基于 Bell 态的两方互认证量子密钥协商协议

何业锋，狄 曼*，庞一博，岳玉茹，李国庆，刘继祥

(西安邮电大学网络空间安全学院 西安 710121)

【摘要】针对已有互认证量子密钥协商协议需要可信或者半可信第三方参与造成的步骤繁琐且通信量大的问题，基于 Bell 态和其纠缠交换性质提出了一个新的两方量子密钥协商协议。该密钥协商协议无需可信或者半可信第三方的参与，就能实现参与者之间的身份互认证和公平的密钥协商，因此降低了协议的通信复杂度。安全性分析表明，该互认证的密钥协商协议能保证身份认证过程可以抵抗假冒攻击，密钥协商过程能抵抗外部攻击和参与者攻击。另外，与已有互认证量子密钥协商协议相比，该协议的量子比特效率较高，且其量子态制备和测量用现有技术更易实现。

关 键 词 Bell 态； 纠缠交换； 身份互认证； 量子密码； 量子密钥协商

中图分类号 TN918 文献标志码 A doi:10.12178/1001-0548.2022008

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

HE Yefeng, DI Man*, PANG Yibo, YUE Yuru, LI Guoqing, and LIU Jixiang

(School of Cyberspace Security, Xi'an University of Posts and Telecommunications Xi'an 710121)

Abstract In order to solve the problem of complicated steps and large communication volume caused by the participation of trusted or semi-trusted third parties in the existing mutual authentication quantum key agreement protocols, a new two-party quantum key agreement protocol is proposed based on Bell states and their entangled exchange properties. The key agreement protocol can realize identity mutual authentication and fair key agreement between participants without the participation of trusted or semi-trusted third parties, thus reducing the communication complexity of the protocol. The security analysis shows that its identity authentication process can resist impersonation attack, and its key agreement process can resist external attacks and participant attacks. In addition, compared with the existing mutual authentication quantum key agreement protocols, the quantum bit efficiency of the protocol is also higher, and its quantum state preparation and measurement are easier to achieve with existing technologies.

Key words Bell state; entanglement exchange; mutual identity authentication; quantum cryptography; quantum key agreement

量子密码的安全基于海森堡不确定原理[1]和量子不可克隆定理[2]。近年来，随着量子密码应用的发展，量子密码学引起越来越多的关注，研究成果层出不穷，包括量子密钥分发 (quantum key distribution, QKD)[3-4]、量子密钥协商 (quantum key agreement, QKA)[5]、量子秘密共享 (quantum secret sharing, QSS)[6]、量子安全直接通信 (quantum secure direct communication, QSDC)[7]、量子私有比较 (quantum private comparison, QPC)[8]以及量子远程态准备 (quantum remote state preparation, QRSP)[9]等。量子密钥协商 (QKA) 是量子密码学的一个重要研究方向。它允许所有参与者共同协商一个会话密钥，并且每个参与者对生成会话密钥的贡献是相同的，即会话密钥不能由任意一方完全决定。它显然不同于 QKD，因为 QKD 是由一个参与者决定会话密钥并将其分发给其他各方。因此，QKA 在生成会话密钥方面比 QKD 更加公平。

QKA 经过了多年的研究发展，取得了大量研究成果。2004 年，文献 [5] 提出了第一个 QKA 协议，其中通信方共同确定会话密钥。2010 年，文献 [10] 提出了一种基于 BB84[3] 的 QKA 协议，利用延迟测量技术和双 CNOT 操作，实现了会话密

收稿日期：2021－12－30；修回日期：2022－03－28
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 (2021JM-462)
作者简介：何业锋 (1978－)，女，博士，教授，主要从事量子密码方面的研究.
*通信作者：狄曼，E-mail：1362392440@qq.com

