光学学报

基于贝尔态的两方互认证半量子密钥协商协议

何业锋，梁熙媛*，蔡明月
西安邮电大学网络空间安全学院，陕西 西安 710121

摘要 针对已有量子密钥协商协议存在或对参与者能力和设备要求过高，或易受中间人攻击的问题，利用贝尔态的纠缠特性、置换和幺正操作提出了一种具有互认证功能的两方半量子密钥协商协议。协议仅需一方参与者具备全量子能力，而另一方只需具备半量子能力。由于半量子参与方仅需进行反射操作以及简单的量子态制备与测量操作，因此该协议降低了对参与者量子能力与设备的要求。并且所提协议通过执行参与者之间的身份互认证以防止中间人攻击。安全性分析证明了该协议能够有效抵御参与者攻击和外部攻击。此外，综合考量所提协议的功能并分析其性能，并与已有量子密钥协商协议进行对比，可以说明所提协议在性能方面具有一定优势。

关键词 量子光学；量子密码；半量子密钥协商；身份互认证；贝尔态
中图分类号 TN918 **文献标志码** A **DOI**：10.3788/AOS231780

1 引 言

量子密码以量子态为信息载体，通过量子信道在已授权的用户间进行信息传递。量子密码学与传统密码学不同，前者的安全性是由量子力学基本原理来保证的，因此理论上它是无条件安全的。因此，量子密码受到了众多从事密码学研究工作者的广泛关注，并逐渐发展成密码学领域的一个热点方向。目前，量子密码的研究主要概括为以下几个方向：量子密钥分发(QKD)[1-4]、量子密钥协商(QKA)[5-8]、量子秘密共享(QSS)[9-10]、量子安全直接通信(QSDC)[11-13]以及量子私有比较(QPC)[14]等。QKA作为量子密码的重要研究方向之一，它能够让所有参与方通过安全的量子信道共同协商出一个会话密钥，并且每个参与方对协商出的密钥的贡献是相等的。

自2004年Zhou等[5]提出QKA协议以来，相继出现许多不同的QKA协议[15-20]。这些协议利用单粒子量子态或多粒子量子态实现了两方或多方参与者之间共享密钥的公平协商。除此之外，还有一些研究者专注于提高协议抗集体噪声[18,20]的性能。然而在实际应用中，由于费用昂贵且资源稀缺，绝大多数参与方难以拥有性能良好的量子设备。因此，为了便于协议的实现，需要简化参与方的量子操作。针对这个问题，文献[21]基于贝尔(Bell)态提出了一种两方的半量子密钥协商(SQKA)协议。半量子密钥协商协议要求协议中的一个参与方具有完全的量子能力，其余参与方只具有半量子能力，且半量子方只能进行两种操作：反射操作，对接收到的粒子不进行任何操作，直接返回收到的粒子；测量操作，对接收到的粒子实施Z基测量，并根据测量结果制备新的粒子。2022年，文献[22]基于G-like态提出了一种两方半量子密钥协商协议，该协议的实现需要可信第三方的帮助。同年，文献[23]基于多粒子GHZ(Greenberger-Horne-Zeilinger)纠缠态提出了一种多方半量子密钥协商协议，该协议不需要参与方之间预先共享密钥，也不需要幺正操作或量子纠缠交换就能实现密钥协商，降低了对参与者的能力和设备要求。2023年，文献[24]提出了一种基于四粒子cluster态的四方半量子密钥协商协议。相较于其他协议，该协议的量子比特效率偏低。另一方面，由于参与者在进行密钥协商的过程中可能会受到中间人等攻击，所以在进行密钥协商前，对参与者进行身份认证是非常必要的。近年来，研究者们也提出了一些具有互认证功能的QKA协议[6-7,25]。2022年，文献[6]提出了一种基于Bell态的双向认证QKA协议，该协议利用Bell态的测量相关性相互认证对方的身份，利用Bell态的纠缠交换关系公平地协商会话密钥。而文献[7]基于单粒子态和四粒子GHZ态，提出了一种相互认证的QKA协议。该协议利用共享身份信息的哈希值和随机数进行身份认证，利用四粒子GHZ态的测量关联特性进行共享密钥的协商。在实际应用场景中，

收稿日期：2023-11-10；**修回日期**：2023-12-24；**录用日期**：2023-12-29；**网络首发日期**：2024-01-09
基金项目：国家自然科学基金(61802302)、陕西省自然科学基础研究计划项目(2021JM-462)
通信作者：*xiyuaner2000@163.com

为了便于协议的实现，需要设计对参与者能力和设备要求较低的半量子密钥协商协议；为了防止外部攻击者假冒已授权用户窃取共享密钥，协议需具有互认证功能。因此，设计具有互认证功能的半量子密钥协商协议是非常必要的。

本文基于Bell态，提出了一种具有互认证功能的两方半量子密钥协商协议。其中Alice是全量子方，Bob是半量子方。双方通过制备和测量身份信息粒子，实现身份的互认证；并且利用Bell态的纠缠特性，实现共享密钥的协商。相较于其他纠缠态，本协议用到的Bell态更容易制备，而且协议仅使用Z基测量和Bell测量这两种量子测量操作，在现有技术上也更容易实现。此外，证明所提方案能够有效抵抗参与者攻击和外部攻击，且在性能方面也有一定的优势。

