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

# 带双向身份认证的基于单光子和Bell态混合的量子安全直接通信方案

周贤韬 江英华 郭晓军 彭展

# Quantum secure direct communication scheme based on the mixture of single photon and Bell state with two way authentication

Zhou Xian-Tao Jiang Ying-Hua Guo Xiao-Jun Peng Zhan

引用信息 Citation: Acta Physica Sinica, 72, 130302 (2023) DOI: 10.7498/aps.72.20221972
在线阅读 View online: https://doi.org/10.7498/aps.72.20221972
当期内容 View table of contents: http://wulixb.iphy.ac.cn

---

# 带双向身份认证的基于单光子和 Bell 态混合的量子安全直接通信方案*

周贤韬 江英华† 郭晓军 彭展

(西藏民族大学信息工程学院, 咸阳 712000)

(2022 年 10 月 15 日收到; 2023 年 4 月 10 日收到修改稿)

针对量子安全直接通信中身份认证的需要, 提出一种带双向身份认证的基于单光子和 Bell 态混合的量子安全直接通信方案. 通信开始前通信双方共享一串秘密信息, 先利用单光子来验证接收方的合法性, 再利用 Bell 态粒子验证发送方的合法性, 之后将 Bell 态粒子与单光子混合作为载体发送. 每一次发送量子态时都加入窃听检测粒子, 而一旦窃听者截获发送粒子, 由于得到的是不完整的粒子, 窃听者无法恢复原始信息, 并且窃听行为会立刻被发现, 从而终止通信. 本方案中单光子和 Bell 态充得到分利用, 且混合之后的通信能有效提高传输效率和编码容量以及量子比特利用率. 安全性分析证明, 本方案能抵御常见的外部攻击和内部攻击.

**关键词:** 量子安全直接通信, 混合态, 身份认证, 传输效率

**PACS:** 03.67.Hk, 03.67.Dd **DOI:** 10.7498/aps.72.20221972

## 1 引 言

最早的量子密钥分发协议 (BB84 协议) 在 1984 年由 Bennett 和 Brassard[1] 提出, BB84 协议的基本原理是通过单光子量子比特实现密钥的共享. 1991 年, Ekert[2] 在 BB84 协议的基础上, 提出了一个全新的量子密钥分发协议, E91 协议. 该协议和 BB84 协议在理论上都是无条件安全的, 区别是 E91 协议主要采用两粒子纠缠态 (简称 EPR 对) 和 Bell 不等式来实现密钥的分发, 相比于 BB84 更加高效. 基于这些基础协议的原理, 随后很多专家在该领域提出了可行的量子密钥分发方案 [3–6], 2010 年, 权东晓 [7] 提出了基于单光子单向传输的确定性 QKD 方案. 2015 年, Li 等 [8] 提出一种基于去相干状态的可容错量子安全直接通信协议. 到目前为止, 量子安全直接通信协议已经引起学术界的广泛关注.

最早, 2002 年由龙桂鲁等 [9] 提出量子安全直接通信 (QSDC) 方案, 其他 QSDC 方案可见文献 [9–12]. 2006 年, Wang 等 [13] 对单光子在 QSDC 中的应用进行了一定程度的优化, 基于单光子双向传输用到了单光子的顺序重排技术. 2007 年, Man 和 Xia[14] 分析了前期提出的一种基于 GHZ 态 (一种涉及至少 3 个子系统或粒子纠缠的量子态) 三方 QSDC 方案的安全性, 发现窃听者依据公开信息可得到部分机密, 给出了改进方案. 2011 年, Lan 等 [15] 研究了噪声条件下具有身份认证、基于密集编码的 QSDC 方案. 2012 年, Li 等 [16] 提出基于 EPR 纠缠粒子对的 QSDC 协议. 2014 年, An 等 [17] 研究了基于稳定子码在噪声信道中的 QSDC 方案, 该方案可对单量子的相位和比特错误进行检错纠错, 降低通信误码率. 2015 年, 龙桂鲁 [18] 研究了噪声环境中的 QSDC 方案. 2016 年, Hu 等 [19] 通过频率

* 陕西省教育厅科研专项科学研究计划 (批准号: 19JK0889) 和西藏自治区自然科学基金 (批准号: XZ2019ZRG-36(Z), XZ202101ZR0089G) 资助的课题.

† 通信作者. E-mail: 250364629@qq.com

 

编码的简化实验证明了 Deng 等[11]提出的 DL04 方案. 2017 年, Zhang 等[20]实验演示了高效方案和两步方案. 同年, Zhu 等[21]第 1 次实现了 500 m 内的量子直接通信演示. 以 Cao 等[22−27]为代表的一批学者提出将单光子与纠缠态粒子 (如 Bell 态粒子与 GHZ 态粒子) 结合的 QSDC 方案. 2022 年, Zhao 等[27]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, 不涉及纠缠态和复杂的幺正运算. 同年, 龚黎华等[28]提出基于高维单粒子态的双向半 QSDC 协议. Qi 等[29]报道了实用化样机, 最新的世界纪录是 100 km[30], 最新的 QSDC 见综述见文献 [31].

不论是量子密钥分发还是 QSDC, 都需要身份认证. 本文利用量子混合态在编码和传输上的优势, 结合量子身份认证在安全性方面的优点, 将二者结合提出一种带双向身份认证的单光子和 Bell 态混合的 QSDC 方案, 先利用单光子验证接收方的合法性, 再利用 Bell 态验证发送方的合法性, 最后将单光子和 Bell 态混合传输通信, 该方案不仅可以解决收发双方的合法性问题, 也提高了信息的编码容量和通信的传输效率, 且方案实现简单, 无复杂的幺正运算, 有较高的可实现性.

