基于类GHZ态和Bell态纠缠交换的半量子隐私比较

徐 欣,甘志刚,叶天语
(浙江工商大学信息与电子工程学院,浙江杭州 310018)

摘 要: 本文提出一种基于类GHZ态与Bell态纠缠交换的半量子隐私比较(SemiQuantum Private Comparison,SQPC)协议,在不泄露两个半量子通信者隐秘信息的前提下借助半忠诚第三方(Third Party,TP)正确地比较出隐秘信息的相等性. 半忠诚TP被假定可以发起任何攻击,但不能与她人合谋. 本文详细证明了该协议针对外部窃听者的攻击具备完全鲁棒性,并且分析了该协议针对内部不诚实参与者具备安全性. 本文还通过IBM的Qiskit对该协议的流程和输出正确性进行实验仿真.

关键词: 半量子隐私比较;纠缠交换;类GHZ态;Bell态;Qiskit
基金项目: 国家自然科学基金(No.62071430)
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2025)03-0836-13
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20240193

Semiquantum Private Comparison Based on Entanglement Swapping of GHZ-Like State and Bell State

XU Xin, GAN Zhi-gang, YE Tian-yu
(*College of Information & Electronic Engineering*, *Zhejiang Gongshang University*, *Hangzhou*, *Zhejiang* 310018, *China*)

Abstract: This paper proposed a protocol of semiquantum private comparison (SQPC) based on entanglement swapping of GHZ-like state and Bell state, which allows the classical participants to compare the equality of their secret message under the help of a semi-honest third party (TP). TP is allowed to misbehave but cannot collude with anyone else. This paper provides a detailed proof of the protocol's complete robustness against external eavesdroppers' attacks, and analyzes its security against dishonest internal participants. This paper also conducted experimental simulations on the flow and output correctness of the protocol using IBM's Qiskit. In addition, the security of the proposed protocol is confirmed and it can effectively prevent various kinds of attacks.

Key words: semiquantum private comparison; entanglement swapping; GHZ-like state; Bell state; Qiskit
Foundation Item(s): National Natural Science Foundation of China (No.62071430)

1 前言

经典安全计算起源于Yao[1]提出的百万富翁问题. 百万富翁问题是指两富翁希望在自己的财富数量不被外泄的情况下得到谁更富有的结果. 经典安全计算在隐秘招标、隐秘拍卖、隐秘选举等场合有着广泛的应用. 经典隐私比较是经典安全计算的一个重要分支,其安全性取决于解决数学问题的复杂度.

在2009年,Yang等人[2]将量子力学与经典隐私比较结合在一起从而首次提出量子隐私比较(Quantum Private Comparison,QPC)的概念. 在一个量子隐私比较方案中,两个量子通信者在不泄露自身隐秘信息的前提下可以正确地比较出隐秘信息的相等性或大小关系. QPC是量子安全计算的一个重要分支,其安全性是基于量子力学规律而非解决数学问题的复杂度.

在一个量子密码协议中,量子通信者往往需要进行量子叠加态或量子纠缠态的制备或测量,从而需要配备昂贵的量子设备. 然而,并非所有通信者都具备这样的条件. 在2009年,为了将部分通信者从量子叠加态或量子纠缠态的制备或测量中解脱出来,Boyer等人[3,4]首次提出半量子的概念. 在一个半量子密码协议中,半量子通信者只能进行如下操作[3,4]:(1)制备粒子处于$\{|0\rangle,|1\rangle\}$基(即Z基);(2)利用Z基测量粒子;(3)通过量子信道传送粒子;(4)置乱粒子. 在2016年,Chou等人[5]将半量子概念引入到QPC

收稿日期:2024-02-27;修回日期:2024-11-18;责任编辑:李勇锋

从而提出首个半量子隐私比较(SemiQuantum private comparison,SQPC)协议. 此后,一系列基于不同类型量子态的SQPC协议被先后设计出来,如基于单粒子态[6~10]、基于Bell态[5,11~21]、基于W态[22]、基于类GHZ态[23,24]和基于四粒子团簇态[19]等.

