带身份认证的量子安全直接通信方案*

周贤韬 江英华†

(西藏民族大学信息工程学院, 咸阳 712000)

(2022 年 8 月 24 日收到; 2022 年 10 月 3 日收到修改稿)

针对传统量子安全直接通信方案中需提前假设通信双方合法性的问题, 提出一种带身份认证的基于 GHZ 态 (一种涉及至少三个子系统或粒子纠缠的量子态) 的量子安全直接通信方案. 该方案将 GHZ 态粒子分成三部分, 并分三次发送, 每一次都加入窃听检测粒子检测信道是否安全, 并在第二次发送的时候加入身份认证, 用以验证接收方的身份, 在第三次发送完粒子之后, 接收方将所有检测粒子抽取出来, 之后对 GHZ 态粒子做联合测量, 并通过原先给定的编码规则恢复原始信息. 本方案设计简单、高效, 无需复杂的幺正变换即可实现通信. 安全性分析证明, 该方案能抵御常见的内部攻击和外部攻击, 并且有较高的传输效率、量子比特利用率和编码容量, 最大的优势在于发送方发送信息的时候不需要假设接收方的合法性, 有较高的实际应用价值.

关键词: 量子安全直接通信, GHZ 态, 身份认证, 传输效率

PACS: 03.67.Hk, 03.67.Dd **DOI**: 10.7498/aps.72.20221684

1 引 言

1969 年, 哥伦比亚大学的 Wiesner[1] 在《Conjugate Conding》上提出了两个全新的观点, 分别是复用信道和量子钞票, 首次开启了量子信息的大门. 1984 年, Bennett 和 Brassard[2] 提出首个正式的量子通信协议, 这便是著名的 BB84 协议. 而量子安全直接通信 (QSDC) 的概念直到 2002 年才由 Long 和 Liu[3] 正式提出. Almut 等[4] 第一次使用单光子实现了量子安全的直接通信, 但这两个协议并不满足直接通信的条件, 它们需要经典信息的辅助. 同年 Boström 和 Felbinger[5] 利用密集编码的技术提出了第一个 QSDC 协议, 即 Ping Pong 协议, 但该协议存在安全性的问题[6,7]. 2003 年, 邓富国等[8] 基于块传输和密集编码的理论, 提出 Bell 态两步 QSDC 方案, 此后研究者们在此基础上又提出了一系列新的协议[8–29]. 例如, 2005 年 Gao[9] 首次提出受控量子安全直接通信协议——CQSDC, 后续 Dong 等[10] 提出类 GHZ 态 (一种涉及至少三个子系统或者粒子纠缠的量子态) 的 QSDC 协议. 2006 年, 王剑等[11] 提出一种基于单光子序列顺序重排的 QSDC 协议, 但传输效率并未提高, 仍是 1. 2007 年, Yan 等[12] 利用受控非门 (controlled-not gate)、本地测量以及量子隐形传输提出一种 QSDC 协议. 2008 年, Lin 等[13] 提出了利用 χ 型纠缠态的 QSDC 方案. 同年, Dong 等[14] 基于 W 态提出了相应的 QSDC 协议, 之后 Hassanpour 和 Houshmand[15] 研究了此方案在噪声环境中的情况. 2016 年曹正文等[16] 首次将两类例子结合起来进行安全直接通信, 将 Bell 态粒子和单光子结合从而提升了通信效率. 2022 年, 赵宁等[25] 提出一种基于单光子的高效 QSDC 方案, 利用多次发送单光子实现直接通信, 一是不涉及纠缠态, 二是没有复杂的幺正运算. 同年, 龚黎华等[26] 提出基于高维单粒子态的双向半 QSDC 协议.

早期的量子通信因为要考虑通信的安全而无法直接传输信息, 因而学者们提出的一系列协议都

* 陕西省教育厅科研专项科学研究计划 (批准号: 19JK0889) 资助的课题.

† 通信作者. E-mail: 250364629@qq.com

是在为传输信息做准备, 如量子密钥分发是为了保证信道的安全或通信双方的合法性, 在完成这一点后才能通信. 但自从 QSDC 的概念在 2002 年提出以来, 人们逐渐将研究重心转向通信本身, 思考如何利用量子态直接进行通信, 并提出了基于 Bell 态粒子、GHZ 态粒子以及单光子的 QSDC 方案等. 可是这些方案都必须有一个前提: 那就是通信双方都合法, 只有确保这个前提才能进行通信, 否则通信将不成立, 但实际情况难以确保通信双方合法, 一旦通信双方被冒充通信将不安全, 要解决这一问题就要引入身份认证功能. 身份认证的目的是在通信开始前在通信双方之间共享一串身份密钥用以确认通信双方的合法身份, 理论研究证明, 在 QSDC 中引入身份认证功能能确保通信双方的合法性. 身份认证分为单向身份认证和双向身份认证, 单向身份认证可以检验通信一方的合法性, 而双向身份认证可以检验通信双方的合法性, QSDC 由于是单向传输, 因此适合单向身份认证, 来检验接收方的合法性. 自从人们将量子身份认证 (quantum identity authentication, QIA) 应用于量子安全直接通信 (QSDC) 并取得成功之后, 不断有人提出带身份认证的 QSDC 协议. 因此在介绍 GHZ 态 QSDC 方案的基础上, 加入身份认证的功能. 分析证明, 加入身份认证功能之后原始方案的效率不变, 但可以省去复杂的幺正运算, 在不需要第三方 (third party, TP) 制备量子态的同时能够保证方案的安全性, 并且不需要事先约定接收方的合法性, 可以解决冒充接收方的问题.

