学会 Chinese Physical Society

列中, 同一测量基下的两种量子态表示的经典比特不存在相同部分, 以免第三方通过 Alice 公布的正确测量基推断出部分秘密信息. 如 2.1 节中公布正确测量基 Z 基对应的量子态 $|0\rangle$ 表示 00, $|1\rangle$ 表示 11, 第三方从公布的测量基中无法得到任何秘密信息. 若 $|0\rangle$ 表示 00, $|1\rangle$ 表示 01, 则第三方可根据公布的 Z 测量基得出秘密信息中两比特经典信息的第一位为 0, 造成信息泄漏.

假设以下通信方案中为合法通信双方, 发送方为 Alice, 接收方为 Bob.

2.1 单次发送单光子的 QSDC 方案

步骤 1 Alice 制备一串单光子, 并按照以下编码规则将秘密信息 M 编码在单光子序列上, Alice 记下编码后的单光子序列 S, 然后打乱顺序并加入检测粒子发送给接收方 Bob. 具体编码规则如下见表 1.

表 1 编码规则一

Table 1. Coding Rule 1.

信息序列	量子态	信息序列	量子态
00	$\|0\rangle$	10	$\|+\rangle$
11	$\|1\rangle$	01	$\|-\rangle$

步骤 2 窃听检测. Bob 在收到所有信息后告知 Alice, Alice 公布发送序列中检测粒子的位置和对应的测量基, Bob 根据 Alice 公布的检测粒子的位置和测量基对检测粒子进行测量, 并将测量结果发送给 Alice. Alice 将 Bob 的测量结果与加入检测粒子的初始态进行对比, 若误差率高于双方设定的安全阈值, 则可能存在第三方窃听, 放弃通信. 若低于阈值, 则通信安全, Alice 进行后续步骤.

步骤 3 Alice 向 Bob 公布单光子序列 S 的排列顺序及正确的测量基序列. Bob 根据 Alice 公布的排列顺序, 还原 S 并选择正确的测量基序列进行测量. 利用编码规则对测量结果解码得出秘密信息 M.

综上步骤, 方案流程图如图 1 所示. 从图 1 可以看出, Alice 向 Bob 发送一次单光子序列并加入检测粒子, 即可完成信息传输和窃听检测. 后续提出的多次发送都是以图 1 中的方案步骤为基础进行多次发送, 将单光子序列分类并提高传输效率.

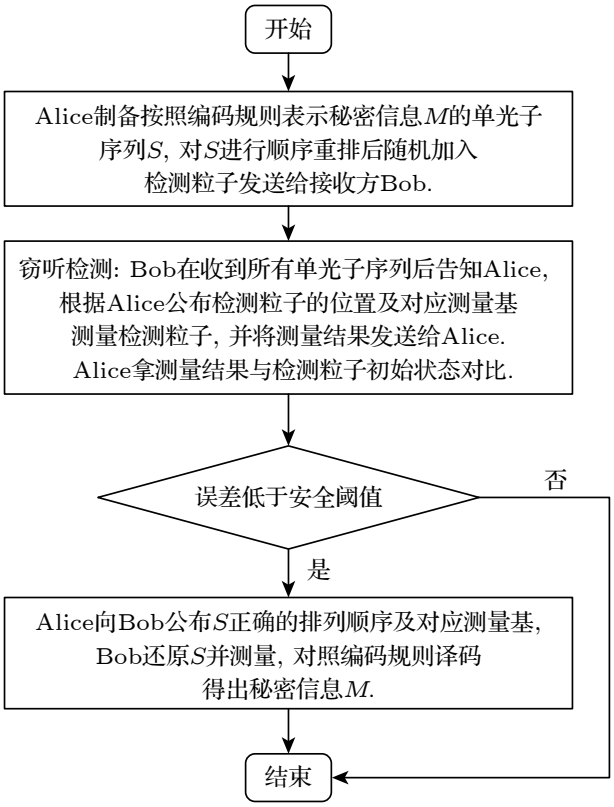

图 1 方案流程图 1

Fig. 1. Scheme flow chart 1.