量子纠缠交换是一种非常重要的量子资源,被广泛应用于量子安全计算协议的设计中. 就我们所知,目前只有文献[5,19,21]三个SQPC协议是基于量子纠缠交换. 具体来讲,文献[5,21]的两个SQPC协议是基于两个Bell态之间的纠缠交换,文献[19]的SQPC协议是基于Bell态和四粒子团簇态之间的纠缠交换. 总体上说,目前基于纠缠交换的SQPC协议还比较匮乏,值得进一步去研究. 而且,文献[19]的SQPC协议需采用在实际中不易制备的四粒子团簇态作为量子资源;文献[21]的SQPC协议需采用环形粒子传输模式,不易保证半量子方的独立性;文献[19]的SQPC协议的量子比特效率并不理想,有待进一步提高;文献[5]和文献[19]的协议并未对协议流程和输出正确性进行量子仿真.

基于以上分析,本文提出一种基于类GHZ态与Bell态纠缠交换的SQPC协议,在不泄露两个半量子通信者隐秘信息的前提下正确地比较出隐秘信息的相等性. 该协议针对外部窃听者攻击的完全鲁棒性和针对内部参与者攻击的安全性得到详细验证. 我们通过IBM的Qiskit对本文协议的流程和输出正确性进行实验仿真. 由于只采用类GHZ态和Bell态作为量子资源,本文协议在量子资源的使用上比文献[19]的SQPC协议更具优势;由于只采用树型粒子传输模式,相比于文献[21]的SQPC协议,本文协议更易保证半量子方的独立性;本文协议的量子比特效率高于文献[19]的SQPC协议.

2　所提出的SQPC协议

类GHZ基是三粒子量子系统空间的一组标准正交基,由以下八个量子态构成[25]:

$$|\vartheta_0\rangle=\frac{1}{2}\left(|000\rangle+|011\rangle+|101\rangle+|110\rangle\right) \tag{1}$$

$$|\vartheta_1\rangle=\frac{1}{2}\left(|001\rangle+|010\rangle+|100\rangle+|111\rangle\right) \tag{2}$$

$$|\vartheta_2\rangle=\frac{1}{2}\left(|000\rangle-|011\rangle-|101\rangle+|110\rangle\right) \tag{3}$$

$$|\vartheta_3\rangle=\frac{1}{2}\left(|001\rangle-|010\rangle-|100\rangle+|111\rangle\right) \tag{4}$$

$$|\vartheta_4\rangle=\frac{1}{2}\left(|000\rangle-|011\rangle+|101\rangle-|110\rangle\right) \tag{5}$$

$$|\vartheta_5\rangle=\frac{1}{2}\left(|001\rangle-|010\rangle+|100\rangle-|111\rangle\right) \tag{6}$$

$$|\vartheta_6\rangle=\frac{1}{2}\left(|000\rangle+|011\rangle-|101\rangle-|110\rangle\right) \tag{7}$$

$$|\vartheta_7\rangle=\frac{1}{2}\left(|001\rangle+|010\rangle-|100\rangle-|111\rangle\right) \tag{8}$$

Bell基是两粒子量子系统空间的一组标准正交基,由以下四个量子态构成:

$$|\phi^+\rangle=\frac{1}{2}\left(|00\rangle+|11\rangle\right) \tag{9}$$

$$|\phi^-\rangle=\frac{1}{2}\left(|00\rangle-|11\rangle\right) \tag{10}$$

$$|\phi^+\rangle=\frac{1}{2}\left(|01\rangle+|10\rangle\right) \tag{11}$$

$$|\phi^-\rangle=\frac{1}{2}\left(|01\rangle-|10\rangle\right) \tag{12}$$

$|\vartheta_1\rangle_{123}$与$|\phi^+\rangle_{45}$之间的纠缠交换描述如下:

$$|\vartheta_1\rangle_{123}\otimes|\phi^+\rangle_{45}=\frac{1}{2}\left(|001\rangle+|010\rangle+|100\rangle+|111\rangle\right)_{123}\otimes\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)_{45} \tag{13}$$