2　新的两方互认证半量子密钥协商协议

2.1　Bell态和幺正变换

Bell态是两粒子最大纠缠态。四个Bell态构成了Hilbert空间的一组正交基，即$\left|\Phi^{\pm}\right\rangle=\left(\left|00\right\rangle\pm\left|11\right\rangle\right)/\sqrt{2}$，$\left|\Psi^{\pm}\right\rangle=\left(\left|01\right\rangle\pm\left|10\right\rangle\right)/\sqrt{2}$。常用的两个量子幺正操作$I$和$X$具体表达式为$I=\left|0\right\rangle\left\langle 0\right|+\left|1\right\rangle\left\langle 1\right|$，$X=\left|0\right\rangle\left\langle 1\right|+\left|1\right\rangle\left\langle 0\right|$。若对单量子态执行幺正操作$I$或$X$，则变换结果分别为$I\left|0\right\rangle=\left|0\right\rangle$，$I\left|1\right\rangle=\left|1\right\rangle$，$X\left|0\right\rangle=\left|1\right\rangle$，$X\left|1\right\rangle=\left|0\right\rangle$。可以用量子电路来实现Bell态的制备和测量[26]，具体过程如图1所示，其中q_0、q_1为输入的量子比特，c'为输出的经典比特。H和X分别表示量子逻辑门Hadamard门和Pauli-X门。

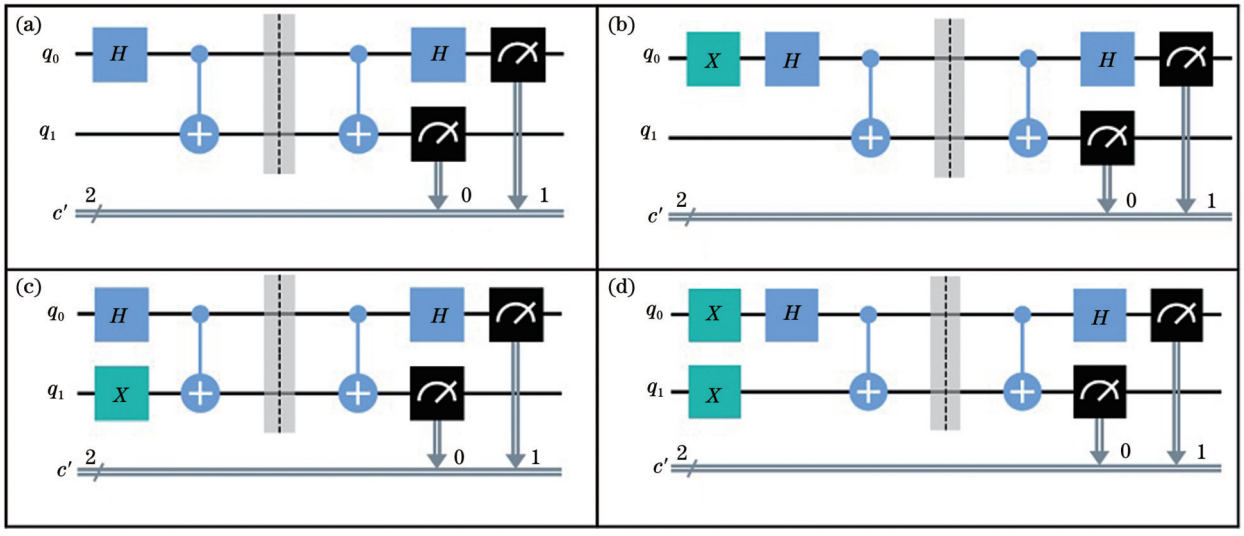

图1　制备和测量Bell态的量子电路图。(a)$\left|\Phi^{+}\right\rangle$；(b)$\left|\Phi^{-}\right\rangle$；(c)$\left|\Psi^{+}\right\rangle$；(d)$\left|\Psi^{-}\right\rangle$

Fig. 1　Quantum circuit diagrams of preparing and measuring Bell state.(a)$\left|\Phi^{+}\right\rangle$; (b)$\left|\Phi^{-}\right\rangle$; (c)$\left|\Psi^{+}\right\rangle$; (d)$\left|\Psi^{-}\right\rangle$

2.2　新的两方互认证半量子密钥协商协议

假设全量子方Alice和半量子方Bob想要协商出一个共享密钥，需要先对彼此的身份进行认证，身份认证通过后，Alice和Bob再进行密钥协商。

假定Alice和Bob在此之前已经秘密地共享了一对身份信息序列$R_{\mathrm{A}}=R_{\mathrm{A},1}R_{\mathrm{A},2}\cdots R_{\mathrm{A},n}$和$R_{\mathrm{B}}=R_{\mathrm{B},1}R_{\mathrm{B},2}\cdots R_{\mathrm{B},n}$，其中$R_{\mathrm{A},i}$，$R_{\mathrm{B},i}\in\{0,1\}$，且$i\in\{1,2,\cdots,n\}$。在协议开始前，Alice和Bob随机生成私钥$K_{\mathrm{A}}=\{K_{\mathrm{A},1},K_{\mathrm{A},2},\cdots,K_{\mathrm{A},n}\}$和$K_{\mathrm{B}}=\{K_{\mathrm{B},1},K_{\mathrm{B},2},\cdots,K_{\mathrm{B},n}\}$，其中$K_{\mathrm{A},i}$，$K_{\mathrm{B},i}\in\{0,1\}$，且$i\in\{1,2,\cdots,n\}$。协议的具体步骤如下：