钥的公平建立。2013 年，文献 [11] 提出了利用 EPR 对和纠缠交换技术将参与者由两方扩展为多方的 QKA 协议。2017 年，文献 [12] 提出了两种不受集体噪声影响的 QKA 协议，这两种协议主要利用逻辑量子态、多粒子纠缠态的测量相关特性和延迟测量技术，使得协议的性能得到提升。2020 年，文献 [13] 提出了一种三方半量子密钥协商协议，降低了对参与者能力和设备的要求。2020 年，文献 [14] 提出了基于最大三粒子纠缠态的受控量子密钥协商协议，与之前的两方和三方 QKA 协议相比较，最大的变化是引入了一个监督者来控制协议过程，以提高协议的可控性。2021 年，文献 [15] 提出了基于类 GHz 态的半诚实三方互认证量子密钥协商协议，利用身份认证部分验证用户身份的真实性，确保密钥协商双方身份的正确性与可靠性，并且能防止外部攻击者冒充合法用户传递虚假信息窃取会话密钥。这与其他 QKA 协议相比，更符合实际应用需求。因此，设计具有互认证功能的 QKA 协议有重要意义。

然而已有的互认证量子密钥协商协议需要在可信或者半可信第三方的帮助下才能实现参与者之间的密钥协商，因此步骤繁琐且通信量较大。利用 Bell 态，本文提出了一个无需第三方参与的两方互认证 QKA 协议。在该协议中，两个参与方通过对身份信息粒子的制备和测量，来实现双方身份的互认证；并且利用 Bell 态的纠缠交换关系和编码实现密钥协商。新的 QKA 协议被证明是安全的且有较高的量子比特效率。

1　理论知识

4 个 Bell 态构成了四维 Hilbert 空间的一组正交基，即：

$$\left|\phi^{+}\right\rangle=\left(|00\rangle+|11\rangle\right)\Big/\sqrt{2} \tag{1}$$

$$\left|\phi^{+}\right\rangle=\left(|00\rangle+|11\rangle\right)\Big/\sqrt{2} \tag{2}$$

$$\left|\psi^{+}\right\rangle=\left(|01\rangle+|10\rangle\right)\Big/\sqrt{2} \tag{3}$$

$$\left|\psi^{-}\right\rangle=\left(|01\rangle-|10\rangle\right)\Big/\sqrt{2} \tag{4}$$

任意两个 Bell 态纠缠交换后仍然处于一对 Bell 态，如：

$$\begin{aligned}\left|\phi^{+}\right\rangle_{12}\left|\phi^{+}\right\rangle_{34}=&\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{12}\otimes\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{34}=\\&\frac{1}{2}\left(\begin{array}{l}\left|\phi^{+}\right\rangle_{13}\left|\phi^{+}\right\rangle_{24}+\left|\phi^{-}\right\rangle_{13}\left|\phi^{-}\right\rangle_{24}+\\\left|\psi^{+}\right\rangle_{13}\left|\psi^{+}\right\rangle_{24}+\left|\psi^{-}\right\rangle_{13}\left|\psi^{-}\right\rangle_{24}\end{array}\right)\end{aligned} \tag{5}$$

根据式 (5) 可知，若对粒子1,3进行 Bell 基测量，测量结果为$\left|\phi^{+}\right\rangle_{13},\left|\phi^{-}\right\rangle_{13},\left|\psi^{+}\right\rangle_{13}$或$\left|\psi^{-}\right\rangle_{13}$的概率各是1/4，相应粒子2,4的状态也是类似的情况。其他 Bell 态的纠缠交换情况详见表 1。

表 1　Bell 态的纠缠交换[11]