$$|\vartheta_1\rangle_{123}\otimes|\phi^+\rangle_{45}=\frac{1}{2\sqrt{2}}\begin{pmatrix}|0\rangle_1|00\rangle_{24}||10\rangle_{35}+|0\rangle_1|01\rangle_{24}|11\rangle_{35}\\+|0\rangle_1|10\rangle_{24}|00\rangle_{35}+|0\rangle_1|11\rangle_{24}|01\rangle_{35}\\+|1\rangle_1|00\rangle_{24}|00\rangle_{35}+|1\rangle_1|01\rangle_{24}|01\rangle_{35}\\+|1\rangle_1|10\rangle_{24}|10\rangle_{35}+|1\rangle_1|11\rangle_{24}|11\rangle_{35}\end{pmatrix} \tag{14}$$

$$\begin{aligned}|\vartheta_1\rangle_{123}\otimes|\phi^+\rangle_{45}=&\frac{1}{4}|00\rangle_{24}\left[|0\rangle_1\left(|\phi^+\rangle_{35}-|\phi^-\rangle_{35}\right)+|1\rangle_1\left(|\phi^+\rangle_{35}+|\phi^-\rangle_{35}\right)\right]\\&+\frac{1}{4}|01\rangle_{24}\left[|0\rangle_1\left(|\phi^+\rangle_{35}-|\phi^-\rangle_{35}\right)+|1\rangle_1\left(|\phi^+\rangle_{35}+|\phi^-\rangle_{35}\right)\right]\\&+\frac{1}{4}|10\rangle_{24}\left[|0\rangle_1\left(|\phi^+\rangle_{35}+|\phi^-\rangle_{35}\right)+|1\rangle_1\left(|\phi^+\rangle_{35}-|\phi^-\rangle_{35}\right)\right]\\&+\frac{1}{4}|11\rangle_{24}\left[|0\rangle_1\left(|\phi^+\rangle_{35}+|\phi^-\rangle_{35}\right)+|1\rangle_1\left(|\phi^+\rangle_{35}-|\phi^-\rangle_{35}\right)\right]\end{aligned} \tag{15}$$

$$\begin{aligned}|\vartheta_1\rangle_{123}\otimes|\phi^+\rangle_{45}=&\frac{1}{4}|00\rangle_{35}\left[|0\rangle_1\left(|\phi^+\rangle_{24}-|\phi^-\rangle_{24}\right)+|1\rangle_1\left(|\phi^+\rangle_{24}+|\phi^-\rangle_{24}\right)\right]\\&+\frac{1}{4}|01\rangle_{35}\left[|0\rangle_1\left(|\phi^+\rangle_{24}-|\phi^-\rangle_{24}\right)+|1\rangle_1\left(|\phi^+\rangle_{24}+|\phi^-\rangle_{24}\right)\right]\\&+\frac{1}{4}|10\rangle_{35}\left[|0\rangle_1\left(|\phi^+\rangle_{24}+|\phi^-\rangle_{24}\right)+|1\rangle_1\left(|\phi^+\rangle_{24}-|\phi^-\rangle_{24}\right)\right]\\&+\frac{1}{4}|11\rangle_{35}\left[|0\rangle_1\left(|\phi^+\rangle_{24}+|\phi^-\rangle_{24}\right)+|1\rangle_1\left(|\phi^+\rangle_{24}-|\phi^-\rangle_{24}\right)\right]\end{aligned} \tag{16}$$

$$|\vartheta_1\rangle_{123}\otimes|\phi^+\rangle_{45}=\frac{1}{2\sqrt{2}}\begin{pmatrix}|0\rangle_1|\phi^+\rangle_{24}|\phi^+\rangle_{35}-|0\rangle_1|\phi^-\rangle_{24}|\phi^-\rangle_{35}\\+|0\rangle_1|\phi^+\rangle_{24}|\phi^+\rangle_{35}-|0\rangle_1|\phi^-\rangle_{24}|\phi^-\rangle_{35}\\+|1\rangle_1|\phi^+\rangle_{24}|\phi^+\rangle_{35}+|1\rangle_1|\phi^-\rangle_{24}|\phi^-\rangle_{35}\\+|1\rangle_1|\phi^+\rangle_{24}|\phi^+\rangle_{35}+|1\rangle_1|\phi^-\rangle_{24}|\phi^-\rangle_{35}\end{pmatrix} \tag{17}$$

