第 59 卷 第 11 期/2022 年 6 月/激光与光电子学进展 研究论文

激光与光电子学进展

基于Brown态的可认证半量子对话协议

冯舟靓[1,2]，柏明强[1,2*]，莫智文[1,2**]

[1]四川师范大学数学科学学院，四川 成都 610066；

[2]四川师范大学智能信息和量子信息研究所，四川 成都 610066

摘要 半量子对话在量子通信中具有较强的实用性，其部分用户端无需配备昂贵的量子设备。基于Brown态提出了一个四方的可认证半量子对话协议，并利用广义的Brown态将上述协议推广到多方。通过安全性分析，验证了协议不存在信息泄露问题，且能有效抵抗截获重发攻击、中间人攻击、干扰攻击和特洛伊木马攻击。与同类型协议的分析比较表明，所提协议具有较高的量子通信效率。

关键词 量子光学；半量子对话；Brown态；身份认证；多方协议

中图分类号 O413.2 **文献标志码** A **DOI**：10.3788/LOP202259.1127003

Authenticated Semi-Quantum Dialogue Protocol Based on Brown States

Feng Zhoujing[1,2], Bai Mingqiang[1,2*], Mo Zhiwen[1,2**]

[1]*School of Mathematical Sciences, Sichuan Normal University, Chengdu* 610066, *Sichuan, China*;

[2]*Institute of Intelligent Information and Quantum Information, Sichuan Normal University, Chengdu* 610066, *Sichuan, China*

Abstract Semi-quantum dialogue has a relatively strong practicality in quantum communications, and its partial users do not need to be equipped with expensive quantum devices. A four-party authenticated semi-quantum dialogue protocol based on the Brown states is proposed. Then, the proposed protocol is extended to multi-party using the generalized Brown states. Through security analysis, it is verified that the proposed protocol does not have the information leakage problem and can effectively resist the intercept-resend attack, man-in-the-middle attack, disturbance attack and Trojan horse attack. The analysis comparison with the similar protocols shows that the proposed protocol has high quantum communication efficiency.

Key words quantum optics; semi-quantum dialogue; Brown state; identity authentication; multi-party protocol

1 引 言

基于量子力学特性，量子通信具有物理原理上的绝对安全性[1]。随着国内外学者的深入研究，众多量子通信协议被相继提出，主要包括量子密钥分配协议[2-6]、量子隐形传态协议[7-10]、量子安全直接通信协议[11-13]。大部分量子通信协议的实现，要求通信双方都具备量子制备、Bell测量等较强的量子操作能力。由于量子态生成器、量子测量等相关设备价格昂贵，普通用户无法具备上述能力，这为量子通信在现实生活中的应用增加了困难。2007年，Boyer等[14]给出半量子概念，在Bob为经典方的前提下提出了量子密钥分配协议。在半量子通信中，通信方包括量子方和经典方。其中，量子方具有完

收稿日期：2021-06-25；**修回日期**：2021-07-21；**录用日期**：2021-07-30

基金项目：国家自然科学基金(11671284)、四川省科技计划资助项目(2020YFG0290)

通信作者：*baimq@sicnu.edu.cn；**mozhiwen@sicnu.edu.cn

全的量子操作能力，经典方只具备如下能力：1）返还：对收到的粒子不做任何处理，直接返还给量子方；2）测量：利用Z基（{| 0 〉,| 1 〉}）对粒子进行测量；3）制备：利用Z基制备粒子，并将其发送给量子方；4）重排：借助延迟装置，对收到的粒子进行重新排序。通常约定，返还操作也称CTRL操作，经典方测量收到的粒子并制备相同状态的粒子发送给量子方称测量重发（SIFT）操作。此后，半量子概念被广泛应用于量子通信中[15-17]。2017年，Shukla等[18]指出在量子方使用量子资源增加的前提下，绝大部分由两个量子方执行的通信都可以通过半量子方式执行，并提出半量子密钥协商协议、半量子受控安全直接通信协议和半量子对话协议。