Bell态	Bell态	纠缠交换后的Bell态			
$\left\|\phi^{+}\right\rangle_{12}$	$\left\|\phi^{+}\right\rangle_{34}$	$\left\|\phi^{+}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$	$\left\|\phi^{-}\right\rangle_{13}\left\|\phi^{-}\right\rangle_{24}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$
$\left\|\phi^{+}\right\rangle_{12}$	$\left\|\phi^{-}\right\rangle_{34}$	$\left\|\phi^{+}\right\rangle_{13}\left\|\phi^{-}\right\rangle_{24}$	$\left\|\phi^{-}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$
$\left\|\phi^{+}\right\rangle_{12}$	$\left\|\psi^{+}\right\rangle_{34}$	$\left\|\phi^{+}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$	$\left\|\phi^{-}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\phi^{-}\right\rangle_{24}$
$\left\|\phi^{+}\right\rangle_{12}$	$\left\|\psi^{-}\right\rangle_{34}$	$\left\|\phi^{+}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$	$\left\|\phi^{-}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\phi^{-}\right\rangle_{24}$
$\left\|\phi^{-}\right\rangle_{12}$	$\left\|\phi^{+}\right\rangle_{34}$	$\left\|\phi^{-}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$	$\left\|\phi^{+}\right\rangle_{13}\left\|\phi^{-}\right\rangle_{24}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$
$\left\|\phi^{-}\right\rangle_{12}$	$\left\|\phi^{-}\right\rangle_{34}$	$\left\|\phi^{-}\right\rangle_{13}\left\|\phi^{-}\right\rangle_{24}$	$\left\|\phi^{+}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$
$\left\|\phi^{-}\right\rangle_{12}$	$\left\|\psi^{+}\right\rangle_{34}$	$\left\|\phi^{-}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\phi^{-}\right\rangle_{24}$	$\left\|\phi^{+}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$
$\left\|\phi^{-}\right\rangle_{12}$	$\left\|\psi^{-}\right\rangle_{34}$	$\left\|\phi^{-}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\phi^{-}\right\rangle_{24}$	$\left\|\phi^{+}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$
$\left\|\psi^{+}\right\rangle_{12}$	$\left\|\phi^{+}\right\rangle_{34}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$	$\left\|\phi^{+}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$	$\left\|\phi^{-}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\phi^{-}\right\rangle_{24}$
$\left\|\psi^{+}\right\rangle_{12}$	$\left\|\phi^{-}\right\rangle_{34}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\phi^{-}\right\rangle_{24}$	$\left\|\phi^{-}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$	$\left\|\phi^{+}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$
$\left\|\psi^{+}\right\rangle_{12}$	$\left\|\psi^{+}\right\rangle_{34}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$	$\left\|\phi^{+}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$	$\left\|\phi^{-}\right\rangle_{13}\left\|\phi^{-}\right\rangle_{24}$
$\left\|\psi^{+}\right\rangle_{12}$	$\left\|\psi^{-}\right\rangle_{34}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$	$\left\|\phi^{+}\right\rangle_{13}\left\|\phi^{-}\right\rangle_{24}$	$\left\|\phi^{-}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$
$\left\|\psi^{-}\right\rangle_{12}$	$\left\|\phi^{+}\right\rangle_{34}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$	$\left\|\phi^{+}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$	$\left\|\phi^{-}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\phi^{-}\right\rangle_{24}$
$\left\|\psi^{-}\right\rangle_{12}$	$\left\|\phi^{-}\right\rangle_{34}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\phi^{-}\right\rangle_{24}$	$\left\|\phi^{-}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$	$\left\|\phi^{+}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$
$\left\|\psi^{-}\right\rangle_{12}$	$\left\|\psi^{+}\right\rangle_{34}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$	$\left\|\phi^{+}\right\rangle_{13}\left\|\phi^{-}\right\rangle_{24}$	$\left\|\phi^{-}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$
$\left\|\psi^{-}\right\rangle_{12}$	$\left\|\psi^{-}\right\rangle_{34}$	$\left\|\psi^{-}\right\rangle_{13}\left\|\psi^{-}\right\rangle_{24}$	$\left\|\psi^{+}\right\rangle_{13}\left\|\psi^{+}\right\rangle_{24}$	$\left\|\phi^{+}\right\rangle_{13}\left\|\phi^{+}\right\rangle_{24}$	$\left\|\phi^{-}\right\rangle_{13}\left\|\phi^{-}\right\rangle_{24}$