1) Alice根据身份信息序列R_{A}制备对应的量子粒子序列$r_{\mathrm{A}}=r_{\mathrm{A},1}r_{\mathrm{A},2}\ldots r_{\mathrm{A},n}$，其中当$R_{\mathrm{A},i}=0$时，$r_{\mathrm{A},i}$被制备为$\left|0\right\rangle$态，当$R_{\mathrm{A},i}=1$时，$r_{\mathrm{A},i}$被制备为$\left|1\right\rangle$态。同样地，Bob也根据其身份信息序列$R_{\mathrm{B}}$制备其量子粒子序列$r_{\mathrm{B}}=r_{\mathrm{B},1}r_{\mathrm{B},2}\ldots r_{\mathrm{B},n}$。

2) Alice从集合$\left\{\left|\Phi^{+}\right\rangle,\left|\Phi^{-}\right\rangle,\left|\Psi^{+}\right\rangle,\left|\Psi^{-}\right\rangle\right\}$中随机选取$6n$个Bell态，形成一个Bell态序列。接下来，Alice将这个Bell态序列分为序列S_{A}和S_{B}，其中S_{A}由Bell态序列中的所有1粒子组成，S_{B}由Bell态序列中的所有2粒子组成。再选择一个置换算子$\Pi_{\mathrm{A},n}$来重排序列r_{A}，得到r_{A}^{*}。最后，Alice将序列r_{A}^{*}随机插入到序列S_{B}中，形成新序列记作S_{B}^{*}，Alice将其通过量子信道发送给Bob，并保留S_{A}。

3) Bob收到序列S_{B}^{*}后，Alice通过安全的经典信道公布r_{A}^{*}的位置。随后，Bob还原出序列S_{B}和r_{A}^{*}，对r_{A}^{*}中所有粒子进行Z基测量，并根据步骤1)将测量结果解码为二进制序列$R_{\mathrm{A}}^{*'}$。再对S_{B}中粒子执行以下操作：i)随机选择$2n$个粒子进行

反射操作；ii）对剩余 $4n$ 个粒子进行 Z 基测量，并记录测量结果。

Bob 选择一个置换算子 $\Pi_{B,n}$ 来重排序列 r_B 得到 r_B^*，再将序列 r_B^* 中的 n 个粒子以及 $2n$ 个反射粒子随机组合得到新序列 $S_B^{*'}$。随后，Bob 将序列 $S_B^{*'}$ 通过量子信道发送给 Alice。

4）当 Alice 收到 Bob 发来的 $S_B^{*'}$ 后，Bob 通过经典信道公布执行了反射操作的粒子位置（在序列 S_B 中的位置）以及 r_B^* 的位置。按照 Bob 公布的信息，Alice 还原出序列 r_B^*，并对 r_B^* 中所有粒子进行 Z 基测量，根据步骤 1）将测量结果解码为二进制序列 $R_B^{*'}$。然后，Alice 在序列 S_A 中选择同一位置粒子，与收到的反射粒子一同实行 Bell 测量（BM）。得到的测量结果与该位置的初始 Bell 态进行比较，计算错误率。若错误率低于事先约定的阈值，则认为量子信道是安全的，协议继续，否则，协议终止并回到步骤 1）。

5）当信道通过窃听检测后，Alice（Bob）通过经典信道公布置换算子 $\Pi_{A,n}$（$\Pi_{B,n}$），根据置换算子 $\Pi_{A,n}$（$\Pi_{B,n}$）和 $R_A^{*'}$（$R_B^{*'}$），Bob（Alice）可以得到 R_A'（R_B'），然后将序列 R_A'（R_B'）和 R_A（R_B）进行对比，来判断 Alice（Bob）的身份。若错误率低于事先约定的阈值[15]（根据通信双方的安全需求及实际通信设备的情况选择合适的阈值），则成功认证 Alice（Bob）的身份。若相互身份认证成功，协议继续，否则协议终止。

6）双方身份认证通过后，序列 S_A 中的 $2n$ 个粒子和 S_B 中对应位置的 $2n$ 个粒子已经被用来进行信道检测和身份认证。Alice 将剩余的 $4n$ 个粒子组成序列 S_A'，Bob 根据步骤 3）中操作 ii）所记录的测量结果制备 $4n$ 个状态与测量结果相同的新粒子，记作序列 S_B'。Alice 在 S_A' 中选择前 $2n$ 个粒子，随机选择其中 n 个粒子按照以下规则组成序列 S_{A1}'：当 $K_{A,i}=0$ 时，Alice 对第 i 个粒子执行幺正操作 I；当 $K_{A,i}=1$ 时，Alice 对第 i 个粒子执行幺正操作 X。然后，再将剩下 n 个粒子组成窃听粒子序列记作 S_{A2}'。随后，Alice 根据和 Bob 的共享身份信息 R_A 和 R_B，将序列 S_{A1}' 和 S_{A2}' 重新组合成序列 S_{A12}'，具体组合规则如下：当 $R_{AB,i}=0$ 时，将 $S_{A1,i}'$ 放在 $S_{A2,i}'$ 前；当 $R_{AB,i}=1$ 时，将 $S_{A1,i}'$ 放在 $S_{A2,i}'$ 后。其中，$R_{AB}=R_A\oplus R_B$（$\oplus$ 表示异或运算）。最后，Alice 将组合序列 S_{A12}' 通过量子信道发送给 Bob。

与此同时，Bob 在 S_B' 中选择后 $2n$ 个粒子，根据相同的规则制备粒子序列 S_{B1}'、S_{B2}' 和 S_{B12}'，Bob 将组合序列 S_{B12}' 通过量子信道发送给 Alice。此时，所有需要通过量子信道来传输的粒子已传输结束，由于粒子在量子信道中被多次传输，因此 Alice 和 Bob 两端都需要安装波长量子滤波器以及光子数分离器来避免特洛伊木马攻击。