假设Alice和Bob是两个都具有有限量子能力的半量子通信者. Alice的隐秘信息为$M_{\mathrm{A}}=(M_{\mathrm{A}}^0,M_{\mathrm{A}}^1,\cdots,M_{\mathrm{A}}^{L-1})$, Bob的隐秘信息为$M_{\mathrm{B}}=(M_{\mathrm{B}}^0,M_{\mathrm{B}}^1,\cdots,M_{\mathrm{B}}^{L-1})$, 其中, $M_{\mathrm{A}}^i,M_{\mathrm{B}}^i\in\{0,1\},i=0,1,\cdots,L-1,L$为隐秘信息的长度. Alice和Bob试图借助一个拥有完全量子能力的半忠诚第三方(Third Party,TP)来比较出M_A和M_B的相等性. 这里,TP被假定为不能与她人合谋但被允许发起任何攻击[26].

所提出的SQPC协议流程被描述如下,其中三方的测量结果$|0\rangle$都对应经典比特0,三方的测量结果$|1\rangle$都对应经典比特1.

步骤1 Alice和Bob利用文献[27]的带TP的SQKD协议预共享密钥序列$K_{\mathrm{AB}}=(K_{\mathrm{AB}}^0,K_{\mathrm{AB}}^1,\cdots,K_{\mathrm{AB}}^{L-1})$, 其中$K_{\mathrm{AB}}^i\in\{0,1\},i=0,1,\cdots,L-1$.

步骤2 TP制备$8L$个类GHZ态都处于$|\vartheta_1\rangle$以构成序列$S_1=\left[P_1^0P_2^0P_3^0,P_1^1P_2^1P_3^1,\cdots,P_1^{8L-1}P_2^{8L-1}P_3^{8L-1}\right]$, 并且制备$8L$个Bell态都处于$|\phi^+\rangle$以构成序列$S_2=\left[P_4^0P_5^0,P_4^1P_5^1,\cdots,P_4^{8L-1}P_5^{8L-1}\right]$. 这里,上标$\{0,1,\cdots,8L-1\}$表示TP制备的量子纠缠态的序号,下标$\{1,2,3\}$表示$S_1$中每个类GHZ态的三个不同粒子,下标$\{4,5\}$表示$S_2$中每个Bell态的两个不同粒子. 然后,TP提取$S_1$中每个类GHZ态的第一个粒子组成序列$S_{\mathrm{C}}=\left[P_1^0,P_1^1,\cdots,P_1^{8L-1}\right]$,提取$S_1$中每个类GHZ态的第二个粒子和$S_2$中每个Bell态的第四个粒子组成序列$S_{\mathrm{A}}=\left[P_2^0P_4^0,P_2^1P_4^1,\cdots,P_2^{8L-1}P_4^{8L-1}\right]$,并且提取$S_1$中每个类GHZ态的第三个粒子和$S_2$中每个Bell态的第五个粒子组成序列$S_{\mathrm{B}}=\left[P_3^0P_5^0,P_3^1P_5^1,\cdots,P_3^{8L-1}P_5^{8L-1}\right]$. 最后,TP把$S_{\mathrm{C}}$保留在自己手中,并将$S_{\mathrm{A}}$和$S_{\mathrm{B}}$分别发送给Alice和Bob. 除了第一对粒子外,TP只有在收到前一对粒子后才将下一对粒子发送给Alice和Bob.

步骤3 Alice在自己的设备前安装波长滤波器和光子数分割器以抵抗特洛伊木马攻击[28,29]. Alice随机选择进入REFLECT模式或MEASURE模式. 在REFLECT模式下,Alice直接将接收到的S_{A}的一对粒子无干扰地反射给TP,而在MEASURE模式下,Alice用Z基测量接收到的S_{A}的一对粒子,制备新的量子态处于所测量到的状态并发送给TP. 根据测量结果,Alice得到一个二进制序列$C_{\mathrm{A}}=(C_{\mathrm{A}}^0,C_{\mathrm{A}}^1,\cdots,C_{\mathrm{A}}^{4L-1})$, 其中$C_{\mathrm{A}}^j\in\{00,01,10,11\},j=0,1,\cdots,4L-1$.