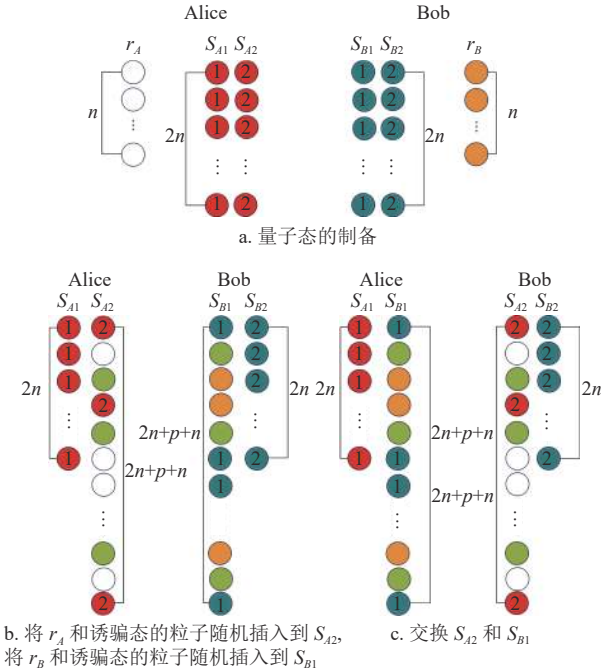
然后，定义 Bell 态的一种编码规则，即将$|\phi^+\rangle$编码为 00，$|\phi^-\rangle$编码为 01，$|\psi^+\rangle$编码为 10，$|\psi^-\rangle$编码为11。当用C_{12},C_{34}，C_{13},C_{24}分别表示不同粒子 Bell 态的二进制编码时，根据表 1 可得$C_{12}\oplus C_{34}=C_{13}\oplus C_{24}$，其中⊕表示按位异或。

2 两方互认证量子密钥协商协议

当 Alice 和 Bob 想要协商一个会话密钥时，他们需要先相互认证对方的身份，当身份认证通过后，Alice 和 Bob 再进行密钥协商。协议的身份认证及密钥协商的具体步骤如下。

1) Alice 和 Bob 事先秘密共享一对身份信息序列 $R_A=R_A^1R_A^2\cdots R_A^n$和 $R_B=R_B^1R_B^2\cdots R_B^n$，其中，$R_A^i$，$R_B^i\in\{0,1\}$，并且$i\in\{1,2,3,\cdots,n\}$。Alice 根据身份信息序列$R_A$制备相应的粒子序列$r_A=r_A^1r_A^2r_A^3\cdots r_A^n$，当$R_A^i=0$时，$r_A^i$被随机制备为$|0\rangle$态或$|+\rangle$态；当$R_A^i=1$时，$r_A^i$被随机制备为$|1\rangle$态或$|-\rangle$态。同理，Bob 根据身份信息序列$R_B$制备相应的粒子序列$r_B=r_B^1r_B^2r_B^3\cdots r_B^n$。

2) Alice 从集合$\{|\phi^+\rangle,|\phi^-\rangle,|\psi^+\rangle,|\psi^-\rangle\}$中随机选择$2n$个 Bell 态，形成一个 Bell 态序列$S_A=s_{a_{12}}^1s_{a_{12}}^2s_{a_{12}}^3\cdots s_{a_{12}}^{2n}$。采用同样的方法，Bob 也得到一个长度为$2n$的 Bell 态序列$S_B=s_{b_{12}}^1s_{b_{12}}^2s_{b_{12}}^3\cdots s_{b_{12}}^{2n}$。量子态的制备如图 1a 所示。