## 2 方案流程

图 1 为方案流程图. 假设 Alice 仅具备量子态制备能力, Bob 仅具备测量能力. 通信前, Alice 与 Bob 需要共享一串秘密的二进制字符串来进行身份认证[30], 即长度为 $n$ 的二进制秘钥 $K(K_1K_2\cdots K_n)$, $K_i=0$或1, $i\in[0,\ n]$.

**步骤 1** 通信中发送方为 Alice, 接收方 Bob. 发送方 Alice 的准备工作如下.

1) 制备一串单光子序列 $S_{\rm S}$, 该单光子序列存在 4 种偏振态: 水平偏振 $\rightarrow|0\rangle$垂直偏振 $\rightarrow|1\rangle$, 45°偏振 $\rightarrow|+\rangle$, 135°偏振 $\rightarrow|-\rangle$.

2) 制备一串 Bell 态粒子对即 EPR 纠缠粒子对, 其制备的 Bell 态存在 4 种状态 $|\psi^+\rangle$, $|\psi^-\rangle$, $|\varphi^+\rangle$, $|\varphi^-\rangle$:

$$\varphi^+=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{12},\ \ \varphi^-=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)_{12},$$
$$\psi^+=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)_{12},\ \ \psi^-=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)_{12}. \tag{1}$$

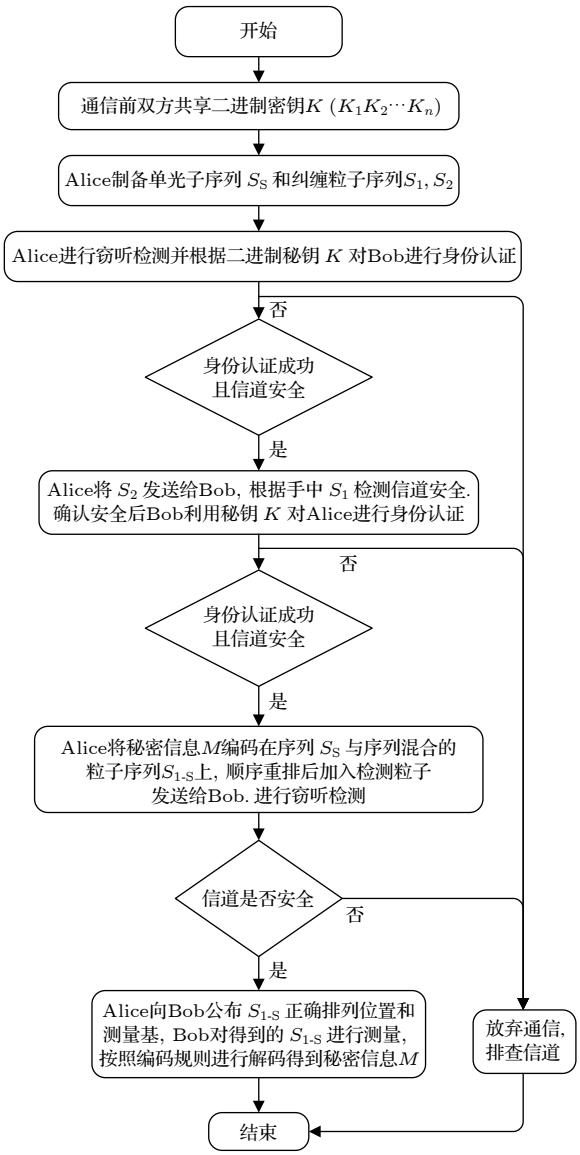


图 1 方案流程图

Fig. 1. Scheme flow chart.

将每对 EPR 纠缠粒子对的第一个纠缠粒子分离出来组成粒子序列 $S_1$, 剩下的组成粒子序列 $S_2$.

**步骤 2** Alice 确定接收方 Bob 的身份 (基于单光子的身份认证). Bob 根据共享秘钥 $K(K_1K_2\cdots K_n)$制备单光子序列, 规则如下: $K_i=0$时, 制备第 $i$ 个单光子为$|0\rangle$; $K_i=1$时, 制备第 $i$ 个单光子为$|+\rangle$. 遍历完 $K$ 制备出 $n$ 位的单光子序列 $S_n$.

Bob 在序列 $S_n$ 中加入检测粒子发送给 Alice, 检测粒子是 4 种单光子 0, 1, $|+\rangle$, $|-\rangle$, Alice 在收到粒子序列后通知 Bob, 随后 Bob 向 Alice 公布检测粒子的位置和需要用到的测量基, Alice 根据 Bob 公布的位置选出检测粒子, 使用 Bob 公布的测量基进行测量, 将测量结果与正确结果进行对

比. 若误差率低于设定的阈值说明不存在第三方窃听, 进行下一步的身份认证; 若误差率高于设定的阈值说明可能存在第三方窃听, 放弃通信.

Alice 去除检测粒子, 对剩下的序列 $S_n$ 进行测量, 根据事先共享秘钥 $K\,(K_1K_2\cdots K_n)$ 来选择测量基. 当 $K_i=0$ 时, 选择 $Z$ 基对序列 $S_n$ 中第 $i$ 个单光子进行测量; 当 $K_i=1$ 时, 选择 $X$ 基对序列 $S_n$ 中第 $i$ 个单光子进行测量.