2 理论研究

2.1 测量基

在量子通信过程中进行窃听检测和身份认证均要用到两种测量基, 分别是 Z 基 ($|0\rangle$, $|1\rangle$) 以及 X 基 ($|+\rangle$, $|-\rangle$). 其中 ($|0\rangle$, $|1\rangle$) 是一组标准正交基, ($|+\rangle$, $|-\rangle$) 是一组标准正交基, 而 X 基和 Z 基是非正交基, 并且 X 基与 Z 基通过 H 门可进行如下转换:

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

H 门表示为

$$H=\frac{1}{\sqrt{2}}[(|0\rangle+|1\rangle)\langle 0|+(|0\rangle-|1\rangle)\langle 1|], \tag{2}$$

$$H=\frac{1}{\sqrt{2}}(U_x+U_z)=\frac{1}{\sqrt{2}}\left[\begin{pmatrix}0&1\\1&0\end{pmatrix}+\begin{pmatrix}1&0\\0&-1\end{pmatrix}\right]$$
$$=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}. \tag{3}$$

操作过程及结果为

$$H|0\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$$
$$=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),$$
$$H|1\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}$$
$$=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle). \tag{4}$$

由 (4) 式可知, 如果量子态状态是$|0\rangle$(或$|1\rangle$), 则用 Z 基就一定能测出其状态是$|0\rangle$(或$|1\rangle$); 如果采用 X 基测量, 那么结果会有 50% 的概率塌缩为$|+\rangle$, 50% 的概率塌缩为$|-\rangle$. 同理, 如果量子态状态是$|+\rangle$(或$|-\rangle$), 采用 X 基就一定能测出它的状态是$|+\rangle$(或$|-\rangle$); 如果采用 Z 基测量, 则结果会有 50% 的概率塌缩为$|0\rangle$, 50% 的概率塌缩为$|1\rangle$.

2.2 单光子和 GHZ 态

4 种单光子分别为$|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, 表示单光子的四种偏振态, 即水平偏振、垂直偏振、45°偏振和 135°偏振. 8 种 GHZ 态粒子在 Z 基下分别表示为

$$\varphi_0=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)123,$$
$$\varphi_1=\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle)123,$$
$$\varphi_2=\frac{1}{\sqrt{2}}(|001\rangle+|110\rangle)123,$$
$$\varphi_3=\frac{1}{\sqrt{2}}(|001\rangle-|110\rangle)123,$$
$$\varphi_4=\frac{1}{\sqrt{2}}(|010\rangle+|101\rangle)123,$$
$$\varphi_5=\frac{1}{\sqrt{2}}(|010\rangle-|101\rangle)123,$$
$$\varphi_6=\frac{1}{\sqrt{2}}(|011\rangle+|100\rangle)123,$$
$$\varphi_7=\frac{1}{\sqrt{2}}(|011\rangle-|100\rangle)123. \tag{5}$$

将上述 8 种 GHZ 态粒子进行编码, 见表 1.

表 1 GHZ 态粒子对应的编码

Table 1. Corresponding codes of GHZ state particles.

GHZ态	对应的编码
$\varphi_0=\frac{1}{\sqrt{2}}\|000\rangle+\|111\rangle_{123}$	000
$\varphi_1=\frac{1}{\sqrt{2}}\|001\rangle+\|110\rangle_{123}$	001
$\varphi_2=\frac{1}{\sqrt{2}}\|010\rangle+\|101\rangle_{123}$	010
$\varphi_3=\frac{1}{\sqrt{2}}\|100\rangle+\|011\rangle_{123}$	011
$\varphi_4=\frac{1}{\sqrt{2}}\|100\rangle+\|011\rangle_{123}$	100
$\varphi_5=\frac{1}{\sqrt{2}}\|010\rangle+\|101\rangle_{123}$	101
$\varphi_6=\frac{1}{\sqrt{2}}\|001\rangle+\|110\rangle_{123}$	110
$\varphi_7=\frac{1}{\sqrt{2}}\|000\rangle+\|111\rangle_{123}$	111

2.3 量子身份认证

传统的 QIA 协议被当作一类独立的量子通信协议来单独研究, 其功能简而言之就是证明通信双方是原始、合法的, 没有被冒充. 基于 QIA 的思想, 将其加入到 QSDC 中作为一种辅助手段, 事先在通信双方之间共享一串身份密钥, 然后将 GHZ 态粒子分成 3 个部分 S_1, S_2 和 S_3, 分别发送给 Bob, 在 Alice 发送 S_2 给 Bob 的这一步加入身份认证, 之后经过一系列的检测, 可以判断接收方是否被冒充. 加入身份认证在于增加信道的安全性, 同时能保证原先的通信效率, 简化复杂的幺正运算, 且不需要第三方 TP 制备量子态, 最大的优势在于不需要假设接收方的合法性, 只需确保发送方的合法性. 相比传统的 QSDC 要假设通信双方的合法性, 本方案无疑具有明显的优势.