2.2 分两次发送单光子的 QSDC 方案

步骤 1 Alice 制备两个单光子序列 S_1 ($|0_1\rangle$, $|1_1\rangle$, $|+_1\rangle$, $|-_1\rangle$) 和 S_2 ($|0_2\rangle$, $|1_2\rangle$, $|+_2\rangle$, $|-_2\rangle$), S_1 表示第一次发送给 Bob 的单光子, S_2 表示第二次发送给 Bob 的单光子. 根据编码规则用 S_1 与 S_2 结合的单光子序列 S 表示秘密信息 M, 记下 S 的排列顺序. 具体编码规则如下见表 2.

表 2 编码规则二

Table 2. Coding Rule 2.

信息序列	量子态	信息序列	量子态
000	$\|0_1\rangle$	001	$\|0_2\rangle$
111	$\|1_1\rangle$	110	$\|1_2\rangle$
011	$\|+_1\rangle$	010	$\|+_2\rangle$
100	$\|-_1\rangle$	101	$\|-_2\rangle$

步骤 2 Alice 将 S_1 顺序重排并加入检测粒子发送给 Bob, 之后窃听检测同 2.1 方案中步骤 2. 再将 S_2 重复上述操作.

步骤 3 Alice 向 Bob 公布序列 S 的排列顺序和正确的测量基, Bob 根据第一次收到的为 S_1, 第二次收到的为 S_2. 还原序列 S 并选择正确的测量

基进行测量, 根据编码规则对测量结果解码得到秘密信息 M.

2.3 分四次发送单光子的 QSDC 方案

Alice 制备四个单光子序列 $S_1\left(|0_1\rangle, |1_1\rangle, |+_1\rangle, |-_1\rangle\right)$, $S_2\left(|0_2\rangle, |1_2\rangle, |+_2\rangle, |-_2\rangle\right)$, $S_3\left(|0_3\rangle, |1_3\rangle, |+_3\rangle, |-_3\rangle\right)$, $S_4\left(|0_4\rangle, |1_4\rangle, |+_4\rangle, |-_4\rangle\right)$. 编码码规则如表 3 所列.

表 3 编码规则三

Table 3. Coding Rule 3.

信息序列	量子态	信息序列	量子态
0000	$\|0_1\rangle$	1000	$\|0_3\rangle$
1111	$\|1_1\rangle$	0111	$\|1_3\rangle$
0001	$\|+_1\rangle$	0011	$\|+_3\rangle$
1110	$\|-_1\rangle$	1100	$\|-_3\rangle$
0010	$\|0_2\rangle$	0101	$\|0_4\rangle$
1101	$\|1_2\rangle$	1010	$\|1_4\rangle$
0100	$\|+_2\rangle$	1001	$\|+_4\rangle$
1011	$\|-_2\rangle$	0110	$\|-_4\rangle$

方案具体步骤同 2.2 中的方案, 在步骤 2 中分四次发送即可.

2.4 分多次发送的单光子 QSDC 方案

综上所述, 单次发送单光子序列, 有 4 种量子态可以表示 4 种经典信息 (00, 01, 10, 11), 即可以表示 $\log_2(4\times1)=2$ 比特经典信息的所有情况, 2^2 种可能. 当分 n 次发送单光子序列, 可分为 $4n$ 种量子态表示出 $4n$ 种经典信息, 即可以表示 $\log_2(4n)$ 比特经典信息的所有可能, 也就是说分 n 次发送单光子序列时每量子比特可以表示 $\log_2(4n)$ 比特经典信息. 增大每量子比特表示的经典比特数, 可以提高量子比特的利用率. 由

$$\log_2(4n)=2+\log_2 n \tag{1}$$

得, 方案的发送次数 n 必须是 2 的整数次幂.