测量得到的单光子序列, 量子态 $|0\rangle$ 用 0 表示, 量子态 $|+\rangle$ 用 1 表示. 得到 $n$ 位二进制字符串 $K_{\rm a}$, Alice 将 $K_{\rm a}$ 与事先共享秘钥 $K$ 进行对比, $K_{\rm a}=K$ 则身份认证成功, Alice 确认 Bob 的身份, 通信继续. 若 $K_{\rm a}\neq K$ 或测量结果中出现除 $|0\rangle$ 与 $|+\rangle$ 外的其他量子态, 则认证失败, 放弃通信.

**步骤 3** Bob 确定发送方 Alice 的身份 (基于 Bell 态的身份认证); 信道安全检测并发送部分 Bell 态用于后续的 Bell 基联合测量.

Alice 将 $S_2$ 发送给 Bob, $S_1$ 自己保留. Bob 随机选择测量基对序列 $S_2$ 中部分粒子进行测量, 并将选择的粒子位置、使用的测量基、测量结果通过无法更改的经典信道发送给 Alice. Alice 对序列 $S_1$ 中 Bob 抽样粒子对应位置的粒子进行测量, 选择与 Bob 相同的测量基, 测量结果与 Bob 发送的测量结果进行对比. 例如对于量子态为 $1/\sqrt{2}(|00\rangle+|11\rangle)$, 用 $Z$ 基对 1 个粒子测量后再对第 2 个粒子测量, 两个粒子的测量结果将相同; 对于量子态为 $1/\sqrt{2}\,(|01\rangle+|10\rangle)$, 用 $Z$ 基对第 1 个粒子测量后再对第 2 个粒子测量, 两个粒子的测量结果将相反. 若误差率高于双方可承受的最大阈值则可能存在第三方窃听, 放弃通信排查信道; 若低于阈值, 则信道安全, 通信继续.

Alice 与 Bob 去除用于窃听检测的抽样粒子得到新的 $S_1$ 与 $S_2$.

Alice 根据共享秘钥 $K\,(K_1K_2\cdots K_n)\,(K_i=0$ 或 $1,\ i\in[1,\ n])$, 对序列 $S_1$ 按照一定规则进行操作, 得出一段位置序列 $L\,(L_1L_2\cdots L_n)$ 规则如下.

1) 若 $K_1=0$, 先测量 $S_1$, 再在测量后的 $S_1$ 中找到第一个 $|0\rangle$; 若 $K_1=1$, 先测量 $S_1$, 再在测量后的 $S_1$ 中找到第一个 $|+\rangle$, 然后记录其位置 $L_1$.

2) 若 $K_2=0$, 在 $S_1$ 中位置 $L_1$ 之后找到第一个 $|0\rangle$; 若 $K_2=1$, 在 $S_1$ 序列中位置 $L_1$ 之后找到第一个 $|+\rangle$, 然后记录其位置 $L_2$.

……

$n$) 若 $K_n=0$, 在 $S_1$ 序列中位置 $L_{n-1}$ 之后找到第一个 $|0\rangle$; 若 $K_n=1$, 在 $S_1$ 序列中位置 $L_{n-1}$ 之后找到第一个 $|+\rangle$, 然后记录其位置 $L_n$.

遍历完共享密钥 $K$ 之后, 得出一个位置序列 $L\,(L_1L_2\cdots L_n)$, 并将该位置序列公布给 Bob, 步骤 2)—$n$) 可能需要消耗大量的 Bell 态粒子.

Bob 根据之前掌握的共享秘钥 $K(K_1K_2\cdots K_n)$:

当 $K_i=0$ 时, 取 $Z$ 基对序列 $S_2$ 中位置 $L_i$ 处的 Bell 态粒子进行单光子测量;

当 $K_i=1$ 时, 取 $X$ 基对序列 $S_2$ 中位置 $L_i$ 处的 Bell 态粒子进行单光子测量.

对测量结果进行解码: $|0\rangle\to0$, $|+\rangle\to1$. 由此得到一个二进制字符串 $K_{\rm b}$, 对比两个字符串 $K_{\rm b}$ 与 $K$. 当 $K_{\rm b}=K$ 时身份认证成功, Bob 确认 Alice 的身份, 继续通信. 当 $K_{\rm b}\neq K$ 或测量结果中出现除 $|0\rangle$ 与 $|+\rangle$ 外的其他量子态时身份认证失败, 放弃通信.

**步骤 4** 编码信息, 制作可以表示秘密信息的混合态量子序列.

在双方进行身份认证后, 去掉用于身份认证的粒子序列. 此时 Bob 已经获得了粒子序列 $S_2$, Alice 将自己手中的 Bell 态粒子序列 $S_1$ 与单光子序列 $S_{\rm S}$ 共同组成混合量子态序列 $S_{1\text{-}{\rm S}}$, 并记下 $S_1$ 与 $S_{\rm S}$ 在 $S_{1\text{-}{\rm S}}$ 的位置. 按照双方事先商量好的编码规则编码, 按照对应的编码规则用量子态来表示要传输的二进制信息.