3 方案描述

假设 Alice 是合法的发送方, Bob 是否为合法的接收方尚不清楚, Alice 在之前已经将其身份密钥 IDA 共享给 Bob, 协议描述如下.

Ⅰ) 设 Alice 要发送的信息是 M, 身份密钥是 IDA, 首先将 M 每 3 位分成一段, 假设共分为 n 段, 根据表 1 的编码规则, 制备相应的 GHZ 态粒子.

Ⅱ) Alice 将每个 GHZ 态粒子的第一个粒子按顺序提取出来组成序列 S_1. 根据表 1 的编码规则随机制备用于窃听检测的诱惑粒子, 诱惑粒子的状态为$|0\rangle,|1\rangle,|+\rangle,|-\rangle$ 4 种单光子之一. 接着在 S_1 序列中的随机位置随机插入 4 种诱惑粒子形成新的序列$|0\rangle,|+\rangle$, 并记录插入诱惑粒子的位置, 然后 Alice 将$|0\rangle,|+\rangle$发送给 Bob.

Ⅲ) Bob 收到$|0\rangle,|+\rangle$序列后通知 Alice, Alice 通过不可篡改的经典信道公布诱惑粒子的位置和应使用的测量基, Bob 选取对应的测量基在相应位置进行测量. 测量完成后将结果发送给 Alice, Alice 将 Bob 的测量结果与正确结果相比较: 如果窃听检测的结果小于阈值, 则认为没有窃听, 可以继续通信; 否则结束通信.

Ⅳ) Alice 将每个 GHZ 态粒子的第二个粒子提取出来形成序列 S_2. Alice 根据序列 IDA 的值进行如下操作.

1) 若 $k_1=0$, 则在 S_2 中寻找第一个$|0\rangle$, 并记录位置 L_1; 若 $k_1=1$, 则在 S_2 中寻找第一个$|+\rangle$, 并记录位置 L_1.

2) 若 $k_2=0$, 则在 S_2 中位置 L_1 之后寻找第一个$|0\rangle$, 并记录位置 L_2; 若 $k_1=1$, 则在 S_2 中位置 L_1 之后寻找第一个$|+\rangle$, 并记录位置 L_2.

……

n) 若 $k_n=0$, 则在 S_2 中位置 L_{n-1} 之后寻找第一个$|0\rangle$, 并记录位置 L_n; 若 $k_n=1$, 则在 S_2 中位置 L_{n-1} 之后寻找第一个$|+\rangle$, 并记录位置 L_n.

这样遍历完 IDA 之后形成一个位置序列 $L=L_1L_2\cdots L_i\cdots L_n$, Alice 将位置序列 L 发送给 Bob, 但不告知 Bob 所采用的测量基以及测量结果.

Ⅴ) Alice 在 S_2 序列中的随机位置插入制备好的诱骗粒子, 并记录诱惑粒子的位置, 形成新的序列$|0\rangle,|+\rangle$, 最后将序列$|0\rangle,|+\rangle$发送给 Bob.

Ⅵ) Bob 收到$|0\rangle,|+\rangle$序列后, 按照第Ⅲ) 步的方法先进行窃听检测, 如果窃听检测通过后, 将诱骗粒子抽取出来恢复成 S_2 序列. 接下来进行身份认证环节, Bob 根据之前 Alice 公布的位置序列 L 进行如下测量:

1) 当$K_i=0$时, 选择 Z 基对序列 S_2 中第 L_i 个单光子进行测量;

2) 当$K_i=1$时, 选择 X 基对序列 S_2 中第 L_i 个单光子进行测量.

对测量得到的结果进行编码, $|0\rangle$编码为 0, $|+\rangle$编码为 1, 得到 n 位二进制字符串 K, Alice 将 K

与事先共享密钥 IDA 进行对比. 若 K = IDA, 则身份认证成功, Alice 确认 Bob 的身份, 通信继续. 若 $K \neq$ IDA 或测量结果中出现$|0\rangle$与$|+\rangle$以外的其他量子态, 则认证失败, 放弃通信.

Ⅶ) Alice 将 GHZ 态粒子的第三个粒子组合形成序列 S_3, 并将诱惑粒子插入 S_3 生成新的序列$|0\rangle, |+\rangle$, 发送给 Bob. 然后按照第Ⅲ) 步的方法进行窃听检测, 检测结果低于阈值可以继续下一步, 否则放弃通信.