7）Bob 收到 S_{A12}' 后，根据 R_{AB} 可知 S_{A1}' 和 S_{A2}' 的正确顺序，由此还原出序列 S_{A1}' 和 S_{A2}'。此时，Alice 通过经典信道公布 S_{A1}' 和 S_{A2}' 中每个粒子在原序列 S_A 中对应的位置，以及对应的初始 Bell 态。Bob 对序列 S_{A1}' 和 S_{A2}' 进行 Z 基测量。并将序列 S_{A2}' 的测量结果和 S_B' 中对应位置粒子的测量结果与 Alice 公布的相应初始 Bell 态进行比较，计算错误率。具体描述为：若 Alice 制备的粒子状态为 $|\Phi^{\pm}\rangle$（$|\Psi^{\pm}\rangle$），则 Bob 对 S_{A2}' 和对应位置的 S_B' 中粒子的测量结果应为 $|00\rangle$ 或 $|11\rangle$（$|10\rangle$ 或 $|01\rangle$）。

同样地，Alice 收到 S_{B12}' 后，可还原出序列 S_{B1}' 和 S_{B2}'。根据 Bob 公布的 S_{B1}'、S_{B2}' 的位置，Alice 对序列 S_{B1}'、S_{B2}' 进行 Z 基测量，将序列 S_{B2}' 的测量结果和 S_A' 中对应位置粒子的测量结果与初始 Bell 态进行比较，计算错误率。

如果 Alice 和 Bob 计算的错误率都低于事先约定的阈值，则认为量子信道是安全的，协议继续，否则，协议终止。

8）Bob 将 S_{A1}' 与 S_B' 中对应位置粒子的测量结果，同 Alice 公布的初始 Bell 态进行比较，就可以得到 K_A 的值。Alice 通过同样的方法可得出 K_B 的值。具体方法见表 1，当初态为 $|\Phi^{\pm}\rangle$ 时，1、2 粒子状态相同；当初态为 $|\Psi^{\pm}\rangle$ 时，1、2 粒子状态相反。最后，Alice 和 Bob 可以计算出最终的共享密钥 $K=K_A\oplus K_B$。整个协议的量子态传输过程如图 2 所示。

表 1 Bob 获取 Alice 的密钥 K_A 的过程

Table 1 Process of Bob obtaining Alice's key K_A

Initial Bell state	$S_{A1,i}'$	Particle state in S_A'	Particle state in S_B'	$K_{A,i}$	Unitary operation
$\|\Phi^{\pm}\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	0	I
	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	1	X
	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	1	X
	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	0	I
$\|\Psi^{\pm}\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	1	X
	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	0	I
	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	0	I
	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	1	X