将方案扩展为分 n(n 是 2 的整数次幂) 次发送单光子的 QSDC 方案.

步骤 1 Alice 制备n个单光子序列$S_1(|0_1\rangle,|1_1\rangle, |+_1\rangle, |-_1\rangle), \cdots, S_n\left(|0_n\rangle, |1_n\rangle, |+_n\rangle, |-_n\rangle\right)$, 编码规则如表 4 所列.

方案具体步骤同 2.2 节中的方案, 在步骤 2 中分 n(n 是 2 的整数次幂) 次发送即可.

例如, 分 8(2 的 3 次幂) 次发送单光子来进行 QSDC 通信, 则可将表示秘密信息 M 的单光子序列分为 8 类, 每一类中含有 4 种量子态 ($|0\rangle, |1\rangle, |+\rangle$ $|-\rangle$), 即整个通信中存在$4\times8=32$种量子态, 每个量子态可以表示 $\log_2(4\times8)=5$ 比特的经典信息 (5 比特经典信息有 $2^5=32$ 种可能).

表 4 编码规则四

Table 4. Coding Rule 4.

信息序列	量子态	...	信息序列	量子态
$\overbrace{0\cdots0}^{\log_2(4n)}$	$\|0_1\rangle$	...	$\overbrace{0\cdots10}^{\log_2(4n)}$	$\|0_n\rangle$
$\overbrace{1\cdots1}^{\log_2(4n)}$	$\|1_1\rangle$	...	$\overbrace{1\cdots01}^{\log_2(4n)}$	$\|1_n\rangle$
$\overbrace{0\cdots1}^{\log_2(4n)}$	$\|+_1\rangle$	...	$\overbrace{0\cdots11}^{\log_2(4n)}$	$\|+_n\rangle$
$\overbrace{1\cdots0}^{\log_2(4n)}$	$\|-_1\rangle$	...	$\overbrace{1\cdots00}^{\log_2(4n)}$	$\|-_n\rangle$

3 安全性分析

安全性分析是指在通信过程中不存在第三方窃听导致信息泄漏, 或者即使有第三方的窃听, 也一定会被通信双方发现, 且不会泄漏任何有用信息.

3.1 测量与截获重发攻击

方案分 n (n 是 2 的整数次幂) 次传输单光子, 在每次传输中都进行了顺序重排并加入检测粒子. 第三方在不清楚检测粒子的位置及正确量子态的情况下, 即使截获到部分量子态也只能进行随机测量, 根据非正交量子态不可区分定理, 在随机选择测量基测量的情况下一定会引起量子态的塌缩, 在后续对检测粒子进行的窃听检测中一定会被发现. 而且每次传输的量子序列都进行了顺序重排且只含有部分信息, 即使第三方侥幸测量正确, 也得不到任何有用信息. 同样, 在第三方不知道发送量子态的情况下发起截获重发攻击, 也一定会被后续的窃听检测发现.

因为每次发送都会进行窃听检测, 方案中 n (n 是 2 的整数次幂) 取值越大, 进行窃听检测的次数就越多, 更能确保整个通信的安全性. 即第三方多次侥幸测量正确逃过检测的可能性微乎其微, 且多次窃听检测可以反复确保信道的安全性, 第三方即使侥幸逃过一次检测, 在 n (n 是 2 的整数次幂) 基数较大的情况下编码规则也会比较复杂, 第三方对掌握的序列属于第几次发送的信息、正确的粒子

排列顺序、编码规则都无从得知, 得不到任何有效信息.

3.2 拒绝服务攻击和木马攻击

第三方在截获信道中的信息后, 不试图获取信息而是通过随机操作来破坏传输的信息. 该攻击会引起量子态的改变, 在后续的窃听检测中会被发现. 当传输次数较多, 在辨别出是拒绝服务攻击时可以只针对此次信息发送来再次制备量子态重新编码发送即可. 木马攻击存在双向信道之间, 方案提到的基于单光子的通信方案都是单向发送, 因此不存在木马攻击.