编码规则见表 1. 例如现在 Alice 要传输一段二进制字符串 $M$ 给 Bob, 首先要用混合粒子序列 $S_{1\text{-}{\rm S}}$ 来表示字符串 $M$. 这一步存在两种方式: 一种是 Alice 在步骤 1 制备单光子序列与 Bell 态粒子序列时根据传输的信息来制备, 制备的量子比特按照对应的编码规则表示一个 3 位二进制字符串, 在单光子与 Bell 态组成混合粒子序列 $S_{1\text{-}{\rm S}}$ 时按照秘密信息来进行顺序排列. 另一种相比第一种, Alice 需要多进行一些量子逻辑门操作, Alice 利用幺正操作或 Hadamard 门操作对混合量子态序列 $S_{1\text{-}{\rm S}}$

表 1 编码规则

Table 1. Coding rules.

| 单光子 | 表示的经典信息 | Bell态 | 表示的经典信息 |
|---|---|---|---|
| $\|0\rangle$ | 000 | $\|\psi^+\rangle$ | 010 |
| $\|1\rangle$ | 111 | $\|\psi^-\rangle$ | 101 |
| $\|+\rangle$ | 001 | $\|\varphi^+\rangle$ | 011 |
| $\|-\rangle$ | 110 | $\|\varphi^-\rangle$ | 100 |

进行转化, 转化为按照编码规则可以表示秘密信息 $M$ 的粒子序列 (如初始态为$|0\rangle$但欲传输的信息为 111, 可对$|0\rangle$进行$U_x$操作转化为$|1\rangle$, $|1\rangle$对应的编码为 111).

**步骤 5** Alice 使用顺序重排技术对混合量子态序列 $S_{1\text{-S}}$进行顺序重排, 得到序列 $S'_{1\text{-S}}$并在其中加入检测粒子得到 $S''_{1\text{-S}}$. Alice 将序列 $S''_{1\text{-S}}$发送给 Bob, Bob 利用光纤的延时性对 $S''_{1\text{-S}}$进行延迟接收, 防止在 Alice 向 Bob 公布信息时部分量子态还未传输完毕, 造成信息的泄露.

**步骤 6** Bob 收到完整信息后告知 Alice, Alice 向 Bob 公布序列 $S''_{1\text{-S}}$中检测粒子的位置和测量基, Bob 根据 Alice 公布的位置和对应的测量基, 从序列 $S''_{1\text{-S}}$中取出检测粒子进行测量, 得到序列 $S'_{1\text{-S}}$, 同时把测量结果发送给 Alice. Alice 对比加入检测粒子的初始态, 若误差率高于阈值则可能存在窃听, 放弃通信. 若误差率低于阈值则通信继续.

**步骤 7** Alice 向 Bob 公布 $S_{1\text{-S}}$的排列顺序及各位置对应的正确测量基: $Z$ 基 ($|0\rangle$, $|1\rangle$), $X$ 基 ($|+\rangle$, $|-\rangle$)和 Bell 联合基. Bob 根据 Alice 提供排列顺序将 $S'_{1\text{-S}}$还原为 $S_{1\text{-S}}$, 用 Alice 提供的正确测量基测量单光子或对 Bell 态粒子进行 Bell 基联合测量, 对测量结果按照编码规则进行译码得到秘密信息 $M$.

## 3 方案举例说明

假设双方共享秘钥 $K$ 为1001, 传输信息 $M$ 为 010111011110011110000100.

秘钥 0 由$|0\rangle$表示, 1 由$|+\rangle$表示. 第一次身份认证中, Alice 利用 $S_n$ 中随机加入的检测粒子进行窃听检测后, 去除所有的检测粒子, 得到序列 $S_n$. Bob 制备的单光子序列 $S_n$ 为$|+\rangle$, $|0\rangle$, $|0\rangle$, $|+\rangle$, 认证过程见表 2.

表 2 基于单光子身份认证过程

Table 2. Single photon based identity authentication process.

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 秘钥$K$ | 1 | 0 | 0 | 1 |
| 序列 $S_n$ 量子态 | $\|+\rangle$ | $\|0\rangle$ | $\|0\rangle$ | $\|+\rangle$ |
| 合法Alice根据$K$选测量基 | $X$ | $Z$ | $Z$ | $X$ |
| 合法Alice测量结果 | $\|+\rangle$ | $\|0\rangle$ | $\|0\rangle$ | $\|+\rangle$ |
| 冒充Alice测量结果 (随机选择测量基) | 50% $\|+\rangle$<br>25% $\|0\rangle$<br>25% $\|1\rangle$ | 50% $\|0\rangle$<br>25% $\|+\rangle$<br>25% $\|-\rangle$ | 50% $\|0\rangle$<br>25% $\|+\rangle$<br>25% $\|-\rangle$ | 50% $\|+\rangle$<br>25% $\|0\rangle$<br>25% $\|1\rangle$ |

第 2 次身份认证由 Alice 向 Bob 发送 Bell 态粒子序列 $S_2$, Bob 在原序列中随机选择抽样粒子进行窃听检测, 由 Alice 判断信道是否安全. 确定不存在第三方窃听后, 双方去除抽样粒子, 得到新的 $S_1$ 和 $S_2$, 身份认证见表 3. 由表 3 可得 Alice 公布的粒子序列为 $L$ (4, 5, 15, 18), Bob 选择的测量基为 $X$ 基, $Z$ 基, $Z$ 基和 $X$ 基. 测得结果为单光子序列$|+\rangle$, $|0\rangle$, $|0\rangle$, $|+\rangle$, 解码得 1001.

根据表 2 和表 3 可以看出第三方在不知道秘钥 $K$ 的情况下, 测到正确秘钥 $K$ 的概率为 $50\%\times 50\%\times 50\%\times 50\% = 6.25\%$, 第三方想要冒充任意一方进行身份认证, 成功冒充的概率为 6.25%, 即双方共享 $n$ 位秘钥 $K$, 被冒充的概率就为 $(50\%)^n$. $n$ 取值越大被冒充的概率越小, 此处 $n = 4$, 在实际通信中 $n$ 可以取更大的值来确保通信双方身份.

信息传输过程, Alice 去除 $S_1$ 中用于窃听检测和身份认证的粒子, 与单光子混合进行信息编码后加入检测粒子发送给 Bob, 省去窃听检测过程见表 4.