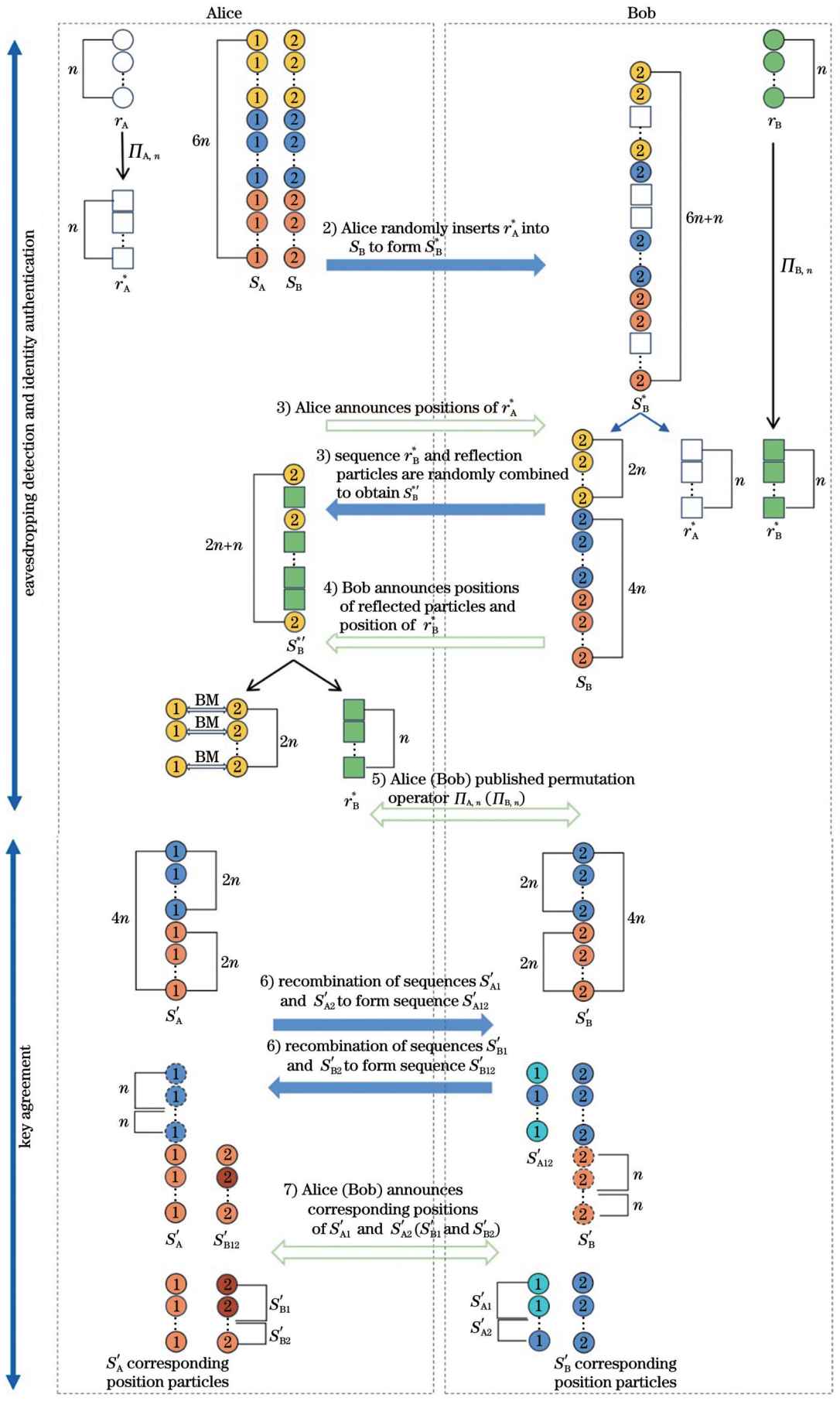

图 2　量子态传输原理图

Fig. 2　Schematic diagram of quantum-state transmission

3 分析与讨论

3.1 安全性分析

互认证半量子密钥协商协议的安全性分析不仅要考虑密钥协商过程的安全性，还需要考虑身份认证过程是否安全。对于密钥协商过程，需要考虑参与者攻击和外部攻击。而身份认证过程中没有参与者攻击[6-7]，所以只需要分析外部攻击。下面将从参与者攻击和外部攻击这两个方面对协议的安全性进行分析。

3.1.1 参与者攻击

假设Bob是不诚实的参与者，Bob在与Alice完成身份认证后，想独自决定最后的共享密钥$K=K_A\oplus K_B$，那么Bob需要在发送含有K_B信息的粒子序列S'_{B12}前就取得K_A。然而，Alice是在收到S'_{B12}后才将S'_{A1}中粒子对应的位置发送给Bob的，所以Bob无法独自决定该共享密钥。同理，Alice也不能独自决定密钥的生成。

3.1.2 外部攻击

本协议在步骤2)传输序列S_B^*；在步骤3)传输序列$S_B^{*'}$；在步骤6)传输序列S'_{A12}和S'_{B12}。假设攻击者Eve想要窃取最终的会话密钥，那么他只能通过对步骤2)、3)、6)实施如下攻击以达到目的。

针对身份认证的攻击：假设攻击者Eve想假冒Alice的身份与Bob通信，鉴于Eve不知道Alice的身份信息序列R_A，所以需要在步骤1)中随机制备粒子序列$r'_A=r'_{A,1}r'_{A,2}r'_{A,3}\cdots r'_{A,n}$代替Alice的身份粒子序列$r_A$，序列$r'_A$中的粒子在集合$\left\{|0\rangle,|1\rangle\right\}$中选择。然而在步骤5)中Bob对Alice进行身份认证时，Bob测量r'_A得到的结果显然与Alice的身份信息序列R_A不相关。假设Alice的身份信息$R_{A,i}=0$，当$r'_{A,i}=|0\rangle$时，Bob进行Z基测量后将结果编码得到0；当$r'_{A,i}=|1\rangle$时，Bob进行Z基测量后将结果编码得到1。那么Eve伪装成功的概率就为1/2。当R_A长度为n时，Eve伪装成功的概率就为$(1/2)^n$。当n无穷大时，Eve伪装成功的概率无限趋近于0。同理，当Eve想假冒Bob的身份时，成功的概率也趋近于0。

特洛伊木马攻击：在本协议中，信息粒子在量子信道中传输了3次，为了防止受到两种特洛伊木马攻击，本协议要求在Alice和Bob两端添加波长量子滤波器以及光子数分离器。

截获-重发攻击：以步骤1)中Eve截获Alice发送给Bob的序列S_B^*为例。Eve截获序列S_B^*后，随机制备$7n$个单粒子，代替序列S_B^*发送给Bob，其中单粒子在集合$\left\{|0\rangle,|1\rangle\right\}$中选择。由于Eve并不清楚哪些粒子被实行反射操作，所以会打破Bell态粒子间的纠缠特性，因此可在步骤4)中的窃听检测中发现Eve的攻击行为；然后以步骤6)中Eve截获Alice向Bob发送的序列S'_{A12}为例，由于Eve并不清楚Alice与Bob的共享身份信息R_{AB}，将无法还原出序列S'_{A1}和S'_{A2}并得到秘密信息K_A。且Eve的操作有一定概率会被Bob发现。因此本协议可以抵抗截获-重发攻击。

测量-重发攻击：以步骤1)中Eve在Alice向Bob发送的序列S_B^*上实施测量-重发攻击为例。Eve对序列S_B^*进行Z基测量，根据测量结果制备状态相同的粒子序列并发送给Bob。同理，由于Eve并不清楚被实行反射操作的是哪些粒子，所以其操作会打破粒子之间的纠缠特性。因此，Eve伪造的序列不可能通过窃听检测。接下来再以步骤6)中Eve截获Alice发送给Bob的序列S'_{A12}为例，由于Eve并不知道Alice与Bob的共享身份信息R_{AB}，所以无法还原出序列S'_{A1}和S'_{A2}并得到秘密信息K_A。因此本协议可以抵抗测量-重发攻击。

纠缠-测量攻击：以步骤1)中Eve准备对Alice发送给Bob的粒子实施纠缠-测量攻击为例。假设Eve准备用辅助态粒子$|E\rangle$对Bell态$|\Psi^+\rangle$(其余三种Bell态情况类似)中的2粒子执行纠缠操作U，形成一个三比特纠缠态，具体过程为

$$U|\Psi^+\rangle_{12}|E\rangle=\frac{1}{\sqrt{2}}\left[|0\rangle_1\left(a_0|0\rangle_2|e_0\rangle+b_0|1\rangle_2|e_1\rangle\right)\right]+\frac{1}{\sqrt{2}}\left[|1\rangle_1\left(c_0|0\rangle_2|e_2\rangle+d_0|1\rangle_2|e_3\rangle\right)\right],\quad(1)$$