与其他类型的半量子通信相比，半量子对话具有通信双方可同时交换秘密信息的优势。随着在半量子对话领域的不断探索，各种类型的半量子对话协议纷纷被提出[19-20]。2018年，Liu等[21]基于安全委托量子计算提出了身份认证半量子对话协议。众所周知，身份认证的加入可以提高协议的实际应用性和安全性。一方面，通信方的身份是否合法是未知的，身份认证的步骤不可缺少；另一方面，身份认证的加入可以在一定程度上抵抗中间人攻击的问题。因此，探索如何在通信协议中引入身份认证具有一定的理论价值和实际意义。

多粒子纠缠态在量子通信中扮演着重要的角色。利用不同的纠缠态，大量的半量子对话协议被提出。例如，2020年，Xu等[22]基于Cluster态提出了三方半量子对话协议；2021年，Zhou等[23]基于GHZ态提出了三方的半量子对话协议。事实上，在大多实际的通信过程中，参与者的数量是远大于三方的。因此，研究如何完成更多参与方的半量子对话是必然的。2005年，Brown等[24]通过数值优化过程发现了Brown态。2008年，Muralidharan等[25]将上述Brown态应用于量子隐形传态、量子态共享和超密集编码，并给出了广义的Brown态定义。与GHZ态、W态和Cluster态相比，Brown态表现出了更强的纠缠性[26]。本文以Brown态为信道，提出了一个四方的可认证半量子对话协议，并利用广义的Brown态将上述协议推广到多方。对协议的安全性进行分析，其中包括信息泄露分析和常见攻击分析。同时计算了协议的效率，并将其与几个同类型的协议进行对比分析和总结。

2 协议提出及推广

在提出协议之前，先给出Brown态和广义Brown态的具体形式，分别为

$$\left|B_5\right\rangle=\left(\left|001\right\rangle\left|\phi^-\right\rangle+\left|010\right\rangle\left|\phi^-\right\rangle+\left|100\right\rangle\left|\phi^+\right\rangle+\left|111\right\rangle\left|\phi^+\right\rangle\right)/2, \tag{1}$$

$$\left|B_{n+5}\right\rangle=\left(\left|\eta_1\right\rangle_n\left|001\right\rangle\left|\phi^-\right\rangle+\left|\eta_2\right\rangle_n\left|010\right\rangle\left|\phi^-\right\rangle+\left|\eta_3\right\rangle_n\left|100\right\rangle\left|\phi^+\right\rangle+\left|\eta_4\right\rangle_n\left|111\right\rangle\left|\phi^+\right\rangle\right)/2, \tag{2}$$

式中：$\left|\phi^{\pm}\right\rangle=(\left|00\right\rangle\pm\left|11\right\rangle)/\sqrt{2}$；$\left|\psi^{\pm}\right\rangle=(\left|01\right\rangle\pm\left|10\right\rangle)/\sqrt{2}$]；$\left|\eta_i\right\rangle$为形成第$n$阶的计算基。

协议以5粒子的Brown态为信道，参与方有1个量子方Charlie和3个经典方Alice$_i$（$i=1, 2, 3$）。协议的具体步骤如下：

事先约定：身份密钥分别为$K_c=\{K_c^1, K_c^2, \cdots, K_c^N\}$，$K_i=\{K_i^1, K_i^2, \cdots, K_i^N\}$；待传输的秘密信息分别为$m_c=\{m_c^1, m_c^2, \cdots, m_c^N\}$，$m_i=\{m_i^1, m_i^2, \cdots, m_i^N\}$；身份密钥只在量子方与经典方之间共享。