3.3 辅助粒子攻击

第三方在截获通信双方传输的量子态后, 利用提前制备的辅助粒子, 对截获的量子态进行纠缠, 对两粒子执行一个幺正变换. 根据海森伯测不准原理和量子不可克隆原理得出第三方不可能在不引起任何错误的情况下得到有用信息. 且方案中存在多次窃听检测, 一旦发现存在辅助粒子攻击就会放弃通信.

第三方利用辅助粒子$|e\rangle$对单光子识别, 假设没有改变单光子状态.

$$\hat{E}\otimes|0e\rangle = a|0e_{00}\rangle + b|1e_{01}\rangle, \tag{2}$$

$$\hat{E}\otimes|1e\rangle = b'|0e_{10}\rangle + a'|1e_{11}\rangle, \tag{3}$$

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

$$\begin{aligned}&\hat{E}\otimes|-e\rangle\\ =&\frac{1}{\sqrt{2}}\left(a|0e_{00}\rangle + b|1e_{01}\rangle - b'|0_{10}\rangle - a'|1e_{11}\rangle\right)\\ =&\frac{1}{2}\big[|+\rangle\left(a|e_{00}\rangle + b|e_{01}\rangle - b'|e_{10}\rangle - a'|e_{11}\rangle\right)\\ &+|-\rangle\left(a|e_{00}\rangle - b|e_{01}\rangle - b'|e_{10}\rangle + a'|e_{11}\rangle\right)\big],\end{aligned} \tag{5}$$

其中$\{e_{00}, e_{01}, e_{10}, e_{11}\}$为算符$\hat{E}$决定的 4 个纯态, 满足归一化条件:

$$\sum_{\alpha,\beta\in\{0,1\}}\langle e_{\alpha,\beta}|e_{\alpha,\beta}\rangle = 1. \tag{6}$$

第三方的幺正操作$\hat{E}$矩阵表示为

$$\hat{E} = \begin{pmatrix} a & b' \\ b & a' \end{pmatrix}, \tag{7}$$

由$\hat{E}\hat{E}^* = I$, 得

$$\begin{aligned}&|a|^2 + |b|^2 = 1,\\ &|a'|^2 + |b'|^2 = 1,\\ &ab^* = (a')^* b',\end{aligned} \tag{8}$$

得出

$$|a|^2 = |a'|^2,\ |b|^2 = |b'|^2. \tag{9}$$

幺正操作引起的错误率, 即第三方窃听引起错误的概率

$$p_{\text{error}} = |b|^2 = 1 - |a|^2 = |b'|^2 = 1 - |a'|^2. \tag{10}$$

因此, 第三方在辅助粒子攻击下, 为了识别俘获粒子的状态一定会引起粒子状态变化, 在后续的窃听检测中被发现.

4 效率分析

4.1 通信传输效率

从信息论定义通信传输效率:

$$\xi = \frac{b_{\text{s}}}{q_{\text{t}} + b_{\text{t}}}, \tag{11}$$

其中, b_{s}为通信中传输的有用秘密信息比特数, q_{t}为通信中传输的量子比特数, b_{t}为通信中的经典比特数. 因为加入的检测粒子相较于传输信息的粒子较少且数量不明, 通常 QSDC 方案的效率分析不考虑用于窃听检测的单光子消耗和互相公布的信息, 且该方案信息传输过程不涉及经典比特, 则上述各方案的传输效率为

$$\begin{aligned}\xi_1 &= \frac{b_{\text{s}}}{q_{\text{t}} + b_{\text{t}}} = \frac{2n}{n} = 2\text{倍},\\ \xi_2 &= \frac{b_{\text{s}}}{q_{\text{t}} + b_{\text{t}}} = \frac{3n}{n} = 3\text{倍},\\ \xi_4 &= \frac{b_{\text{s}}}{q_{\text{t}} + b_{\text{t}}} = \frac{4n}{n} = 4\text{倍},\\ \xi_n &= \frac{b_{\text{s}}}{q_{\text{t}} + b_{\text{t}}} = \log_2(4n)\text{倍}.\end{aligned} \tag{12}$$

即分 n(n 是 2 的整数次幂) 次发送单光子的 QSDC 方案传输效率为$\log_2(4n)$倍, 传输效率会随着发送次数增多而提高.