式中：角标1、2分别表示Bell态中的第一、二个粒子。$|e_0\rangle$、$|e_1\rangle$、$|e_2\rangle$、$|e_3\rangle$是由纠缠操作U唯一确定的纯态，系数满足条件$a_0^2+b_0^2=1$、$c_0^2+d_0^2=1$。

随后，Eve立即将执行纠缠操作的粒子重新发送给Bob。如果Eve想要通过步骤4)的窃听检测，那么Eve执行U操作后，发送给Bob的粒子状态需要保持不变。因此，上述方程应满足$a_0=d_0=0$以及$b_0|e_1\rangle=c_0|e_2\rangle$，那么Eve不能区分状态为$|e_1\rangle$和$|e_2\rangle$的辅助态粒子，所以他无法获得有用的信息。假设$b_0|e_1\rangle=c_0|e_2\rangle=|e\rangle$，方程可化简为

$$U|\Psi^+\rangle_{12}|E\rangle=\frac{1}{\sqrt{2}}\left(b_0|0\rangle_1|1\rangle_2|e_1\rangle\right)+\frac{1}{\sqrt{2}}\left(c_0|1\rangle_1|0\rangle_2|e_2\rangle\right)=|\Psi^+\rangle_{12}|e\rangle,\quad(2)$$

Bell态的坍缩结果与辅助态粒子$|E\rangle$无关。相反地，如果纠缠操作U不满足$b_0|e_1\rangle=c_0|e_2\rangle$，那么Eve将会在步骤4)的安全性检测中被发现。

同样地，假设Eve对步骤6)S'_{A12}中的粒子执行纠缠操作U，形成双粒子纠缠态：$U|0\rangle|E\rangle=a_0|0\rangle|e_0\rangle+b_0|1\rangle|e_1\rangle$，$U|1\rangle|E\rangle=c_0|0\rangle|e_2\rangle+d_0|1\rangle|e_3\rangle$。根据上述分析，此式也应满足同样条件：$b_0=c_0=0$和$a_0|e_0\rangle=d_0|e_3\rangle=|e\rangle$，方程可化简为$U|0\rangle|E\rangle=|0\rangle|e\rangle$，$U|1\rangle|E\rangle=|1\rangle|e\rangle$。Eve不能区分状态为$|e_0\rangle$

和$|e_3\rangle$的辅助态粒子，且不知道Alice与Bob的共享身份信息R_{AB}，所以无法得到任何有用的秘密信息。因此本协议可以抵抗纠缠-测量攻击。

3.2 性能分析

目前，QKA协议的性能主要用Cabello量子比特效率[27]来衡量。Cabello量子比特效率定义为$\eta=c/(q+b)$，其中c表示协商出的共享密钥的比特长度，q表示协议中用到的量子比特总数，b表示交换的经典比特数。

在本协议中，共享密钥的比特长度$c=n$；Alice制备Bell态的数量为$6n$，身份信息粒子的比特数量为$2n$，Bob制备新粒子的数量为$4n$，因此$q=6n\times2+2n+4n=18n$；置换算子$\Pi_{A,n}$和$\Pi_{B,n}$的比特数量各为n，因此$b=2n$。所以本协议的量子比特效率$\eta=n/(18n+2n)=5\%$。与已有QKA协议性能进行比较，结果如表2所示。从表2可以看出，已有的QKA协议只具备单一特性，而本协议既允许半量子方参与以降低对参与者量子能力和量子设备的要求，又能实现参与者之间身份的互认证。然而QKA协议同时满足的特性越多，它所消耗的粒子数量越多，其量子比特效率必然下降。但本协议的量子比特效率为5%，与文献[22]、文献[24]所提协议相比，本协议在量子比特效率方面还有所改善。

需要指出的是，用Cabello量子比特效率来评判QKA协议性能的本质，是依据参与者共同协商出一个比特的共享密钥时所消耗经典比特和量子比特的数量。然而在实际应用中，效率可能会受到一些非理想因素（如Bell态测量产生的损耗、信道损耗、量子比特保真度降低等）的影响。因此，在实际使用中可以借鉴关于测量设备无关的QKD协议[28]中的结果进一步优化本协议。

表2　所提SQKA协议与已有QKA协议的比较

Table 2　Comparison between proposed SQKA protocol and existing QKA protocols

Protocol	Quantum resource	Mutual authentication function	Semi-quantum property	Qubit efficiency /%
He's protocol[6]	Bell state	√	×	16.67
He's protocol[7]	Single-particle state and four-particle GHZ state	√	×	53.33
He's protocol[22]	G-like state	×	√	4.50
He's protocol[24]	Cluster state	×	√	1.60
Yan's protocol[29]	Bell state	×	√	6.70
Zhu's protocol[30]	GHZ-like state	√	×	25.00
Ma's protocol[31]	Five-qubit genuinely entangled state	√	×	7.70
Our protocol	Bell state	√	√	5.00

4 结　论

提出了一个基于Bell态的两方互认证半量子密钥协商协议。该协议不仅确保全量子方Alice与半量子方Bob之间可以公平地协商共享密钥，更重要的是，在密钥协商前双方对彼此的身份进行认证，以抵御外部攻击者冒充合法用户窃取共享密钥。安全性分析表明所提SQKA协议可以很好地抵抗参与者攻击和外部攻击。最后，将本协议与已有的QKA协议相比较，发现本协议不仅在功能方面有一定优势，在量子比特效率方面也有所改善。利用Cabello量子比特效率对QKA协议进行分析，但该评价准则适用于理想环境。在实际使用协议时，效率会受光源、信道和探测器设备等因素的影响，而不能够达到理想要求，针对此问题后续将进一步优化SQKA协议。

参　考　文　献

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

[2] 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.