Bob在自己的设备前安装波长滤波器和光子数分割器以抵抗特洛伊木马攻击[28,29]. Bob随机选择进入REFLECT模式或MEASURE模式. 在REFLECT模式下,Bob直接将接收到的S_{B}的一对粒子无干扰地反射给TP,而在MEASURE模式下,Bob用Z基测量接收到的S_{B}的一对粒子,制备新的量子态处于所测量到的状态并发送给TP. 根据测量结果,Bob得到一个二进制序列$C_{\mathrm{B}}=(C_{\mathrm{B}}^0,C_{\mathrm{B}}^1,\cdots,C_{\mathrm{B}}^{4L-1})$, 其中$C_{\mathrm{B}}^j\in\{00,01,10,11\},j=0,1,\cdots,4L-1$.

步骤4 在TP宣布已收到S_A和S_B后,Alice和Bob分别向TP公布她们对粒子进行的操作. 这里存在四种情形.

情形1 Alice和Bob都选择了REFLECT模式. 这种情形用于窃听检测. TP选出这种情形的三分之一位置,用Z基测量P_1^l,并用Bell基分别测量$P_2^lP_4^l$和$P_3^lP_5^l$. 如果TP对P_1^l的Z基测量结果、对$P_2^lP_4^l$的Bell基测量结果和对$P_3^lP_5^l$的Bell基测量结果都满足式(17),协议将被继续进行;否则,协议将被中止.

TP选出这种情形的三分之一位置,用Z基测量$P_1^lP_2^lP_3^l$,并用Bell基测量$P_4^lP_5^l$. 如果TP对$P_1^lP_2^lP_3^l$的Z基测量结果、对$P_4^lP_5^l$的Bell基测量结果都满足式(13),协议将被继续进行;否则,协议将被中止.

TP选出这种情形的剩余三分之一位置,用类GHZ基测量$P_1^lP_2^lP_3^l$,并用Bell基测量$P_4^lP_5^l$. 如果TP对$P_1^lP_2^lP_3^l$的类GHZ基测量结果、对$P_4^lP_5^l$的Bell基测量结果都满足式(13),协议将被继续进行;否则,协议将被中止.

情形2 Alice选择了REFLECT模式,而Bob选择了MEASURE模式. 这种情形用于窃听检测. TP用Z基分别测量P_1^l和$P_3^lP_5^l$,并用Bell基测量$P_2^lP_4^l$. TP要求Bob告知他对$P_3^lP_5^l$的Z基测量结果. 对于所有的1,TP判断自己对$P_3^lP_5^l$的Z基测量结果是否和Bob对$P_3^lP_5^l$的Z基测量结果一致;而且,TP判断自己对P_1^l的Z基测量结果、对$P_3^lP_5^l$的Z基测量结果和对$P_2^lP_4^l$的Bell基测量结果是否满足式(16). 如果以上都满足,协议将被继续进行;否则,协议将被中止.

情形3 Alice选择了MEASURE模式,而Bob选择了REFLECT模式. 这种情形用于窃听检测. TP用Z基分别测量P_1^l和$P_2^lP_4^l$,并用Bell基测量$P_3^lP_5^l$. TP要求Alice告知她对$P_2^lP_4^l$的Z基测量结果. 对于所有的1,TP判断自己对$P_2^lP_4^l$的Z基测量结果是否和Alice对$P_2^lP_4^l$的Z基测量结果一致;而且,TP判断自己对P_1^l的Z基测量结果、对$P_2^lP_4^l$的Z基测量结果和对$P_3^lP_5^l$的Bell基测量结果是否满足式(15). 如果以上都满足,协议将被继续进行;否则,协议将被中止.