4.2 量子比特利用率

量子比特利用率定义为

$$\eta = \frac{q_{\mathrm{u}}}{q_{\mathrm{t}}}, \tag{13}$$

其中, q_{u}为携带信息的量子比特, q_{t}为传输的量子比特数. 由于检测粒子数量相对于表示秘密信息的单光子数量较少, 可适当忽略不计, 得

$$\eta = q_{\mathrm{u}}/q_{\mathrm{t}} \approx 1. \tag{14}$$

4.3 编码容量及参数对比

从以上方案的编码规则可得在基于 n (n 是 2 的整数次幂) 次发送单光子的 QSDC 方案中, 编码效率为每量子比特可以表示 $\log_2(4n)$ 比特经典信息.

在单光子与纠缠态粒子结合的 QSDC 方案中. 如单光子与 Bell 态的结合, 每种 Bell 态是由两粒子纠缠的一种量子态, 需要 Bell 基联合测量得出, 因此在方案中测出一个 Bell 态需要传输两个量子态, 使得通信传输效率往往会低于量子态的编码容量. 由此可见纠缠态会降低通信的传输效率, 该方案只利用单光子传输信息, 使得每个量子态的传输效率与编码容量一致, 不会造成传输效率下降的现象.

本文所提方案与现有 QSDC 方案的通信效率对比结果如表 5 所列.

表 5 参数对比

Table 5. Parameter comparison.

QSDC通信协议	传输效率	量子比特率	编码容量
邓富国Two-Step [11]	1	1	1 qubit: 2 bit
权东晓基于单光子单向[12]	0.5	1	1 qubit: 1 bit
曹正文基于单光子与Bell态结合[13]	2	1	1 qubit: 3 bit
基于单光子与GHZ态结合[16]	2	1	1 qubit: 4 bit
基于单光子与n粒子GHZ态结合[17]	2	1	1 qubit: $(1+n)$bit
王剑基于纠缠交换[18]	1	1	1 qubit: 2 bit
单次发送单光子	2	1	1 qubit: 2 bit
分两次发送单光子	3	1	1 qubit: 3 bit
分4次发送单光子	4	1	1 qubit: 4 bit
分n(n是2的整数次幂)次发送单光子	$\log_2(4n)$	1	1 qubit: $\log_2(4n)$bit

5 总 结

从表 5 可以直观地看出, 本文提出的 QSDC 方案相较于其他方案在传输效率和编码容量[19]上有着明显的高效性. 而且该方案相较于其他方案, 只用到单光子[20]没有使用到纠缠态粒子, 不涉及量子纠缠原理, 因此该方案实现的难度更小.

参考文献

[1] Xin L 2019 *M. S. Thesis* (Lanzhou: Lanzhou University) (in Chinese) [欣龙 2019 硕士学位论文 (兰州: 兰州大学)]

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

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

[4] Wang Z Y 2019 *M. S. Thesis* (Shenyang: Shenyang Gongye University) (in Chinese) [王争艳 2019 硕士学位论文(沈阳: 沈阳工业大学)]

[5] Sheng Y B, Zhou L, Long G L 2022 *Science Bulletin.* **67** 367

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

[7] Yu S, Bo M Q,Tang Q, Mo Z W 2021 *Chin. J. Quantum Electron* **38** 57 (in Chinese) [余松, 柏明强, 唐茜, 莫智文 2021 量子电子学报 **38** 57]