Ⅷ) 在$|0\rangle, |+\rangle$中除去诱骗粒子和用于身份认证的粒子, 剩下的位置存放的就是秘密信息. 根据量子塌缩性原理, 之前对 S_2 测量之后, S_1 和 S_3 会塌缩成和 S_2 一样的序列, 将 S_1, S_2, S_3 的序列组合起来, 就得到完整的 GHZ 态粒子, 最后根据表 1 解码获得秘密信息.

4 讨论与分析

4.1 正确性

假设身份密钥为 IDA = 1001, 发送方在发送之前测量出 S_2 的值是$|1\rangle|+\rangle|1\rangle|+\rangle|-\rangle|0\rangle|0\rangle|1\rangle|+\rangle|1\rangle$, 当窃听检测通过之后, 省略不需要的粒子, 身份认证的过程见表 2.

表 2 身份认证过程

Table 2. Identity authentication process.

S_2	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$
IDA	1	0	0	1
位置L	2	6	7	9
Bob正确选择的测量基	X基	Z基	Z基	X基
Bob测量结果	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$
Bob(随机选择的测量基)及测量结果	50%$\|+\rangle$ 25%$\|0\rangle$ 25%$\|1\rangle$	50%$\|0\rangle$ 25%$\|+\rangle$ 25%$\|-\rangle$	50%$\|0\rangle$ 25%$\|+\rangle$ 25%$\|-\rangle$	50%$\|+\rangle$ 25%$\|0\rangle$ 25%$\|1\rangle$

由表 2 可知, 位置序列 L = 2679, 合法的 Bob 选择的测量基应该为 X 基, Z 基, Z 基和 X 基, 检测的结果为$|+\rangle|0\rangle|0\rangle|+\rangle$. 如果 Bob 是合法的通信接收方, 且知道身份信息 IDA 的值, 则 Bob 能正确地选择测量基, 得到正确的测量结果, 从而完成身份认证; 如果 Bob 的身份不合法, 那么它不知道身份信息 IDA 的值, 就需要去猜测. 由于我们假设的身份信息为 4 位, 则非法 Bob 猜中身份信息 IDA 的概率为 50%×50%×50%×50% = 6.25%, 也就是说第三方若想冒充接收方 Bob, 则它成功的概率为 6.25%. 推广可得, 若身份信息 IDA 为 n 位, 则第三方冒充成功的概率为 $(50\%)^n$. 当 n 足够大时, 这个概率就接近 0, 因此在实际操作时, 可以将 n 的位数设置得更多来保证接收方的合法性.

4.2 安全性

4.2.1 截获/测量重发攻击

截获/测量重发攻击是指在 Alice 将量子序列发送给 Bob 的过程中, 攻击者 Eve 截获 Alice 发送的序列. 如果用自己预先准备好的序列替代原序列发送给 Bob 的话, 就是接获重发攻击; 如果用 Z 基或 X 基对截获的序列进行测量, 然后将测量结果发送给 Bob 的话就是测量重发攻击. 而对于该协议, 一共发送了 S_1', S_2', S_3'三个序列, 每一个序列都加入了诱惑粒子, 对于每一串序列外部窃听者 Eve 都不知道诱惑粒子在什么位置, 也不知道该用什么测量基去测量. Eve 对每个量子态选择正确测量基进行测量的概率只有 50%, 因此 Eve 对截获单光子序列测量结果正确的概率为 $(50\%)^n$, n 为 Eve 截获单光子的个数. 一旦 Eve 选错测量位置和测量基, 再将测量后的结果发送给 Bob, 那么在窃听检测阶段, 就一定会被 Alice 发现. 而且即便 Eve 对 Alice 发送的序列进行测量, 它也得不到任何有用的消息, 因为我们的消息需要对 S_1, S_2, S_3 进行整合测量, 才能恢复初始消息, 若 Eve 对其中单独的序列进行测量而不做整合, 则它得到的只是一串毫无意义的数字.

4.2.2 木马攻击和拒绝服务攻击

木马攻击一般分为隐形光子木马攻击和延迟光子木马攻击. 这两种攻击只存在于双向通信当中, 而本方案只有 Alice 向 Bob 单向传输信息, 故不存在木马攻击. 拒绝服务攻击指窃听者 Eve 对捕获到的量子进行一些随机操作, 从而破坏发送方欲传输的信息, 而自己也不获取相关的信息的过程. 由于窃听者并不知道诱骗粒子的位置, 所以当攻击者 Eve 对诱惑粒子进行随机操作时, 那么就会被窃听检测出来, 因此拒绝服务攻击对本方案也是无效的.

4.2.3 辅助粒子攻击

辅助粒子攻击是 Eve 借助辅助粒子对截获的

量子态进行纠缠. 该攻击涉及 Eve 对一个更大的复合系统进行幺正操作, 幺正操作会引起一定的错误率. 对该攻击的安全性分析包括 Eve 攻击被检测到的概率, 即幺正操作引起的错误率和 Eve 可以访问到的最大信息量 $I_{\rm E}$. 通信中涉及单光子和 Bell 态粒子两种量子态, 对该安全性分析也分为对截获两种量子态的分析.