a. 量子态的制备

b. 将 r_A 和诱骗态的粒子随机插入到 S_{A2}，将 r_B 和诱骗态的粒子随机插入到 S_{B1}

c. 交换 S_{A2} 和 S_{B1}

图 1 量子态的制备与传输

3) Alice 将S_A中 Bell 态的所有第一个粒子按原顺序形成序列$S_{A1}=s_{a_1}^1s_{a_1}^2s_{a_1}^3\cdots s_{a_1}^{2n}$；将$S_A$中 Bell 态的所有第二个粒子按原顺序形成序列$S_{A2}=s_{a_2}^1s_{a_2}^2s_{a_2}^3\cdots s_{a_2}^{2n}$。并将$p$个诱骗态粒子和序列$r_A=r_A^1r_A^2r_A^3\cdots r_A^n$中的$n$个粒子随机插入序列$S_{A2}$中，其中，诱骗态粒子是从集合$\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$中随机选取的。新序列记为$S_{A2}^*$，Alice 将它发给 Bob，自己保留$S_{A1}$。生成新粒子序列$S_{A2}^*$和$S_{B1}^*$如图 1b 所示。

与此同时，Bob 执行类似操作，得到序列S_{B1}^*和S_{B2}，其中S_{B1}^*也插入了诱骗态粒子和序列r_B中的所有粒子。Bob 将S_{B1}^*发送给 Alice，保留S_{B2}。如图 1c 粒子序列的交换所示。

4) 当 Alice 收到 Bob 发来的S_{B1}^*后，Bob 公布诱骗态粒子位置以及相应测量基。Alice 对诱骗态粒子进行测量，并公布测量结果。Bob 比较测量结果与诱骗态粒子的初始量子态，计算错误率。同时，当 Bob 收到 Alice 发来的S_{A2}^*后，Alice 和 Bob 执行类似操作。然后 Alice 计算错误率。

如果 Alice 和 Bob 计算的错误率都低于门限值[16]，则认为信道是安全的，Alice 和 Bob 可以继续进行下一步；如果 Alice 和 Bob 哪一方计算的错误率高于门限值，则停止该步骤并重新开始。

5) 当两方的信道都通过了安全检测后，就对双方进行身份认证。

当认证 Alice 身份时，由 Alice 公布r_A中所有粒子的位置和测量基，而 Bob 则对r_A中所有粒子进行测量。然后 Bob 根据r_A的测量结果和步骤 1)，得到相应二进制序列R_A'，通过比较R_A'与R_A是否相等，来判断 Alice 的身份是否正确。通过对S_{B1}^*中的r_B粒子执行类似操作，来判断 Bob 的身份是否正确。

如果 Alice 和 Bob 双方都通过了身份认证，则可以继续进行协议的下一步，否则终止协议并重新开始。信道安全性检测与身份认证如图 2 所示。先测量诱骗态粒子，完成信道安全性检测后，再测量身份信息粒子，完成身份认证。

6) 去掉S_{B1}^*中的r_B和诱骗态粒子恢复序列S_{B1}后，Alice 对S_{B1}和S_{A1}中的对应粒子做 Bell 基测量，得到新序列$S_A'=s_{a_1b_1}^1s_{a_1b_1}^2s_{a_1b_1}^3\cdots s_{a_1b_1}^{2n}$。同时 Bob 执行类似操作，得到新序列$S_B'=s_{a_2b_2}^1s_{a_2b_2}^2s_{a_2b_2}^3\cdots s_{a_2b_2}^{2n}$。

7) Alice 根据第 1 节中的编码规则将序列S_A和S_A'转换为二进制序列$C_A=C_{a_1a_2}^1C_{a_1a_2}^2C_{a_1a_2}^3\cdots C_{a_1a_2}^{2n}$和$C_A'=C_{a_1b_1}^1C_{a_1b_1}^2C_{a_1b_1}^3\cdots C_{a_1b_1}^{2n}$；同时 Bob 执行类似操作将$S_B$和$S_B'$转换为二进制序列$C_B=C_{b_1b_2}^1C_{b_1b_2}^2$