表 3 基于 Bell 态身份认证过程

Table 3. Identity authentication process based on Bell state.

| $\varphi^+$或$\varphi^-$在$S_1$中位置 | 1 | 4 | 5 | 9 | 11 | 12 | 15 | 17 | 18 | ··· |
|---|---|---|---|---|---|---|---|---|---|---|
| 量子态 | $\|0\rangle$ | $\|+\rangle$ | $\|0\rangle$ | $\|+\rangle$ | $\|-\rangle$ | $\|1\rangle$ | $\|0\rangle$ | $\|-\rangle$ | $\|+\rangle$ | ··· |
| 共享秘钥$K$ | | 1 | 0 | | | | 0 | | 1 | |
| Alice公布位置$L$ | | 4 | 5 | | | | 15 | | 18 | |
| 根据$K$选择测量基 | | $X$ | $Z$ | | | | $Z$ | | $X$ | |
| 合法Bob测量结果 | | $\|+\rangle$ | $\|0\rangle$ | | | | $\|0\rangle$ | | $\|+\rangle$ | |
| 冒充Bob 测量结果 | | 50%$\|+\rangle$<br>25%$\|0\rangle$<br>25%$\|1\rangle$ | 50%$\|0\rangle$<br>25%$\|+\rangle$<br>25%$\|-\rangle$ | | | | 50%$\|0\rangle$<br>25%$\|+\rangle$<br>25%$\|-\rangle$ | | 50%$\|+\rangle$<br>25%$\|0\rangle$<br>25%$\|1\rangle$ | |

表 4 信息传输过程

Table 4. Information transmission process.

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 秘密信息$M$ | 010 | 111 | 011 | 110 | 011 | 110 | 000 | 100 |
| 混合态序列$S_{1-S}$量子态 | $\|\psi^+\rangle$ | $\|1\rangle$ | $\|\varphi^+\rangle$ | $\|-\rangle$ | $\|\varphi^+\rangle$ | $\|-\rangle$ | $\|0\rangle$ | $\|\varphi^-\rangle$ |
| Alice公布的测量基 | Bell基 | $Z$基 | Bell基 | $X$基 | Bell基 | $X$基 | $Z$基 | Bell基 |
| Bob测量结果 | $\|\psi^+\rangle$ | $\|1\rangle$ | $\|\varphi^+\rangle$ | $\|-\rangle$ | $\|\varphi^+\rangle$ | $\|-\rangle$ | $\|0\rangle$ | $\|\varphi^-\rangle$ |
| 解码得信息$M$ | 010 | 111 | 011 | 110 | 011 | 110 | 000 | 100 |

## 4 安全性分析

QSDC 方案中的通信安全是指通信过程中不存在第三方 Eve 的窃听, 即使存在窃听, 第三方 Eve 也一定会被合法的通信双方发现, 且 Eve 不能从截获的量子态中获得任何秘密信息. 方案中用到的顺序重排和延时接收技术都是为了确保通信安全, 下面从 3 种典型的攻击模式分析方案安全性.

### 4.1 截获/测量重发攻击

该方案在第 1 次传输只用到单光子, 第 2 次只用到 Bell 态粒子, 第 3 次用到了 Bell 态与单光子混合的混合态粒子. 测量重发攻击: 第三方 Eve 成功截获 Alice 发送给 Bob 的量子序列, 并进行测量后发送给 Bob, 意在做到双方不知情的情况下获取秘密信息.

第 1 次通信, Bob 在得到 Alice 收到信息的通知后才会公布检测粒子的位置和测量基, 因此 Eve 在截获单光子序列后只能随机选择测量基进行测量, 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, 即 Eve 截获量子态越多其不被发现的概率就越小. 错误的测量基会使单光子状态发生塌缩, 在后续的窃听检测中就会被发现.

第 2 次通信 Alice 发送 Bell 态粒子序列给 Bob, Bob 随机测量发送给 Alice 进行窃听检测. 如果 Eve 截获部分 Bell 态序列 $S_2$ 并随机选择测量基进行单光子测量后发送给 Bob, 必定会引起 Alice 手中纠缠粒子序列 $S_1$ 的塌缩, 在后续 Alice 的窃听检测中必定会被发现.

第 3 次通信双方传输秘密信息, 并在混合粒子序列中加入检测粒子. 接收方 Bob 采用延时接收来确保不会因为部分光子态未接收完毕造成信息泄露, Eve 若能截获到粒子序列, 只能进行随机测量, 因此必定会在 Bob 进行窃听检测时被发现. 即使 Eve 能够侥幸对部分序列做出正确的测量, 因为 Alice 在发送信息时进行了顺序重排, Eve 对正确排列顺序无从得知, 所以 Eve 得不到任何有用信息.

截获重发攻击: 在通信过程中, Eve 截获部分量子序列并将自己提前准备的量子态发送给接收方, 在双方后续公布测量基等信息时完成信息窃取. 但是 Eve 对量子态的制备只能通过随机数来完成, 在合法双方的窃听检测中一定会被发现, 终止通信, Eve 因此无法进行正确的测量, 不能获得任何有用信息.