1) Eve 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,

$$\widehat{\boldsymbol{E}}\otimes|0e\rangle=a\,|0e_{00}\rangle+b\,|1e_{01}\rangle, \tag{6}$$

$$\widehat{\boldsymbol{E}}\otimes|1e\rangle=b'\,|0e_{10}\rangle+a'\,|1e_{11}\rangle, \tag{7}$$

$$\begin{aligned}\widehat{E}\otimes|+e\rangle=&\frac{1}{\sqrt{2}}\left(a|0e_{00}\rangle+b|1e_{01}\rangle+b'|0e_{10}\rangle\right.\\&\left.+a'|1e_{11}\rangle\right)\\=&\frac{1}{2}\left[|+\rangle\left(a|e_{00}\rangle+b|e_{01}\rangle+b'|e_{10}\rangle+a'|e_{11}\rangle\right)\right.\\&\left.+|-\rangle\left(a|e_{00}\rangle-b|e_{01}\rangle+b'|e_{10}\rangle-a'|e_{11}\rangle\right)\right],\end{aligned} \tag{8}$$

$$\begin{aligned}\widehat{E}\otimes|-e\rangle=&\frac{1}{\sqrt{2}}\left(a|0e_{00}\rangle+b|1e_{01}\rangle-b'|0e_{10}\rangle\right.\\&\left.-a'|1e_{11}\rangle\right)\\=&\frac{1}{2}\left[|+\rangle(a|e_{00}\rangle+b|e_{01}\rangle-b'|e_{10}\rangle-a'|e_{11}\rangle)\right.\\&\left.+|-\rangle(a|e_{00}\rangle-b|e_{01}\rangle-b'|e_{10}\rangle+a'|e_{11}\rangle)\right].\end{aligned} \tag{9}$$

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

$$\sum_{\alpha,\beta\in\{0,1\}}\langle e_{\alpha,\beta}|e_{\alpha,\beta}\rangle=1. \tag{10}$$

Eve 的幺正操作$\widehat{\boldsymbol{E}}$矩阵表示为

$$\widehat{\boldsymbol{E}}=\begin{pmatrix}a & b'\\ b & a'\end{pmatrix}. \tag{11}$$

由$\widehat{\boldsymbol{E}}\widehat{\boldsymbol{E}}^{*}=I$, 得

$$\begin{aligned}|a|^2+|b|^2=1,\\ |a'|^2+|b'|^2=1,\\ ab^{*}=(a')^{*}b',\end{aligned} \tag{12}$$

得出

$$|a|^2=|a'|^2,\ \ |b|^2=|b'|^2. \tag{13}$$

幺正操作引起的错误率, 即 Eve 窃听被检测到的概率

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

2) Eve 对截获的 Bell 态粒子进行幺正操作$\widehat{\boldsymbol{E}}$, 攻击后量子态$|0\rangle$和$|1\rangle$变为

$$\widehat{\boldsymbol{E}}\otimes|0e\rangle=a\,|0e_{00}\rangle+b\,|1e_{01}\rangle, \tag{15}$$

$$\widehat{\boldsymbol{E}}\otimes|1e\rangle=b'\,|0e_{10}\rangle+a'\,|1e_{11}\rangle. \tag{16}$$

假设 Eve 攻击 Bell 态纠缠粒子$|\varphi^{+}\rangle$后系统的变化

$$\begin{aligned}|\varphi\rangle_{\rm Eve}=&E\otimes\frac{|0e\rangle\otimes|0\rangle+|1e\rangle\otimes|1\rangle}{\sqrt{2}}\\=&\frac{1}{\sqrt{2}}\left[(a\,|0e_{00}\rangle+b\,|1e_{01}\rangle)\otimes|0\rangle\right.\\&\left.+(b'\,|0e_{10}\rangle+a'\,|1e_{11}\rangle)\otimes|1\rangle\right]\\=&\frac{1}{\sqrt{2}}\left[(a\,|0e_{00}0\rangle+b\,|1e_{01}0\rangle)\right.\\&\left.+(b'\,|0e_{10}1\rangle+a'\,|1e_{11}1\rangle)\right].\end{aligned} \tag{17}$$

合法通信方对$|\phi^{+}\rangle$做测量时, 当且仅当$|a|=|a'|$, 没有窃听的概率

$$p_{\rm Eve}=\frac{|a|^2+|a'|^2}{2}=|a|^2. \tag{18}$$

窃听被检测到的概率

$$p_{\rm error}=1-p_{\rm Eve}=1-|a|^2=1-|a'|^2. \tag{19}$$

因此, 使用辅助粒子对截获的量子态进行攻击, 一定会对粒子状态的改变产生干扰, 在后续合法通信方的窃听检测中一定会被发现.