$C^3_{b_1b_2}\cdots C^{2n}_{b_1b_2}$和$C'_B=C^1_{a_2b_2}C^2_{a_2b_2}C^3_{a_2b_2}\cdots C^{2n}_{a_2b_2}$。然后，Alice 和 Bob 在经典信道公布$C_A$和$C_B$。

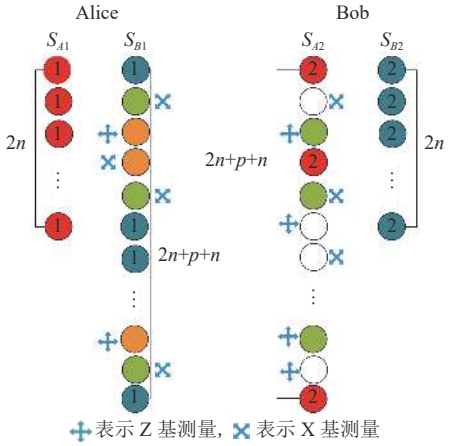


图 2　信道安全性检测与身份认证

8) Alice 根据公式$C_A\oplus C_B=C'_A\oplus C'_B$和她拥有的$C'_A$可以计算出$C'_B$；同理 Bob 可以计算出$C'_A$。那么他们协商的会话密钥是$K_{AB}=\{C^1_{a_1b_1},C^2_{a_2b_2},\cdots,C^{2n-1}_{a_1b_1},C^{2n}_{a_2b_2}\}$。Bell 态的测量与密钥协商如图 3 所示，其中 BM 表示 Bell 态的测量。

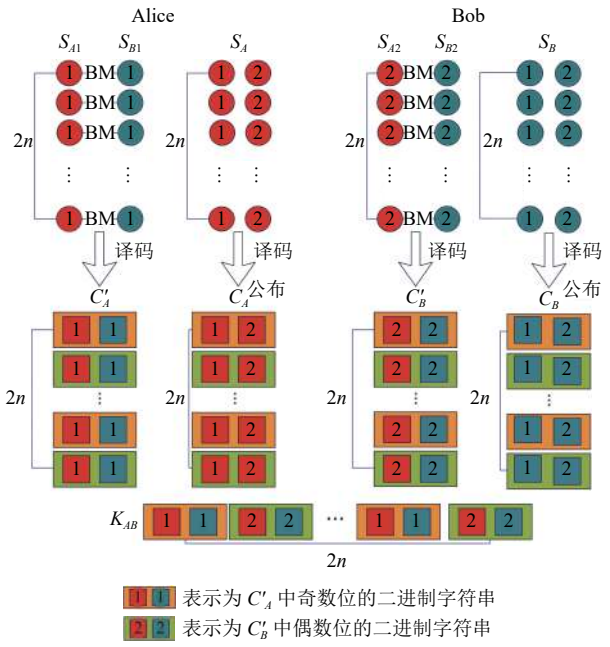


图 3　Bell 态的测量与密钥协商

3　分析与讨论

一个好的 QKA 协议应该既可以抵抗外部攻击，也可以抵抗内部攻击。

3.1　外部攻击

Alice 和 Bob 在步骤 1)、2) 制备序列r_A，r_B，S_A和S_B；在步骤 3) 传输序列S^*_{A2}和S^*_{B1}；在步骤 4) 测量序列S^*_{A2}和S^*_{B1}中的诱骗态粒子进行信道安全性检测；在步骤 5) 对序列S^*_{A2}和S^*_{B1}中的粒子r^i_A和r^i_B进行测量完成身份认证；在步骤 6)～8) 完成会话密钥协商。通过对协议的分析知，双方只在步骤 3) 进行了信息的传输，其他步骤只进行了量子态的制备和测量。