### 4.2 辅助粒子攻击

辅助粒子攻击指的是 Eve 借助辅助粒子对截获的量子态进行纠缠. 该攻击涉及到 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 $I_{\rm E}$. 通信中涉及到单光子和 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:

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

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

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

$$\hat{\boldsymbol{E}}\otimes|-e\rangle=\frac{1}{\sqrt{2}}(a\,|0e_{00}\rangle+b|1e_{01}\rangle-b'\,|0e_{10}\rangle - a'|1e_{11}\rangle)$$

$$=\frac{1}{2}[|+\rangle(a|e_{00}\rangle+b|e_{01}\rangle-b'|e_{10}t\rangle-a'|e_{11}\rangle) + |-\rangle(a|e_{00}\rangle-b|e_{01}\rangle-b'|e_{10}\rangle+a'|e_{11}\rangle)]. \quad (5)$$

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

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

Eve 的幺正操作$\hat{\boldsymbol{E}}$矩阵表示为

$$\hat{\boldsymbol{E}}=\begin{pmatrix}a & b'\\ b & a'\end{pmatrix}. \quad (7)$$

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

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

所以有

$$|a|^2=|a'|^2,\ |b|^2=|b'|^2. \quad (9)$$

幺正操作引起的错误率, 即 Eve 窃听被检测到的概率:

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

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

$$\hat{\boldsymbol{E}}\otimes|0e\rangle=a|0e_{00}\rangle+b|1e_{01}\rangle, \quad (11)$$

$$\hat{\boldsymbol{E}}\otimes|1e\rangle=b'\,|0e_{10}\rangle+a'\,|1e_{11}\rangle. \quad (12)$$

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

$$|\varphi\rangle_{\text{Eve}}=\hat{\boldsymbol{E}}\otimes\frac{|0e\rangle\otimes|0\rangle+|1e\rangle\otimes|1\rangle}{\sqrt{2}}$$

$$=\frac{1}{\sqrt{2}}[(a\,|0e_{00}\rangle+b\,|1e_{01}\rangle)\otimes|0\rangle + (b'\,|0e_{10}\rangle+a'\,|1e_{11}\rangle)\otimes|1\rangle]$$

$$=\frac{1}{\sqrt{2}}[(a\,|0e_{00}0\rangle+b\,|1e_{01}0\rangle) + (b'\,|0e_{10}1\rangle+a'\,|1e_{11}1\rangle)]. \quad (13)$$

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

$$p_{\text{Eve}}=\frac{|a|^2+|a'|^2}{2}=|a|^2. \quad (14)$$

窃听被检测到的概率:

$$p_{\text{error}}=1-p_{\text{Eve}}=1-|a|^2=1-|a'|^2. \quad (15)$$

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$I_{\text{E}}$的分析.

每一个光子的约化密度矩阵为

$$\boldsymbol{\rho}=\frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}. \quad (16)$$

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

$$|\varphi\rangle_{\text{Eve}}=\hat{\boldsymbol{E}}\otimes|0e\rangle=a\,|0e_{00}\rangle+b\,|1e_{01}\rangle. \quad (17)$$

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

$$\boldsymbol{\rho}'=|\varphi\rangle_{\text{Eve}}\langle\varphi|_{\text{Eve}}$$

$$=|a|^2\,|0e_{00}\rangle\langle 0e_{00}|+|b|^2\,|1e_{01}\rangle\langle 1e_{01}| + ab^{*}\,|0e_{00}\rangle\langle 1e_{01}|+a^{*}b\,|1e_{01}\rangle\langle 0e_{00}|. \quad (18)$$

用矩阵表示为

$$\boldsymbol{\rho}'=\begin{pmatrix}|a|^2 & ab^{*}\\ a^{*}b & |b|^2\end{pmatrix}. \quad (19)$$

解密度算子$\boldsymbol{\rho}'$的特征值$\lambda$:

$$\det\begin{bmatrix}|a|^2-\lambda & ab^{*}\\ a^{*}b & |b|^2-\lambda\end{bmatrix}=0. \quad (20)$$

特征方程:

$$\left(|a|^2-\lambda\right)\times\left(|b|^2-\lambda\right)-ab^{*}\times a^{*}b=0. \quad (21)$$

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

$$I_{\text{E}}=\chi(\boldsymbol{\rho}')=-\sum_{i=0}^{1}\lambda_i\log_2\lambda_i=0. \quad (22)$$

由 (22) 式得, 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:

$$\chi(\boldsymbol{\rho})=S(\boldsymbol{\rho})-\sum_{i=1}^{8}p_iS(\rho_i), \quad (23)$$

式中, $S(\boldsymbol{\rho})$为态$\boldsymbol{\rho}$的 von-Neumann 熵.

$$\rho=\sum_{i=1}^{8}p_i\rho_i,$$

式中, $\rho_i$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

$$\begin{aligned} H(p) =& -\sum_{i=1}^{8} p_i \log_2 p_i \\ =& -p_{000}\log_2 p_{000} - p_{001}\log_2 p_{001} \\ & - p_{010}\log_2 p_{010} - p_{100}\log_2 p_{100} \\ & - p_{101}\log_2 p_{101} - p_{110}\log_2 p_{110} \\ & - p_{011}\log_2 p_{011} - p_{111}\log_2 p_{111} \\ =& 3, \end{aligned} \tag{24}$$

则可以得到

$$I_{\mathrm{E}} = \chi(\boldsymbol{\rho}') = S(\boldsymbol{\rho}') - \sum_{i=1}^{8} p_i S(\rho_i') < H(p). \tag{25}$$

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

### 4.3 身份冒充攻击

身份冒充: 通信双方中任一方被第三方 Eve 冒充代替, 造成信息泄露.