3) 对 Eve 获取最大信息量 $I_{\rm E}$ 的分析. 每一个光子的约化密度矩阵为

$$\boldsymbol{\rho}=\frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \tag{20}$$

可以看出 Eve 测量光子得$|0\rangle$或$|1\rangle$的概率都是 50%, 量子态$|0\rangle$被 Eve 攻击,

$$|\varphi\rangle_{\rm Eve}=\widehat{\boldsymbol{E}}\otimes|0e\rangle=a\,|0e_{00}\rangle+b\,|1e_{01}\rangle. \tag{21}$$

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

$$\begin{aligned}\rho'=&|\varphi\rangle_{\rm Eve}\langle\varphi|_{\rm Eve}\\=&|a|^2\,|0e_{00}\rangle\langle0e_{00}|+|b|^2\,|1e_{01}\rangle\langle1e_{01}|\\&+ab^{*}\,|0e_{00}\rangle\langle1e_{01}|+a^{*}b\,|1e_{01}\rangle\langle0e_{00}|.\end{aligned} \tag{22}$$

用矩阵表示为

$$\boldsymbol{\rho}'=\begin{pmatrix}|a|^2 & ab^{*}\\ a^{*}b & |b|^2\end{pmatrix}, \tag{23}$$

解密度算子$\boldsymbol{\rho}'$的特征值λ:

$$\det\begin{bmatrix} |a|^2-\lambda & ab^* \\ a^*b & |b|^2-\lambda \end{bmatrix}=0. \tag{24}$$

特征方程:

$$\left(|a|^2-\lambda\right)\times\left(|b|^2-\lambda\right)-ab^*\times a^*b=0. \tag{25}$$

$\boldsymbol{\rho}'$ 的两个特征值$\lambda_1=0$, $\lambda_2=1$, 则 Eve 的 Von-Neumann 熵为

$$I_{\rm E}=\chi(\boldsymbol{\rho}')=-\sum_{i=0}^{1}\lambda_i\log_2\lambda_i=0. \tag{26}$$

由 (26) 式可得, Eve 对截获粒子采用 U 操作来窃听, 获得信息仍为 0. 根据信息论可知 Eve 在量子系统中可获取最大信息量受于 Holevo 限:

$$\chi(\rho)=S(\rho)-\sum_{i=1}^{8}p_iS(\rho_i), \tag{27}$$

其中, $S(\rho)$为态ρ的 Von-Neumann 熵, $\rho=\sum_{i=1}^{8}p_i\rho_i$, ρ_i是以概率p_i制备的量子态, 如果发送方 Alice 以 1/8 概率发送 000, 001, 010, 100, 101, 110, 011, 111. 那么发送的信息熵为

$$\begin{aligned} H_{(p)}=&-\sum_{i=1}^{8}p_i\log_2p_i\\ =&-p_{000}\log_2p_{000}-p_{001}\log_2p_{001}\\ &-p_{010}\log_2p_{010}-p_{100}\log_2p_{100}\\ =&-p_{101}\log_2p_{101}-p_{110}\log_2p_{110}\\ &-p_{011}\log_2p_{011}-p_{111}\log_2p_{111}=3, \end{aligned} \tag{28}$$

则

$$I_{\rm E}=\chi(\rho')=S(\rho')-\sum_{i=1}^{8}p_iS(\rho_i')<H(p). \tag{29}$$

由此可知合法双方互信息为 3, 而 Eve 得到的信息 $I_{\rm E}$=0, 所以第三方 Eve 无法窃取到任何有用信息.

4.2.4 身份冒充攻击

由于通信前已假定发送方 Alice 是合法的, 因此 Alice 不存在被冒充的情况, 这里讨论接收方 Bob 被冒充的情况. 通信开始后, 当 Bob 被第三方冒充, 那么冒充者不知道身份信息 IDA 的值, 因而需要去猜测, 由上文分析可知, 如果身份密钥的位数为 n, 则冒充者猜对身份密钥的概率为 $(50\%)^n$, 当 $n\geqslant 7$, 也就是密钥位数≥7 位的时候, 冒充者猜对的概率不足 1%, 即被发现的概率大于 99%, 这时可以认为协议安全. 一旦冒充者猜错了 IDA 的值, 就会错误地选择测量基, 从而得出错误的测量结果 K, 因为 $K\neq$ IDA, 冒充者的身份就会被发现, 通信随即终止.

4.2.5 信息泄露问题

信息泄露指外部窃听者 Eve 不需要去截获发送方发送的粒子, 而仅仅只通过窃听发送方和接收方在经典信道中公布的信息就可以得到全部或部分的秘密信息, 这种攻击主要存在于双向量子通信中协议. 对于该方案, Alice 公布了 S_1', S_3'序列中插入的诱惑粒子的位置和应选用的测量基, 攻击者并不能根据诱惑粒子的位置和应选用的测量基获得和推测出任何有关秘密信息的消息. 接着 Bob 告知了 Alice 测量结果, 测量结果为与阈值相关的信息, 攻击者并不能依此获得和推测到任何有关秘密消息的信息. 对于序列 S_2', Alice 除了公布诱惑粒子的信息外, 还公布了表示身份信息的单光子态的位置和应选用的测量基. 同样, 因为只有诱惑粒子和表示身份信息的单光子的位置和应选用的测量基, 窃听者 Eve 仍然得不到任何有关秘密消息的信息. 所以该方案理论上不会有任何的信息泄露.