[3] He Y F, Ma W P. Measurement-device-independent quantum key distribution protocols against collective noise[J]. Modern Physics Letters B, 2021, 35(11): 2150195.

[4] He Y F, Ma W P. The decoy-state measurement-device-independent quantum key distribution with heralded single-photon source[J]. International Journal of Theoretical Physics, 2020, 59(3): 908-917.

[5] Zhou N, Zeng G, Xiong J. Quantum key agreement protocol[J]. Electronics Letters, 2004, 40(18): 1149-1150.

[6] He Y F, Pang Y B, Di M. Mutual authentication quantum key agreement protocol based on Bell states[J]. Quantum Information Processing, 2022, 21(8): 290.

[7] He Y F, Yue Y R, Di M, et al. Two-party mutual authentication quantum key agreement protocol[J]. International Journal of Theoretical Physics, 2022, 61(5): 145.

[8] 何业锋, 李智, 杨梦玫. 基于四粒子团簇态的量子密钥协商协议[J]. 激光与光电子学进展, 2023, 60(21): 2127001.

He Y F, Li Z, Yang M M. Quantum key agreement protocol based on four-particle cluster states[J]. Laser & Optoelectronics Progress, 2023, 60(21): 2127001.
[9] Wu X D, Wang Y J, Huang D. Passive continuous-variable quantum secret sharing using a thermal source[J]. Physical Review A, 2020, 101(2): 022301.
[10] Liao Q, Liu H J, Zhu L J, et al. Quantum secret sharing using discretely modulated coherent states[J]. Physical Review A, 2021, 103(3): 032410.
[11] He Y F, Ma W P. Multiparty quantum secure direct communication immune to collective noise[J]. Quantum Information Processing, 2018, 18(1): 4.
[12] Long G L, Deng F G, Wang C, et al. Quantum secure direct communication and deterministic secure quantum communication [J]. Frontiers of Physics in China, 2007, 2(3): 251-272.
[13] 郭瀚, 李云霞, 魏家华, 等. 抗集体噪声的测量设备无关的量子安全直接通信[J]. 激光与光电子学进展, 2022, 59(17): 1727001.
Guo H, Li Y X, Wei J H, et al. Immune to collective noise measurement-device-independent quantum secure direct communications[J]. Laser & Optoelectronics Progress, 2022, 59 (17): 1727001.
[14] Liu B, Gao F, Jia H Y, et al. Efficient quantum private comparison employing single photons and collective detection[J]. Quantum Information Processing, 2013, 12(2): 887-897.
[15] He Y F, Ma W P. Quantum key agreement protocols with four-qubit cluster states[J]. Quantum Information Processing, 2015, 14(9): 3483-3498.
[16] Liu B, Gao F, Huang W, et al. Multiparty quantum key agreement with single particles[J]. Quantum Information Processing, 2013, 12(4): 1797-1805.
[17] Shen D S, Ma W P, Wang L L. Two-party quantum key agreement with four-qubit cluster states[J]. Quantum Information Processing, 2014, 13(10): 2313-2324.
[18] Huang W, Su Q, Wu X, et al. Quantum key agreement against collective decoherence[J]. International Journal of Theoretical Physics, 2014, 53(9): 2891-2901.
[19] Sun Z W, Yu J P, Wang P. Efficient multi-party quantum key agreement by cluster states[J]. Quantum Information Processing, 2016, 15(1): 373-384.
[20] He Y F, Ma W P. Two quantum key agreement protocols immune to collective noise[J]. International Journal of Theoretical Physics, 2017, 56(2): 328-338.
[21] 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.
[22] 何业锋, 庞一博, 狄曼, 等. 基于G-like态的两方半量子密钥协商协议[J]. 中国激光, 2022, 49(13): 1312001.
He Y F, Pang Y B, Di M, et al. Two-party semi-quantum key agreement protocol based on G-like states[J]. Chinese Journal of Lasers, 2022, 49(13): 1312001.
[23] Xu T J, Chen Y, Geng M J, et al. Single-state multi-party semiquantum key agreement protocol based on multi-particle GHZ entangled states[J]. Quantum Information Processing, 2022, 21(7): 266.
[24] 何业锋, 庞一博, 狄曼, 等. 基于四粒子cluster态的四方半量子密钥协商协议[J]. 光学学报, 2023, 43(20): 2027001.
He Y F, Pang Y B, Di M, et al. Four-party semi-quantum key agreement protocol based on four particle cluster states[J]. Acta Optica Sinica, 2023, 43(20): 2027001.
[25] Xu Y G, Wang C N, Cheng K F, et al. A novel three-party mutual authentication quantum key agreement protocol with GHZ states[J]. International Journal of Theoretical Physics, 2022, 61(10): 245.
[26] Cross A W. The IBM Q experience and QISKit open-source quantum computing software[C]//APS March Meeting 2018, March 5–9, 2018, Los Angeles, California. New York: Bulletin of the American Physical Society, 2018: L58.003.
[27] Cabello A. Quantum key distribution in the Holevo limit[J]. Physical Review Letters, 2000, 85(26): 5635-5638.
[28] 何业锋, 赵艳坤, 李春雨, 等. 标记配对相干态下有限探测器死时间的测量设备无关量子密钥分配[J]. 光学学报, 2020, 40 (24): 2427001.
He Y F, Zhao Y K, Li C Y, et al. Measurement-device-independent quantum key distribution of finite detector's dead time in heralded pair coherent state[J]. Acta Optica Sinica, 2020, 40(24): 2427001.
[29] Yan L L, Zhang S B, Chang Y, et al. Semi-quantum key agreement and private comparison protocols using bell states[J]. International Journal of Theoretical Physics, 2019, 58(11): 3852-3862.
[30] Zhu H F, Wang C N, Li Z X. Semi-honest three-party mutual authentication quantum key agreement protocol based on GHZ-like state[J]. International Journal of Theoretical Physics, 2021, 60(1): 293-303.
[31] Ma X Y, Hur J, Li Z X, et al. Quantum mutual authentication key agreement scheme using five-qubit entanglement towards different realm architecture[J]. International Journal of Theoretical Physics, 2021, 60(5): 1933-1948.