步骤1 Charlie制备N个Brown态$\left|B_5\right\rangle$，并将这一系列量子态划分为5个粒子序列$C_s=\{q_s^1, q_s^2, \cdots, q_s^N\}$，其中，$s=1, 2, 3, 4, 5$，$q_s$表示态中第$s$个粒子。然后，Charlie根据秘密信息$m_c$的值对粒子序列$C_i$（$i=1, 2, 3$）进行加密得到$C_i'$。规则如下：若$m_c^j=0$，则对$q_i^j$执行$I$操作；若$m_c^j=1$，则对$q_i^j$执行$\sigma_x$操作，其中，$j=1, 2, \cdots, N$，$I=\left|0\right\rangle\left\langle 0\right|+\left|1\right\rangle\left\langle 1\right|$，$\sigma_x=\left|0\right\rangle\left\langle 1\right|+\left|1\right\rangle\left\langle 0\right|$。接着，Charlie随机制备一系列的单光子{| 0 〉,| 1 〉,| + 〉,| − 〉}组成检测粒子序列，并分别记为$D_i=\{d_i^1, d_i^2, \cdots, d_i^N\}$，其中$\left|\pm\right\rangle=(\left|0\right\rangle\pm\left|1\right\rangle)/\sqrt{2}$。最后，根据$K_i$的值，Charlie重组序列$C_i'$，$D_i$得到序列$H_i$，并将其分别发送给Alice$_i$。

步骤2 Alice$_i$收到序列H_i后，根据K_i的值拆分出序列C_i'和D_i。对于序列C_i'，执行Z基测量，并记录结果为Z_i。接着，根据m_i的值，制备新的编码粒子序列，并记为C_i''。规则如下：若$m_i^j=0$，则制备与Z_i^j结果相同的粒子；若$m_i^j=1$，则制备与Z_i^j结果相反的粒子。对于序列D_i，Alice$_i$随机对粒子执行CTRL或SIFT操作得到新的序列D_i'，并将SIFT操作后的测量结果记为C_{D_i}。最后，Alice$_i$根据$K_c\oplus K_i$的值，重组序列C_i''和D_i'得到序列H_i'，并将其发送给Charlie。

步骤 3　Charlie 收到序列 H_i' 后，Alice$_i$ 公布对 D_i' 中粒子执行的操作和相应的结果。Charlie 根据 $K_c \oplus K_i$ 的值拆分出序列 C_i'' 和 D_i'。然后，Charlie 按规则测量检测粒子序列 D_i'，并将结果记为 C_{D_i}'。测量规则如下：若 Alice$_i$ 对粒子 $|+\rangle$，$|-\rangle$ 选择 CTRL 操作，那么 Charlie 对该粒子执行 X 基（$\{|+\rangle, |-\rangle\}$）测量；除此之外，Charlie 对检测粒子均执行 Z 基测量。结果编码规则如下：$|+\rangle \to 0$，$|-\rangle \to 1$，$|0\rangle \to 0$，$|1\rangle \to 1$。最后，Charlie 根据比较测量结果 C_{D_i}'、检测粒子序列 D_i 的值及 Alice$_i$ 公布的结果三者之间的差异，计算下述公式得到误码率：

$$\text{误码率} = \frac{\text{传输的误码数}}{\text{传输的总码数}} \times 100\%。\tag{3}$$

若误码率均低于某个阈值，则身份认证成功且信道安全，可继续通信；反之，停止通信。

步骤 4　Charlie 对序列 C_4，C_5 中的粒子 q_4^j 和 q_5^j 执行 Bell 基测量，并将结果记为 C_B^j。然后利用 Z 基测量序列 C_i''，并记结果为 Z_i'。最后，Charlie 公布 Z_c 和 C_B 的结果，其中，$Z_c = \{(Z_1'^1, Z_2'^1, Z_3'^1), (Z_1'^2, Z_2'^2, Z_3'^2), \cdots, (Z_1'^N, Z_3'^N)\}$，$Z_i'^N$ 为 Z_i' 中第 N 个粒子的值，C_B 的公布规则为 $|\phi^+\rangle \to 00$，$|\phi^-\rangle \to 10$，$|\psi^+\rangle \to 01$，$|\psi^-\rangle \to 11$。