4.3 效率及编码容量

在信息论中量子密码方案的传输效率定义为

$$\xi=\frac{b_{\rm s}}{q_{\rm t}+b_{\rm t}}, \tag{30}$$

式中, $b_{\rm s}$, $q_{\rm t}$ 和 $b_{\rm t}$ 分别表示通信时交换的有用信息比特数、量子比特数和经典比特数. 在一般情况下, 身份认证和窃听检测用到的相关量子比特忽略不计. 因此该方案中, $q_{\rm t}$ 为 $3n$, $b_{\rm s}$ 为 $3n$, $b_{\rm t}$ 为 0, 则该方案传输效率为

$$\eta=\frac{3n}{3n+0}. \tag{31}$$

量子比特利用率定义为

$$\eta=q_{\rm u}/q_{\rm t}, \tag{32}$$

其中, $q_{\rm u}$ 表示用来传递消息的量子比特的个数, 本方案中所有量子比特均携带了信息. 因此在该方案中, $q_{\rm u}$ 为 n 个 GHZ 态的量子比特数 $3n$, $q_{\rm t}$ 为 n 个 GHZ 态的量子比特数 $3n$, 故

$$\eta=\frac{3n}{3n}=1. \tag{33}$$

表 3 相似协议效率对比

Table 3. Efficiency comparison of similar protocols.

协议	传输效率 ξ	量子比特利用率 η	编码容量
Ping-Pong 协议[6]	0.33	0.33	一个态: 1.0 bit
Two-Step QSDC协议[9]	1.00	1.00	一个态: 1.0 bit
One-Pad-Time QSDC协议[27]	1.00	1.00	一个态: 1.0 bit
基于纠缠交换的QSDC协议[11]	1.00	1.00	一个态: 1.0 bit
权东晓单光子的单向QSDC协议[29]	0.50	1.00	一个态: 1.0 bit
Bell态和单光子混合QSDC协议[16]	1.00	1.00	一个态: 1.5 bits
本文所提协议	1.00	1.00	一个态: 3.0 bits

对于刘丹[27]提出的基于 Bell 态的 QSDC, 其通信效率为$\xi = 2n/(2n) = 1$, 其量子比特利用率为$\eta = n/(2n) = 0.5$, 由此可看出基于 GHZ 态的 QSDC 相较于基于 Bell 态的 QSDC 通信效率不变, 但量子比特利用率提高了 1 倍. 编码容量方面, 由表 1 可知, 一个 GHZ 态上可以编码 3 bits 经典信息, 因此该方法的编码容量为一个态: 3 bits. 我们将一些经典的 QSDC 协议的量子传输效率、量子比特利用率和编码容量用 (30) 式—(32) 式计算出来与本文提出的方案进行分析对比, 所得结果见表 3.

5 结 论

经典的基于 GHZ 态粒子 QSDC 方案通常采用三粒子 GHZ 态粒子作为传输粒子, 但是其隐患在于通信过程简单, 安全性难以得到保证, 因此在传统的基于 GHZ 态粒子 QSDC 方案的基础上, 加入了单向身份认证. 在此方案中, 一次秘密信息的发送要分三步, 如此一来, 即便中间有窃听者窃听到了发送的量子态, 那它得到的也只是不完整的信息, 并不能知晓真实信息. 另外每一次发送量子态之前都做一次窃听检测, 也杜绝了外部窃听的干扰, 安全性大有保证. 而接收方也必须获得完整的三串序列才能对消息解码, 因此从理论上可以解决信息的泄露问题, 与传统的方案相比, 效率没有下降, 安全性得到了提高, 并且有效地解决了通信接收方合法性的问题.

参考文献

[1] Wiesner S 1983 *Acm. Sigact. News* **15** 78

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

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

[4] Almut B, Berthold-Georg E, Christian K, Harald W 2002 *J. Phys. A* **35** 46

[5] Boström K, Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

[6] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901

[7] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 266104

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

[9] Gao T, Yan F L, Wang Z X 2005 *Chin. Phys.* **14** 893

[10] Dong Li, Xiu X M, Gao Y J, Chi F 2008 *Commun. Theor. Phys.* **6** 1498

[11] Wang J, Zhang Q, Tang C J 2006 *Phys. Lett. A* **06** 035

[12] Yan F L, Hai R H 2007 *Commun. Theor. Phys.* **47** 629

[13] Lin S, Wen Q Y, Gao F, Zhu F Z 2008 *Phys. Rev. A* **78** 064304

[14] Dong L, Xiu X M, Gao Y J, Chi F 2009 *Commun. Theor. Phys.* **51** 08

[15] Hassanpour S, Houshmand M 2015 *Quantum Information Processing* **14** 15

[16] 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]