当 Eve 试图冒充 Bob 从 Alice 处获得秘密信息. 通信开始, Alice 要求 Bob 进行身份认证, 因为 Eve 没有掌握二进制秘钥 $K$, 只能通过随机数制备单光子序列发送给 Alice, 每位随机数选择正确的概率为 50%, Eve 选取的随机数与 $K$ 相同的概率为 $(50\%)^n$, 当 $n \geqslant 7$ 时, Eve 就有 99% 以上的概率会暴露. 因此只要双方共享二进制秘钥位数足够, Eve 的冒充就一定会被发送方 Alice 发现.

当 Eve 试图冒充 Alice 发送错误信息. 通信开始, Bob 首先向 Eve 发送单光子序列进行身份认证. Bob 仅向 Eve 传输了制备的单光子序列, 没公布其他任何信息, Eve 虽然得到单光子序列但是因为不知道秘钥 $K$, 所以无法选择正确测量基测得正确量子态. 由表 4 可知, 共享 4 位秘钥 $K$, Eve 测得正确量子序列的概率为 $50\%\times50\%\times50\%\times50\% = 6.25\%$. 所以只要共享秘钥 $K$ 位数足够, 后续 Eve 冒充 Alice 向 Bob 发送身份认证信息时, 一定会被接收方 Bob 发现.

可见无论是冒充哪一方, Eve 都需要以得到正确的秘钥 $K$ 为前提. 在 Eve 不知道秘钥 $K$ 的情况下, 其冒充成功的概率为 $(50\%)^n$, 只要秘钥 $K$ 位数 $n \geqslant 7$, Eve 就会有 99% 以上的概率被发现, 不可能成功完成身份冒充.

## 5 效率和编码容量分析

本方案的编码容量见表 5, 每比特的单光子或 Bell 态粒子对可表示 3 bits 的经典信息, 虽然每个 Bell 态纠缠粒子对含有 2 bits 纠缠粒子, 但是在第 1 次传输其中一半 Bell 态粒子序列时不含有秘密信息, 只有在第 2 次传输混合态粒子序列是才对其进行编码. 所以可以认为, 在第 2 次传输时其编码容量达到 1 qubit 可以表示 3 bits 经典信息.

表 5 各方案参数对比

Table 5. Comparison of parameters of various schemes.

| 协议 | 传输效率 $\xi$ | 量子比特利用率 $\eta$ | 编码容量 |
|---|---|---|---|
| QSDC协议[10] | 1 | 1 | 一个态: 1.0 bit |
| One-Pad-Time-QSDC协议[11] | 1 | 1 | 一个态: 1.0 bit |
| 基于纠缠交换的QSDC协议[12] | 1 | 1 | 一个态: 1.0 bit |
| Bell态和单光子混合QSDC协议[22] | 1 | 1 | 一个态: 1.5 bits |
| 本协议 | 1 | 1 | 一个态: 3.0 bits |

传输效率 $\xi$ 可以定义为

$$\xi = \frac{b_{\mathrm{s}}}{q_{\mathrm{t}} + b_{\mathrm{t}}}, \tag{26}$$

式中, $b_{\mathrm{s}}$ 表示通信双方传输秘密信息的二进制比特数, $q_{\mathrm{t}}$ 表示方案中传输的量子比特数, $b_{\mathrm{t}}$ 表示通信中传输的经典比特数.

本方案为 QSDC 方案, 在通信过程中对经典信道的依赖很小, 大多用来辅助通信方案进行窃听检测时使用, 因此在传输效率分析时可以不考虑传输的经典比特数 $b_{\mathrm{t}}$. 根据表 1 可以得出, 每传输一个单光子可以达到传输 3 bits 经典信息的目的, 每传输一个 Bell 态纠缠粒子对也可以达到传输 3 bits 经典信息的目的, 但是每个 Bell 态粒子对含有 2 bits 的粒子. 因此在传输效率的计算中, $3n$ bits 的经典信息可以通过 $n$ bits 的单光子, 或 $2n$ bits 的 Bell 态纠缠粒子来传输. 即

$$\xi = \frac{b_{\mathrm{s}}}{q_{\mathrm{t}} + b_{\mathrm{t}}} = \frac{3n}{(n+2n)/2} = 2\,(\text{倍}). \tag{27}$$

量子比特利用率可以定义为 $\eta = q_{\mathrm{u}}/q_{\mathrm{t}}$, $q_{\mathrm{u}}$ 表示在通信方案中携带信息的有效比特数, $q_{\mathrm{t}}$ 表示方案

中传输的总量子比特数. 本方案中, $\eta = q_{\rm u}/q_{\rm t} = 1$. 结合一些已有的 QSDC 经典方案, 将其与本方案的量子通信传输效率、编码容量作为对比, 结果在表 5 列出. 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, 编码容量较高且方案中不存在文献 [17] 中的信息泄露问题.

## 6 结 论

针对以往的 QSDC 方案需要假设通信双方合法性的问题, 本文提出一种带双向身份认证的 QSDC 方案, 设计了方案的通信过程和编码规则, 其中分别利用单光子和 Bell 态粒子来验证发送方 Alice 和接收方 Bob 的合法性, 一旦检测到冒充攻击可以立刻停止通信, 不会造成信息泄露, 从而解决了通信双方可能被外部攻击者冒充的风险. 安全性分析证明, 本方案可以抵御常见的内部攻击和外部攻击, 此外, 该方案有较高的传输效率和编码容量, 且协议过程简单, 不涉及复杂的幺正变换, 更易于实现.