身份假冒攻击：假设 Eve 想冒充 Alice 身份。由于 Eve 不知道 Alice 的身份信息序列R_A，他只能在步骤 1) 中随机制备粒子序列$r'_A=r'^1_Ar'^2_Ar'^3_A\cdots r'^n_A$。然而在步骤 5) 的身份认证过程中，Bob 测量r'_A的结果和身份信息R_A是无关的。如假设 Alice 的身份信息$R_A=R^1_A=0$，然而 Eve 并不知道R^1_A，他只能从集合$\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$中随机选取粒子态，当他选择$|0\rangle$态或$|+\rangle$态时，Bob 测量结果的编码为 0；当他选择$|1\rangle$态或$|-\rangle$态时，Bob 测量结果的编码为 1。那么 Eve 冒充成功的概率为1/2，当R_A长度为n时，最终 Eve 冒充成功的概率为$(1/2)^n$。当n足够大时，Eve 冒充成功的概率$(1/2)^n$趋于 0。同理当 Eve 冒充 Bob 身份时，Alice 进行类似操作也容易判断出 Eve 的身份是假冒的。

针对会话密钥的攻击：假设 Eve 想窃取会话密钥，他只能在双方通信时，即在步骤 3) 对序列S^*_{A2}和S^*_{B1}执行特洛伊木马攻击、测量−重发攻击、截获−重发攻击或纠缠−测量攻击。由于序列S^*_{A2}和S^*_{B1}在本协议中仅被传输了一次，因此 Eve 无法成功实现两种特洛伊木马攻击[17-19]。若 Eve 进行测量−重发攻击、截获−重发攻击或纠缠−测量攻击，然而 Eve 的操作会影响序列S^*_{A2}和S^*_{B1}中诱骗态粒子的状态[12]，从而 Alice 和 Bob 在步骤 4) 的信道安全性检测中就能发现 Eve 的攻击。

3.2　参与者攻击

当 Alice 和 Bob 通过了身份认证后，他们的身份就是合法的。在后续密钥中，双方交换序列S^*_{A2}和S^*_{B1}，并分别测量序列对(S_{A1},S_{B1})和(S_{A2},S_{B2})。由式 (2) 和表 1 给出的纠缠交换关系可知，Alice 和 Bob 的测量结果是在 4 种 Bell 态中等概率出现的。即双方的测量结果是随机的，Alice 和 Bob 都不能决定他们的测量结果。因此，双方都不能成功执行参与者攻击。

3.3　性能分析

QKA 协议的量子比特效率公式[20]定义为$\eta=c/(q+b)$，其中，c表示协商出的会话密钥的比

特数量，q表示协议中用到的量子比特总数，b表示用于解码的经典信息。

因为本文 QKA 协议中用到的 Bell 态数量为$4n$，诱骗态量子比特数量为$2p$，身份认证粒子的比特数量为$2n$，经典解码信息为$b=4n+4n=8n$，得到的会话密钥比特数量为$c=4n$。所以本文 QKA 的量子比特效率为$\eta=4n/(4n\times2+2p+2n+8n)$。又因为身份认证粒子是随机插入的，可起部分诱骗态粒子的作用，所以可令$p=n$。当$p=n$时，效率为$\eta=4n/20n=20\%$。它与已有互认证的 QKA 协议的比较可以参见表 2。根据表 2 知本文的 QKA 协议在量子比特效率方面也较高。

表 2　本文互认证的 QKA 协议与已有互认证的 QKA 协议的比较

协议	量子态	量子信道	比特效率/%
TSW's协议[15]	GHz-like态	3	25.00
MHZ's协议[21]	五粒子纠缠态	2	7.7
本文协议	Bell态	1	20