[17] 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]

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

[19] Zhao N, Jiang Y H, Zhou X T, Guo C F, Liu B 2021 *Network Security Technol.* **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]

[20] Jiang Y H, Zhang S B, Chang Y, Yang F, Yang M 2018 *J. Quan. Electr.* **35** 49 (in Chinese) [江英华, 张仕斌, 昌燕, 杨帆, 杨敏 2018 量子电子学报 **35** 49]

[21] Jiang Y H, Zhang S B, Yang F, Chang Y, Zhang H 2017 *Prog. Laser and Optoelectr.* **54** 454 (in Chinese) [江英华, 张仕斌, 杨帆, 昌燕, 张航 2017 激光与光电子学进展 **54** 454]

[22] Jiang Y H, Zhang S B, Chang Y, Yang F, Shao T T 2018 *Appl. Res. Compu.* **35** 889 (in Chinese) [江英华, 张仕斌, 昌燕, 杨帆, 邵婷婷 2018 计算机应用研究 **35** 889]

[23] Jiang Y H, Zhang S B, Dai J Q 2018 *Mod. Phys. Lett. B* **32** 1850125

[24] Jiang Y H 2018 *M. S. Thesis* (Chengdu: Chengdu University of Information Engineering) (in Chinese) [江英华 2018 硕士学位论文 (成都: 成都信息工程大学)]

[25] Zhao N, Jiang Y H, Zhou X T 2022 *Acta Phys. Sin.* **71** 150304 (in Chinese) [赵宁, 江英华, 周贤韬 2022 物理学报 **71** 150304]

[26] Gong L H, Chen Z Y, Xu L C, Zhou N R 2022 *Acta Phys. Sin.* **71** 130304 (in Chinese) [龚黎华, 陈振泳, 徐良超, 周南润 2022 物理学报 **71** 130304]

[27] Liu D, Pei C X, Quan D X, Nan Z 2022 *Chin. Phys. Lett.* **27** 050306

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

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

Quantum secure direct communication scheme with identity authentication*

Zhou Xian-Tao Jiang Ying-Hua †

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

(Received 24 August 2022; revised manuscript received 3 October 2022)

Abstract

Aiming at the problem that traditional quantum secure direct communication schemes need to assume the legitimacy of both parties in advance, a GHZ state (a quantum state involving at least three subsystems or particles entanglement) based quantum secure direct communication scheme with identity authentication is proposed. The scheme first encodes GHZ state particles into eight types, divides the particles into three parts, and sends them three times. Each time, eavesdropping is added to detect whether the particle detection channel is secure, and identity authentication is added when sending particles for the second time to verify the identity of the receiver. Specifically, according to the value of the ID key IDA, the specified particles (such as $|0\rangle$ particles or $|+\rangle$ particles) are found in the two particles. Then their positions are marked as L and they traverse down until all the identity keys are traversed, obtaining a position sequence L. After sending the two particles to Bob for eavesdropping detection, Bob measures the L position of the two particles on the corresponding basis according to the value of the identity key, the measurement results are coded, and compared with the identity key IDA to complete the identity authentication. After sending the particles for the third time. the receiver extracts all the detected particles, and then the GHZ state particles are jointly measured, and the original information is recovered through the previously given coding rules, so as to realize quantum safe direct communication. The design of this scheme is simple and efficient, and the communication can be realized without complex unitary transformation. The correctness analysis proves that the scheme is correct in theory. The security analyses of interception/measurement retransmission attack, Trojan horse attack, denial of service attack, auxiliary particle attack, identity impersonation attack, and other attacks prove that the scheme can resist common internal attacks and external attacks, and solve the problem of information leakage. The transmission efficiency of the scheme is 1, the quantum bit utilization is 1, and the coding capacity is a quantum state carrying 3 bits of information. Compared with some previous schemes, this scheme has obvious advantages in these three aspects. The biggest advantage is that the sender does not need to assume the legitimacy of the receiver when sending information, so it has high practical application value.

Keywords: quantum secure direct communication, GHZ state, identity authentication, transmission efficiency

PACS: 03.67.Hk, 03.67.Dd **DOI:** 10.7498/aps.72.20221684

* Project supported by the Special Scientific Research Plan of Shaanxi Provincial Department of Education, China (Grant No. 19JK0889).

† Corresponding author. E-mail: 250364629@qq.com

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

带身份认证的量子安全直接通信方案

周贤韬 江英华

Quantum secure direct communication scheme with identity authentication

Zhou Xian-Tao Jiang Ying-Hua

引用信息 Citation: Acta Physica Sinica, 72, 020302 (2023) DOI: 10.7498/aps.72.20221684
在线阅读 View online: https://doi.org/10.7498/aps.72.20221684
当期内容 View table of contents: http://wulixb.iphy.ac.cn