步骤 5　根据 Charlie 公布的信息，Alice$_1$ 推理出所有 C_i 和 Z_i' 的结果，并将 C_i 的值记为 Z_{C_i}。通过计算 $Z_{C_1} \oplus Z_1$，Alice$_1$ 就可得到秘密信息 m_c。然后，计算 $Z_2' \oplus Z_{C_2} \oplus m_c$ 和 $Z_3' \oplus Z_{C_3} \oplus m_c$，Alice$_1$ 就可以得到秘密信息 m_2 和 m_3。同理，Alice$_2$ 和 Alice$_3$ 可以计算得到其余通信方的秘密信息。Charlie 通过对应 C_B 的值可以推算出 C_i，将 C_i 的值记为 Z_{C_i}'，则计算 $Z_i' \oplus Z_{C_i}' \oplus m_c$ 就可以得到秘密信息 m_i。至此，通信完成。

注 1　为了方便理解协议内容，图 1 给出了协议的部分通信过程。其中，X/I 表示对粒子执行 σ_x 或 I 操作，M 表示对粒子执行测量，OC 表示对粒子进行操作选择，S 表示 SIFT 操作，C 表示 CTRL 操作。

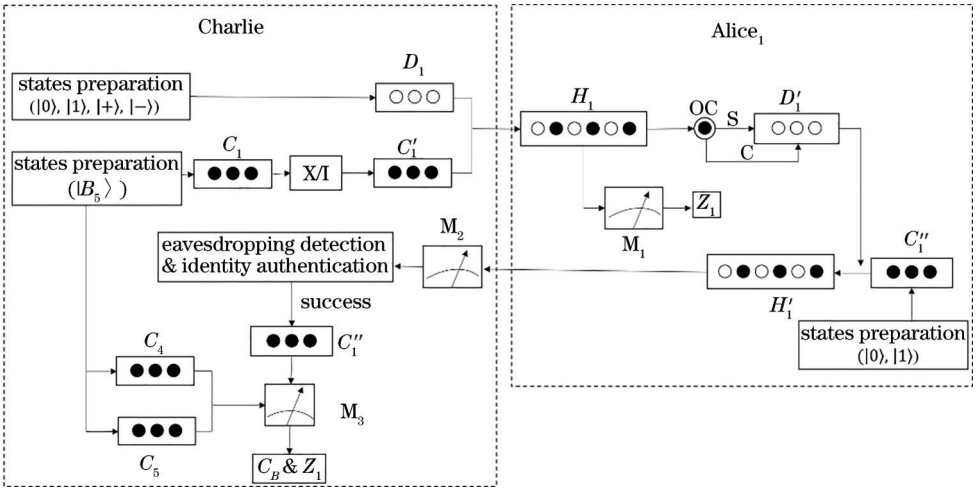

图 1　Charlie 与 Alice$_1$ 的通信框架图

Fig. 1　Framework diagram of communications between Charlie and Alice$_1$

注 2　利用广义的 Brown 态可将上述协议从四方推广到多方，其中参与方有 1 个量子方 Charlie 和 $(n+3)$ 个经典方 Alice$_i$（$i = 1, 2, \cdots, n+3$）。内容描述如下：

事先约定：身份密钥分别为 $K_c = \{K_c^1, K_c^2, \cdots, K_c^N\}$，$K_i = \{K_i^1, K_i^2, \cdots, K_i^N\}$。待传输的秘密信息分别为 $m_c = \{m_c^1, m_c^2, \cdots, m_c^N\}$，$m_i = \{m_i^1, m_i^2, \cdots, m_i^N\}$。同样地，身份密钥也只在量子方与经典方之间共享。协议中，步骤 2、3、5 与上述四方协议相同，其余步骤与上述协议类似。具体步骤 1、4 如下所示：