情形4 Alice和Bob都选择了MEASURE模式. TP用Z基分别测量P_1^l、$P_2^lP_4^l$和$P_3^lP_5^l$. 这种情形用于窃听检测和隐私比较. TP选择这种情形一半的粒子用于窃听检测,并将选中的位置告诉Alice和Bob. TP要求Alice告知她对所选中的$P_2^lP_4^l$的Z基测量结果,并且要求Bob告知他对所选中的$P_3^lP_5^l$的Z基测量结果. 对于所选中的位置,TP判断自己对$P_2^lP_4^l$的Z基测量结果是否和

Alice对$P_2^lP_4^l$的Z基测量结果一致,并且判断自己对$P_3^lP_5^l$的Z基测量结果是否和Bob对$P_3^lP_5^l$的Z基测量结果一致;而且,TP判断自己对所选中的P_1^l的Z基测量结果、对所选中的$P_2^lP_4^l$的Z基测量结果和对所选中的$P_3^lP_5^l$的Z基测量结果是否满足式(14). 如果以上都满足,协议将被继续进行;否则,协议将被中止.

步骤5　TP判断情形4的剩余位置的个数是否大于等于L. 如果大于L,协议将被继续进行;否则,协议将被中止并重新开始.

步骤6　Alice利用情形4的剩余前L个位置根据以下规则产生序列$K_A=(K_A^0,K_A^1,\cdots,K_A^{L-1})$:如果$C_A^i$为00或11,那么$K_A^i=0$;如果$C_A^i$为01或10,那么$K_A^i=1$. 这里,$i=0,1,\cdots,L-1$. 然后,Alice计算

$$R_A^i=M_A^i\oplus K_A^i\oplus K_{AB}^i \tag{18}$$

其中,符号$\oplus$表示进行异或操作. 最后,Alice通过认证经典信道将序列R_A发送给TP,其中$R_A=(R_A^0,R_A^1,\cdots,R_A^{L-1})$.

Bob利用情形4的剩余前L个位置根据以下规则产生序列$K_B=(K_B^0,K_B^1,\cdots,K_B^{L-1})$:如果$C_B^i$为00或11,那么$K_B^i=0$;如果$C_B^i$为01或10,那么$K_B^i=1$. 这里,$i=0,1,\cdots,L-1$. 然后,Bob计算:

$$R_B^i=M_B^i\oplus K_B^i\oplus K_{AB}^i \tag{19}$$

最后,Bob通过认证经典信道将序列R_B发送给TP,其中,$R_B=(R_B^0,R_B^1,\cdots,R_B^{L-1})$.

步骤7　TP计算:

$$T^i=R_A^i\oplus R_B^i\oplus\left(K_C^i\oplus 1\right) \tag{20}$$

其中,$K_C^i\in\{0,1\}$为TP对情形4的剩余前L个位置中P_1^i的测量结果所对应的经典比特,$i=0,1,\cdots,L-1$. 如果TP发现对于某个i存在$T^i\neq 0$,那么她将得出$M_A\neq M_B$;反之,她将得出$M_A=M_B$. 最后,TP向Alice和Bob公布最终的比较结果.

3　正确性分析

根据式(14),可以轻易得到$K_A^i\oplus K_B^i\oplus K_C^i=1$. 因此,将式(18)和式(19)代入式(20)可以得到

$$\begin{aligned}T^i&=R_A^i\oplus R_B^i\oplus\left(K_C^i\oplus 1\right)\\&=\left(M_A^i\oplus K_A^i\oplus K_{AB}^i\right)\oplus\left(M_B^i\oplus K_B^i\oplus K_{AB}^i\right)\oplus\left(K_C^i\oplus 1\right)\\&=M_A^i\oplus K_A^i\oplus M_B^i\oplus K_B^i\oplus K_C^i\oplus 1\\&=M_A^i\oplus M_B^i\end{aligned} \tag{21}$$

显然,如果$T^i\neq 0$,那么将有$M_A^i\neq M_B^i$. 因此,所提出的SQPC协议的输出是正确的.

4　针对外部窃听者的鲁棒性

文献[3]将半量子密码协议针对外部窃听者的攻击的鲁棒性分为完全鲁棒、部分鲁棒和完全非鲁棒三类. 接下来本文将证明所提出的SQPC协议针对外部窃听者的攻击具有完全鲁棒性.

外部窃听者Eve利用两个酉操作U_E和U_F发起如图1所示的攻击. 具体来说,Eve将U_E作用在TP发送给Alice的S_A的粒子、TP发送给Bob的S_B的粒子以及自己的辅助粒子$|\xi\rangle$,然后将U_F作用在Alice发送给TP的粒子、Bob发送给TP的粒子以及自己的辅助粒子. 这里,U_E和U_F共享一个初始状态为$|\xi\rangle$的共同探测空间. 根据定理1及其证明可知,为了在步骤4中不引入错误,Eve无法获得关于C_A或C_B的任何有用信息.