## 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] Kwek L C, Cao L, Luo W, Wang Y X, Sun S H, Wang X B, Liu A Q 2021 *AAPPS Bull.* **31** 15
[4] Guo H, Li Z Y, Yu S, Zhang Y C 2021 *Fundament. Res.* **1** 96
[5] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C, Makarov V 2011 *Nat. Commun.* **2** 349
[6] Beige A, Englert B G, Kurtsiefer C 2002 *J. Phys. A Math. Gen.* **35** L407
[7] Quan D X, Zhu C H, Liu S Q, Pei C X 2015 *Chin. Phys. B* **24** 256
[8] Li Y B, Song T T, Huang W 2015 *Internat. J. Theoretical Phys.* **54** 589
[9] Long G L, Liu X S 2002 *Phys. Rev. A* **65** 032302
[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] Wang C, Deng F G, Li Y S 2005 *Phys. Rev. A* **71** 044305
[13] Wang J, Zhang Q, Tang C J 2006 *Phys. Lett. A* **358** 256
[14] Man Z X, Xia Y J 2007 *Chin. Phys. Lett.* **24** 15
[15] Lan M, Shao T N, Xie J L, Yang X F, Sun K, Cai T T, Wang J Z 2011 *Sci. China Phys. Mech. Astron.* **54** 942
[16] Li K, Huang X Y, Teng J H, Li Z H 2012 *J. Electron. Inf. Tech.* **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] An H Y, Liu D W, Geng R H, Zeng H P, Zhao L X 2016 *Syst. Eng. Electron. Tech.* **38** 1917 (in Chinese) [安辉耀, 刘敦伟, 耿瑞华, 曾和平, 赵林欣 2016 系统工程与电子技术 **38** 1917]
[18] Long G L 2015 *The 11 th National Symposium on Optical Frontiers* Changsha, China, October 9, 2015 p21 (in Chinese) [龙桂鲁 2015 十一届全国光学前沿研讨会 长沙 2015-10-09 p21]
[19] Hu J Y, Yu B, Jing M Y, Xiao L T, Jia S T, Qin G Q, Long G L 2016 *Light Sci. Appl.* **5** e16144
[20] Zhang W, Ding D S, Sheng Y B, Zhou L, Shi B S, Guo G C 2017 *Phys. Rev. Lett.* **118** 220501
[21] Zhu F, Zhang W, Sheng Y B, Huang Y D 2017 *Sci. Bull.* **62** 1519
[22] 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]
[23] 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]
[24] Zhao N, Jiang Y H, Zhou X T, Guo C F, Liu B 2021 *Network Security Technology* **8** 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 **8** 30]
[25] Zhou X T, Jiang Y H, Guo C F, Zhao N, Liu B 2021 *Chin. J. Quantum Electron.* **39** 768 (in Chinese) [周贤韬, 江英华, 郭晨飞, 赵宁, 刘彪 2021 量子电子学报 **39** 768]
[26] 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]
[27] 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]
[28] 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]
[29] Qi R Y, Sun Z, Lin Z S, Niu P H, Hao W T, Song L Y, Huang Q, Gao J C, Yin L G, Long G L 2019 *Light Sci. Appl.* **8** 22
[30] Zhang H R, Sun Z, Qi R Y, Yin L G, Long G L, Lu J H 2022 *Light Sci. Appl.* **11** 83
[31] Wang C 2021 *Fundament. Res.* **1** 91

# Quantum secure direct communication scheme based on the mixture of single photon and Bell state with two way authentication*

Zhou Xian-Tao Jiang Ying-Hua† Guo Xiao-Jun Peng Zhan

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

( Received 15 October 2022; revised manuscript received 10 April 2023 )

**Abstract**

In response to the demand for identity authentication in quantum secure direct communication, this paper proposes a quantum secure direct communication scheme based on a mixture of single photon and Bell state, by combining the bidirectional identity authentication. Before communication begins, both parties share a series of secret information to prepare a series of single photon and Bell state particles. Encoding four single photons and four Bell states yields eight types of encoded information, followed by identity authentication. The first step in identity authentication is to use a single photon to verify the legitimacy of the receiver. If the error exceeds the given threshold, it indicates the presence of eavesdropping. Otherwise, the channel is safe. Then, Bell state particles are used to verify the legitimacy of the sender, and the threshold is also used to determine whether there is eavesdropping. The present method is the same as previous one. If the error rate is higher than the given threshold, it indicates the existence of third-party eavesdropping. Otherwise, it indicates that the channel is secure. As for the specific verification method, it will be explained in detail in the article. Afterwards, Bell state particles are mixed with a single photon as a transmission carrier, and eavesdropping detection particles are added whenever the quantum state is sent. However, once the eavesdropper intercepts the transmitted particles, owing to incomplete information obtained, the eavesdropper is unable to recover the original information, and the eavesdropping behavior will be immediately detected, thus terminating communication. In this scheme, single photon and Bell states are fully utilized, and hybrid communication can effectively improve transmission efficiency, encoding capability, and quantum bit utilization. Security analysis shows that this scheme can resist common external and internal attacks such as interception/measurement replay attacks, auxiliary particle attacks, and identity impersonation attacks. The analysis of efficiency and encoding capacity shows that the transmission efficiency of this scheme is 1, the encoding capacity is 3 bits per state, and the quantum bit utilization rate is 1. Compared with other schemes, this scheme has significant advantages because it uses different particles for bidirectional authentication, making it more difficult for attackers to crack, and thus it has higher security than traditional schemes.

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

**PACS:** 03.67.Hk, 03.67.Dd **DOI:** 10.7498/aps.72.20221972

* Project supported by the Department of Education Research Special Scientific Research Plan of Shaanxi Province, China (Grant No. 19JK0889) and the Natural Science Foundation of Tibet Autonomous Region, China (Grant Nos. XZ2019ZRG-36(Z), XZ202101ZR0089G).

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