步骤 1　Charlie 制备 N 个广义 Brown 态 $|B_{n+5}\rangle$，并将这一系列量子态划分为 $(n+5)$ 个粒子序列 $C_s = \{q_s^1, q_s^2, \cdots, q_s^N\}(s = 1, 2, \cdots, n+5)$。然后，Charlie 根据秘密信息 m_c 的值对粒子序列 $C_i(i = 1, 2, \cdots, n+3)$ 进行加密得到 C_i'。规则如下：若 $m_c^j = 0$，则对 q_i^j 执行 I 操作；若 $m_c^j = 1$，则对 q_i^j 执行 σ_x 操作。接着，Charlie 随机制备一系列的单光子 $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ 组成检测粒子序列，并分别记为 $D_i = \{d_i^1, d_i^2, \cdots, d_i^N\}$。最后，根据 K_i 的值，Charlie 重组序列 C_i'，D_i 得到序列 H_i，并将其分

别发送给 Alice_i。

步骤 4　Charlie 对序列 C_{n+4}, C_{n+5} 中的粒子 q^j_{n+4} 和 q^j_{n+5} 执行 Bell 基测量，并将结果记为 C^j_B。然后利用 Z 基测量序列 C_i''，并记结果为 Z_i'。最后，Charlie 公布 Z_c 和 C_B 的结果，其中 $Z_c=\{(Z_1'^1, Z_2'^1, \cdots, Z'_{n+3}{}^1), (Z_1'^2, Z_2'^2, \cdots, Z'_{n+3}{}^2), \cdots, (Z_1'^N, Z_2'^N, \cdots, Z'_{n+3}{}^N)\}$，$Z_i'^N$ 为 Z_i' 中第 N 个粒子的值。

3　安全性分析

对于半量子对话协议来说，安全性分析至少包括信息泄露分析和能否抵抗常见攻击手段分析。因此以下将对信息泄露问题、截获重发攻击和中间人攻击等进行分析。

3.1　信息泄露

信息泄露是指外部窃听者 Eve 直接通过合法通信参与方在经典通信中公布的信息提取出部分秘密信息。本文协议中公开的经典信息包括窃听检测过程公布的检测粒子信息，编码粒子对应的 Bell 基测量的结果 C_B 和编码粒子 Z 基测量后的重组序列 Z_c。因为检测粒子信息和 C_B 不涉及秘密信息，Z_c 也不是直接测量结果，故 Eve 只能根据 C_B 和 Z_c 的结果来推测秘密信息。对于一个 $(n+4)$ 方的协议来说，Eve 能获得的信息组合有 $4\times 2^{n+3}=2^{n+5}$ 种，且这些情况等概率出现。例如，对于一个量子方和三个经典方来说，Eve 能获得的信息组合如表 1 所示，共有 $4\times 2^3=32$ 种。因此，本文所提协议的信息熵[27]为

$$-2^{n+5}\times\frac{1}{2^{n+5}}\log_2\frac{1}{2^{n+5}}=n+5, \tag{4}$$

而通信参与方要传输的秘密信息的总和为 $n+4$。因此，该半量子对话协议不存在信息泄露的问题。

表 1　Eve 可获得的信息组合

Table 1　Combination of information available to Eve

Z_c	C_B	Z_c	C_B	Z_c	C_B	Z_c	C_B
000	00	001	00	010	00	100	00
	01		01		01		01
	10		10		10		10
	11		11		11		11
011	00	101	00	110	00	111	00
	01		01		01		01
	10		10		10		10
	11		11		11		11

3.2　截获重发攻击

截获重发攻击是指 Eve 测量截获的粒子序列，并利用结果构造一个新的序列发给接收方，以此获取秘密信息。在步骤 1 中，Charlie 将序列 H_i 发送给 Alice_i，在步骤 2 中，Alice_i 将序列 H_i' 发送给 Charlie。在以上两个地方存在 Eve 进行截获重发攻击的可能。假设 Eve 对序列 H_1 进行截获，并用 Z 基测量该序列。由于 Eve 不知道 Alice_1 的身份密钥 K_1，无法分辨哪些是检测粒子，哪些是编码粒子。以粒子 $|+\rangle$ 为例，若 Eve 对该粒子进行 Z 基测量，这会使其坍缩到 $|0\rangle$ 或 $|1\rangle$，当 Alice_1 对该粒子选择 CTRL 操作时，Charlie 一定会发现 Eve 的窃听行为。所以 Eve 被发现的概率为

$$1-\left[\frac{1}{2}+\frac{1}{2}\times\left(\frac{1}{2}+\frac{1}{2}\times\frac{1}{2}\right)\right]^N=1-\left(\frac{7}{8}\right)^N。 \tag{5}$$