4　结 束 语

本文利用 Bell 态提出了一个两方的互认证量子密钥协商协议，它无需第三方的参与就能实现参与者的身份互认证和密钥协商，协议的步骤简单且只需一次交互的量子通信。 安全性分析证明了这个 QKA 协议可以有效抵抗外部攻击和内部攻击。与已有的互认证 QKA 协议相比较，本文提出的新的互认证 QKA 协议不但有较高的量子比特效率，而且仅用到了单粒子测量和 Bell 态测量，在现有技术的基础上更易实现。

参 考 文 献

[1] YANG X J, BALEANU D, MACHADO J. Mathematical aspects of the Heisenberg uncertainty principle within local fractional Fourier analysis[J]. Boundary Value Problems, 2013(1): 131.

[2] NAGATA K, NAKAMURA T, FAROUK A, et al. No-Cloning theorem, kochen-specker theorem, and quantum measurement theories[J]. International Journal of Theoretical Physics, 2019, 58(6): 1845-1853.

[3] BENNETT C H, BRASSARD G. Quantum cryptography: Public key distribution and coin tossing[C]//Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing. Bangalore: IEEE, 1984: 175-179.

[4] 何业锋, 赵艳坤, 郭佳瑞, 等. 基于标记配对相干态的量子密钥分配协议的统计涨落分析[J]. 中国激光, 2020, 40(7): 09120002.
HE Y F, ZHAO Y K, GUO J R, et al. Statistical fluctuation analysis of quantum key distribution protocols based on heralded pair coherent state[J]. Chinese Journal of Lasers, 2020, 40(7): 09120002.

[5] ZHOU N, ZENG G, XIONG J. Quantum key agreement protocol[J]. Electronics Letters, 2004, 40(18): 1149-1150.

[6] QIN L, LIU H J, ZHU L J, et al. Quantum secret sharing using discretely modulated coherent states[J]. Physical Review A, 2021, 103(3): 032410.

[7] HE Y F, MA W P. Multiparty quantum secure direct communication immune to collective noise[J]. Quantum Information Process, 2019, 18(1): 1-11.

[8] JI Z X, FAN P R, ZHANG H G, et al. Cryptanalysis and improvement of several quantum private comparison protocols[J]. Communications in Theoretical Physics, 2020, 72(8): 085101.

[9] SUN S, ZHANG H. Double-Direction quantum cyclic controlled remote state preparation of two-qubit states[J]. Quantum Information Processing, 2021, 20(6): 1-33.

[10] CHONG S K, HWANG T. Quantum key agreement protocol based on BB84[J]. Optics Communications, 2010, 283(6): 1192-1195.

[11] SHI R H, ZHONG H. Multi-Party quantum key agreement with bell states and bell measurements[J]. Quantum Information Processing, 2013, 12(2): 921-932.

[12] 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.

[13] ZHOU N R, ZHU K N, WANG Y Q. Three-Party semi-quantum key agreement protocol[J]. International Journal of Theoretical Physics, 2020, 59(3): 663-676.

[14] TANG J, SHI L, WEI J. Controlled quantum key agreement based on maximally three-qubit entangled states[J]. Modern Physics Letters B, 2020, 34(18): 2050201.

[15] 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.

[16] ZHU Z C, HU A Q, FU A M. Cryptanalysis of a new circular quantum secret sharing protocol for remote agents[J]. Quantum Information Processing, 2013, 12(2): 1173-1183.

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

[18] DENG F G, LI X H, ZHOU H Y, et al. Improving the security of multiparty quantum secret sharing against Trojan horse attack[J]. Physical Review A, 2005, 72(4): 044302.

[19] LI X H, DENG F G, ZHOU H Y. Improving the security of secure direct communication based on the secret transmitting order of particles[J]. Physical Review A, 2006, 74(5): 054302.

[20] FAHMI A, GOLSHANI M. Quantum key distribution in the Holevo limit[J]. Physical Review Letters, 2000, 85(1): 5635-5638.

[21] 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.

编　辑　蒋　晓