[8] Liu Z H, Chen H W 2013 *Chin. Phys. Lett.* **30** 079901

[9] Liu Z H, Chen H W, Liu W J 2016 *Chin. Phys. Lett.* **33** 070305

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

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

[12] 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]

[13] Cao Z W, Zhao G, Zhang S H, Feng X Y, Peng J Y 2016 *Acta Phys. Sin.* **65** 230301 (in Chinese) [曹正文, 赵光, 张爽浩, 冯晓毅, 彭进业 2016 物理学报 **65** 230301]

[14] Liu Z H, Chen H W 2017 *Acta Phys. Sin.* **66** 130304 (in Chinese) [刘志昊, 陈汉武 2017 物理学报 **66** 130304]

[15] Zhao N, Jiang Y H, Zhou X T, Guo C F, Liu B 2021 *Network Security Technology* **08** 30 (in Chinese) [赵宁, 江英华, 周贤韬, 郭晨飞, 刘彪 2021 网络安全技术与应用 **08** 30]

[16] Zhou X T, Jiang Y H, Guo C F, Zhao N, Liu B 2021 *Chin. J. Quantum Electron.* https://kns.cnki.net/kcms/detail/34.1163.TN.20210927.2021.002.html (in Chinese) [周贤韬, 江英华, 郭晨飞, 赵宁, 刘彪 2021 量子电子学报 https://kns.cnki.net/kcms/detail/34.1163.TN.20210927.2021.002.html]

[17] Zhou X T, Jiang Y H 2022 *Laser Technology* **46** 79 (in Chinese) [周贤韬, 江英华 2022 激光技术 **46** 79]

[18] Wang J, Zhang S, Zhang S L, Zhang Q 2009 *J. Nat. Univ. Defense* **31** 51 (in Chinese) [王剑, 张盛, 张守林, 张权 2009 国防科技大学学报 **31** 51]

[19] Li X Y, Chang Y, Zhang S B, Dai J Q, Zheng T 2020 *Computer Applications and Software* **37** 292 (in Chinese) [李雪杨, 昌燕, 张仕斌, 代金鞘, 郑涛 2020 计算机应用与软件 **37** 292]

[20] Wei Y Y, Gao Z K, Wang S Y, Zhu Y J, Li T 2022 *Acta. Phy. Sin.* **71** 050302 (in Chinese) [危语嫣, 高子凯, 王思颖, 朱雅静, 李涛 2022 物理学报 **71** 050302]

Efficient quantum secure direct communication scheme based on single photons

Zhao Ning † Jiang Ying-Hua Zhou Xian-Tao

(*School of Information Engineering, Xizang Minzu University, Xianyang* 712000, *China*)

(Received 28 January 2022; revised manuscript received 28 March 2022)

Abstract

In this work, we first introduce the specific steps of a quantum-secure direct communication scheme that sends a single photon at a time. Based on the basic steps of the scheme, it is gradually extended to a quantum secure direct communication scheme that transmits single-photon sequences twice and four times, with emphasis on the coding rules corresponding to each scheme. The purpose is that through the above scheme, it can be intuitively seen in the subsequent efficiency analysis that with the increase of the number of transmissions, the classification of single photons can be increased, and the encoding capacity of each single photon and the transmission efficiency of quantum states in the entire communication can be greatly improved. Finally, a universal scheme and coding rules for quantum secure direct communication by sending single photons in an integer power of 2 are proposed, and after security analysis the scheme proves to be safe and feasible. Through the efficiency analysis, the communication efficiency of this scheme is higher than that of the existing scheme, and the implementation of this scheme only uses a single photon, does not involve with quantum entanglement, and this scheme has more application values.

Keywords: single photon, multiple sending, encoding rules, efficiency analysis

PACS: 03.67.Hk, 03.67.Dd **DOI:** 10.7498/aps.71.20220202

† Corresponding author. E-mail: 1720277914@qq.com