当 N 足够大时，Eve 的攻击一定会被检测到。

3.3　中间人攻击

中间人攻击即 Eve 在合法用户之间，通过截获粒子序列，模仿合法用户向其他用户发起对话，从而获取有用信息。假设 Eve 制备一系列 Brown 态并做相应的处理，并在截取 Charlie 发送的序列 H_i 后，将自己手中的序列发给 Alice_i。由于 Eve 不知道参与方的身份密钥 K_c、K_i，无法知晓粒子的正确排列，故无法从 Alice_i 传回的序列中获得秘密信息。同时，Eve 在与 Charlie 的交流中，无法正确地重排粒子序列，这使得其攻击行为一定会被 Charlie 发现。

3.4　干扰攻击

Eve 通过执行酉变换对量子位进行恶意改变，使得接收方收到错误的信息。在本文协议中，由于 Eve 不知道参与方的身份密钥，其干扰无法准确地作用于编码粒子。假设在步骤 1 中，Charlie 将序列 H_1 发送给 Alice_1，Eve 执行 σ_x 操作于检测粒子，那么会对 $|0\rangle$、$|1\rangle$ 造成影响。由表 2 可知，此时 Eve 的干扰行为会被 Charlie 发现。因此，Eve 被发现的概率为

$$1-\left(\frac{1}{2}+\frac{1}{2}\times\frac{1}{2}\right)^N=1-\left(\frac{3}{4}\right)^N。 \tag{6}$$

当 N 足够大时，Eve 的攻击一定会被检测到。

表 2　检测粒子的测量结果

Table 2　Detection of particle measurement results

D_1	C_B	C_{D_1}	C'_{D_1}
$\|0\rangle$	CTRL	—	1
	SIFT	1	1
$\|1\rangle$	CTRL	—	0
	SIFT	0	0

3.5　特洛伊木马攻击

不同于上述攻击手段，Eve并不从通信方交换的量子比特中获取信息。量子特洛伊木马攻击是指Eve在量子信号中插入间谍光子，从而进入合法用户的设备，以此获取有用信息。在双向的量子通信协议中，常见的量子特洛伊木马攻击一般有延迟光子攻击和不可见光子攻击[28]。幸运的是，木马攻击是可以通过技术措施来防范的[29]。因此，通过放置波长滤波器和光子数分离器，所提协议就可避免特洛伊木马攻击。

4　效率分析

量子通信协议的效率计算公式为[30]

$$\eta_1=\frac{m}{q+b},\tag{7}$$

式中：m表示传输秘密信息的经典比特总数；q表示通信过程中传递的量子比特总数；b表示通信过程中所交换的经典比特总数。为了实现四方互相发送N个经典比特的信息，量子方需要向一个经典方发送$2N$个量子比特，一个经典方需要向量子方发送$3N/2$个量子比特。忽略窃听检测所需的经典比特，量子方还需要向所有经典方公布$5N$个经典比特。容易得到$m=8N$，$q=(2N+3N/2)\times 3=10.5N$，$b=5N$，计算可得

$$\eta_1=\frac{8N}{10.5N+5N}=\frac{16}{31}\approx 51.6\%。\tag{8}$$

所提协议通过引入身份认证，实现了在窃听检测完成的时候，经典方与量子方之间的身份合法认证。一般来说，将身份认证加入通信协议后，会使用更多的量子资源，但本文将身份认证与窃听检测同时进行，节约了量子资源。如表3所示，将所提协议与现行其他几个半量子对话协议进行比较可以看出，该协议在保障安全性的同时，具有较高的量子通信效率。