Two-Party Mutual Authentication Semi-Quantum Key Agreement Protocol Based on Bell State

He Yefeng, Liang Xiyuan*, Cai Mingyue

School of Cyberspace Security, Xi'an University of Posts & Telecommunications, Xi'an 710121, *Shaanxi, China*

Abstract

Objective Quantum cryptography uses quantum states as the carriers of information transmission and transmits information between authorized users through quantum channels. Different from that of traditional cryptography, the security of quantum cryptography is guaranteed by the basic principles of quantum mechanics. Therefore, it is theoretically unconditionally secure. In recent years, quantum cryptography has received extensive attention from many researchers

engaged in cryptography, and has gradually developed into a popular research direction in the field of cryptography. Specifically, the quantum key agreement is an important research topic in quantum cryptography. It enables all participants to jointly negotiate a session key through a secure quantum channel, and each participant's contribution to the negotiated key is the same. On the one hand, due to the high cost and scarce resources, it is difficult for the vast majority of participants to have well-performing quantum devices. Therefore, in order to facilitate the implementation of the protocol, it is necessary to simplify the quantum operations of the participants. In response to this problem, some scholars have proposed a semi-quantum key agreement protocol. The semi-quantum key agreement protocol requires that one of the participants in the protocol has complete quantum capabilities, and the remaining participants only have semi-quantum capabilities. Moreover, the semi-quantum participants can only perform the following two operations: i) reflection operation. No operation is performed on the received particles, and the received particles are returned directly. ii) Measurement operation. Z-based measurement is performed on the received particles, and new particles are prepared according to the measurement results. On the other hand, since participants may be attacked by man-in-the-middle in the process of key agreement, it is necessary to authenticate participants before the key agreement. In recent years, researchers have also proposed some quantum key agreement protocols with mutual authentication. In practical application scenarios, in order to facilitate the implementation of the protocol, it is necessary to design a semi-quantum key agreement protocol with lower requirements for participants' ability and equipment. In order to prevent external attackers from counterfeiting authorized users to steal shared keys, the protocol needs to have a mutual authentication function. Therefore, it is necessary to design a semi-quantum key agreement protocol with mutual authentication.

Methods Based on the Bell state, we propose a two-party semi-quantum key agreement protocol with a mutual authentication function, where Alice is a full quantum participant and Bob is a semi-quantum participant. The two sides achieve mutual authentication of identity by preparing and measuring identity information particles. By using the entanglement characteristics of the Bell state, the shared key negotiation was realized. Compared with other entangled states, the Bell state used in this protocol is easier to prepare, and the protocol only uses two quantum measurement operations, namely Z-based measurement and Bell measurement, which are easier to implement in existing technology. In addition, we proved that the proposed scheme can effectively resist participant attacks and external attacks, and that the protocol is equipped with a wavelength quantum filter and a photon number separator on both sides of Alice and Bob to avoid Trojan horse attacks. In the performance analysis of this protocol, the Cabello qubit efficiency was used to measure the performance of the quantum key agreement protocol.

Results and Discussions First of all, in the previous research on quantum key agreement protocols, some scholars focus on how to simplify the quantum operation of participants, so as to better apply to the actual scene of resource scarcity, while others pay attention to how to prevent the man-in-the-middle attacks that may be encountered during the key agreement process and further improve the security of the protocol. The two-party mutual authentication semi-quantum key agreement protocol based on the Bell state proposed in this paper can not only reduce the requirements for participants' capabilities and devices, but also realize mutual authentication between participants before key agreement to prevent the protocol from being attacked by man-in-the-middle. Finally, a security analysis shows that the protocol can effectively resist participant and external attacks. In addition, the performance analysis shows that the protocol can improve the quantum bit efficiency compared with some quantum key agreement protocols that meet a single function under the condition of satisfying two functional characteristics at the same time.

Conclusions In this study, a two-party mutual authentication semi-quantum key agreement protocol based on the Bell state is proposed. The protocol not only ensures that the shared key can be fairly negotiated between the full quantum party, Alice, and the semi-quantum party, Bob, but more importantly, the two parties need to authenticate each other's identity before the key agreement, so as to resist external attackers posing as legitimate users to steal the shared key. Security analysis shows that this semi-quantum key agreement protocol can resist both participant and external attacks. Finally, through a performance analysis and comparison with existing quantum key agreement protocols, it is found that the protocol has certain advantages in terms of its function and performance.

Key words quantum optics; quantum cryptography; semi-quantum key agreement; mutual identity authentication; Bell state