表3　几个半量子对话协议的比较

Table 3　Comparison of several semi-quantum dialogue protocols

Protocol	Quantum user	Classical user	Quantum states used	η_1	Authenticated
Ref. [18]	Alice	Bob	Bell states	20%	No
Ref. [21]	Charlie	Alice and Bob	Logical qubits	12.5%	Yes
Ref. [22]	Charlie	Alice and Bob	Cluster states	50%	No
Ref. [23]	Alice	Charlie and Bob	GHZ states	50%	No
Ref. [19]	Alice	Bob	Single photon	28.6%	No
Proposed	Charlie	Alice_i ($i=1, 2, 3$)	Brown states	51.6%	Yes

对于多方的半量子对话来说，为了实现$(n+4)$方互相发送N个经典比特的信息，量子方需要向一个经典方发送$2N$个量子比特，一个经典方需要向量子方发送$3N/2$个量子比特。忽略窃听检测所需的经典比特，量子方还需要向所有经典方公布$2N+N(n+3)$个经典比特。容易得到$m=2N(n+4)$，$q=(7N/2)(n+3)$，$b=2N+N(n+3)$，计算可得

$$\eta_2=\frac{2N(n+4)}{(7N/2)(n+3)+2N+N(n+3)}=\frac{4n+16}{9n+31}。\tag{9}$$

特别是，当$n\to+\infty$时，$\eta_2\to\frac{4}{9}\approx 44.4\%$；当$n=0$时，即当利用5粒子Brown态完成半量子对话时，$\eta_2=\frac{16}{31}\approx 51.6\%=\eta_1$。

5　结　　论

提出了一个基于Brown态的四方认证半量子对话协议，其中四方包括一个量子方和三个经典方。通信中，量子方与经典方完成相互的身份认证后，四方分别将自己待传输的秘密信息安全直接地传给另外三方，完成量子对话。对协议的安全性分析表明，所提协议不存在信息泄露问题，且可以抵抗截获重发攻击、中间人攻击、干扰攻击和特洛伊木马攻击。与其他半量子对话协议相比，所提协议具有身份认证功能，且有较高的量子通信效率。此外，通过广义的Brown态，所提协议可推广到多方，在实际应用中有一定的价值。

参　考　文　献

[1] 邓富国, 李熙涵, 龙桂鲁. 量子安全直接通信[J]. 北京师范大学学报(自然科学版), 2016, 52(6): 790-799.
Deng F G, Li X H, Long G L. Quantum secure direct

communication[J]. Journal of Beijing Normal University (Natural Science), 2016, 52(6): 790-799.

[2] Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing[J]. Theoretical Computer Science, 2014, 560: 7-11.

[3] Wang X B. Quantum key distribution with two-qubit quantum codes[J]. Physical Review Letters, 2004, 92(7): 077902.

[4] Bienfang J C, Gross A J, Mink A, et al. Quantum key distribution with 1.25 Gbps clock synchronization [J]. Optics Express, 2004, 12(9): 2011-2016.

[5] 何业锋, 李春雨, 郭佳瑞, 等. 基于标记配对相干态的被动测量设备无关量子密钥分配[J]. 中国激光, 2020, 47(9): 0912002.
He Y F, Li C Y, Guo J R, et al. Passive measurement-device-independent quantum key distribution based on heralded pair coherent states[J]. Chinese Journal of Lasers, 2020, 47(9): 0912002.

[6] 孙游东, 邢永鑫, 王天一. 基于离散调制的三态连续变量量子密钥分发协议的安全性分析[J]. 激光与光电子学进展, 2021, 58(7): 0727004.
Sun Y D, Xing Y X, Wang T Y. Security analysis of three-state continuous variable quantum key distribution protocol based on discrete modulation[J]. Laser & Optoelectronics Progress, 2021, 58(7): 0727004.

[7] 武天雄, 李云霞, 蒙文, 等. 基于部分记忆信道的量子隐形传态保真度增强方法研究[J]. 激光与光电子学进展, 2021, 58(5): 0527001.
Wu T X, Li Y X, Meng W, et al. Enhancement of quantum teleportation fidelity based on partial memory channel[J]. Laser & Optoelectronics Progress, 2021, 58(5): 0527001.

[8] Bouwmeester D, Pan J W, Mattle K, et al. Experimental quantum teleportation[J]. Nature, 1997, 390(6660): 575-579.

[9] Fattal D, Diamanti E, Inoue K, et al. Quantum teleportation with a quantum dot single photon source [J]. Physical Review Letters, 2004, 92(3): 037904.

[10] Podoshvedov S A. Quantum teleportation of entanglement using four-particle entangled states[J]. Journal of Experimental and Theoretical Physics Letters, 2005, 81(4): 195-197.

[11] Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme[J]. Physical Review A, 2002, 65(3): 032302.

[12] Boström K, Felbinger T. Deterministic secure direct communication using entanglement[J]. Physical Review Letters, 2002, 89(18): 187902.

[13] Deng F G, Long G L, Liu X S. A two-step quantum direct communication protocol using Einstein-Podolsky-Rosen pair block[J]. Physical Review A, 2003, 68(4): 042317.

[14] Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob[J]. Physical Review Letters, 2007, 99(14): 140501.

[15] Yu K F, Yang C W, Liao C H, et al. Authenticated semi-quantum key distribution protocol using Bell states[J]. Quantum Information Processing, 2014, 13 (6): 1457-1465.

[16] Li C M, Yu K F, Kao S H, et al. Authenticated semi-quantum key distributions without classical channel[J]. Quantum Information Processing, 2016, 15(7): 2881-2893.

[17] Yin A H, Wang Z F, Fu F B. A novel semi-quantum secret sharing scheme based on Bell states [J]. Modern Physics Letters B, 2017, 31(13): 1750150.

[18] Shukla C, Thapliyal K, Pathak A. Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue[J]. Quantum Information Processing, 2017, 16(12): 295.

[19] Ye T Y, Ye C Q. Semi-quantum dialogue based on single photons[J]. International Journal of Theoretical Physics, 2018, 57(5): 1440-1454.

[20] Pan H M. Semi-quantum dialogue with bell entangled states[J]. International Journal of Theoretical Physics, 2020, 59(5): 1364-1371.

[21] Liu L, Xiao M, Song X L. Authenticated semi quantum dialogue with secure delegated quantum computation over a collective noise channel[J]. Quantum Information Processing, 2018, 17(12): 342.

[22] Xu L Y, Chen H Y, Zhou N R, et al. Multi-party semi-quantum secure direct communication protocol with cluster states[J]. International Journal of Theoretical Physics, 2020, 59(7): 2175-2186.

[23] Zhou R G, Zhang X X, Li F X. Three-party semi-quantum protocol for deterministic secure quantum dialogue based on GHZ states[J]. Quantum Information Processing, 2021, 20(4): 153.

[24] Brown I D K, Stepney S, Sudbery A, et al. Searching for highly entangled multi-qubit states[J]. Journal of Physics A: Mathematical and General, 2005, 38(5): 1119-1131.

[25] Muralidharan S, Panigrahi P K. Perfect teleportation, quantum state sharing and superdense coding through a genuinely entangled five-qubit state[J]. Physical Review A, 2008, 77(3): 032321.

[26] Chang L W, Zhang Y Q, Tian X X, et al. Fault tolerant controlled quantum dialogue with logical brown states against collective noise[J]. International Journal of Theoretical Physics, 2020, 59(7): 2155-2174.

[27] Shannon C E. Communication theory of secrecy systems[J]. The Bell System Technical Journal, 1949, 28(4): 656-715.

[28] Cai Q Y. Eavesdropping on the two-way quantum communication protocols with invisible photons[J]. Physics Letters A, 2006, 351(1/2): 23-25.

[29] Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography[J]. Reviews of Modern Physics, 2002, 74(1): 145-195.

[30] Wen X J, Zhao X Q, Gong L H, et al. A semi-quantum authentication protocol for message and identity[J]. Laser Physics Letters, 2019, 16(7): 075206.