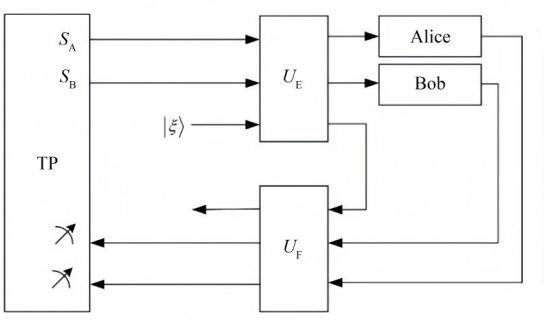


图1　Eve的纠缠-测量攻击

定理1　假设Eve将U_E作用在TP发送给Alice的S_A的粒子、TP发送给Bob的S_B的粒子以及自己的辅助粒子$|\xi\rangle$,然后将U_F作用在Alice发送给TP的粒子、Bob发送给TP的粒子以及自己的辅助粒子. 为了在步骤4中不引入错误,Eve的探测态的最终状态不仅要独立于Alice、Bob和TP的操作,而且还要独立于她们的测量结果. 因此,Eve无法获得关于C_A或C_B的任何有用信息.

证明　U_E对状态$|0\rangle$和$|1\rangle$的影响可被描述为

$$U_E\left(|0\rangle|\xi\rangle_E\right)=\beta_{00}|0\rangle|\xi_{00}\rangle+\beta_{01}|1\rangle|\xi_{01}\rangle \tag{22}$$

$$U_E\left(|1\rangle|\xi\rangle_E\right)=\beta_{10}|0\rangle|\xi_{10}\rangle+\beta_{11}|1\rangle|\xi_{11}\rangle \tag{23}$$

其中$|\xi_{00}\rangle$、$|\xi_{01}\rangle$、$|\xi_{10}\rangle$和$|\xi_{11}\rangle$是Eve的探测态,$|\beta_{00}|^2+|\beta_{01}|=1$且$|\beta_{10}|^2+|\beta_{11}|^2=1$.

根据Stinespring扩张定理,在Eve执行U_E后,复合系统的全局状态为

$$\begin{aligned}&U_E\left(|\vartheta_1\rangle_{123}\otimes|\phi^+\rangle_{45}\otimes|\xi\rangle_E\right)\\&=U_E\left[\begin{array}{l}\frac{1}{2}\left(|001\rangle+|010\rangle+|100\rangle+|111\rangle\right)_{123}\\\otimes\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)_{45}\otimes|\xi\rangle_E\end{array}\right]\\&=\frac{1}{2\sqrt{2}}\Big[|0\rangle_1\left(\beta_{00}|0\rangle_2|\xi_{00}\rangle+\beta_{01}|1\rangle_2|\xi_{01}\rangle\right)\\&\quad\cdot\left(\beta_{00}|0\rangle_4|\xi_{00}\rangle+\beta_{01}|1\rangle_4|\xi_{01}\rangle\right)\\&\quad\cdot\left(\beta_{10}|0\rangle_3|\xi_{10}\rangle+\beta_{11}|1\rangle_3|\xi_{11}\rangle\right)\end{aligned}$$

$$\cdot\left(\beta_{00}|0\rangle_5|\xi_{00}\rangle+\beta_{01}|1\rangle_5|\xi_{01}\rangle\right)$$
$$+|0\rangle_1\left(\beta_{10}|0\rangle_2|\xi_{10}\rangle+\beta_{11}|1\rangle_2|\xi_{11}\rangle\right)$$
$$\cdot\left(\beta_{00}|0\rangle_4|\xi_{00}\rangle+\beta_{01}|1\rangle_4|\xi_{01}\rangle\right)$$
$$+|0\rangle_1\left(\beta_{10}|0\rangle_2|\xi_{10}\rangle+\beta_{11}|1\rangle_2|\xi_{11}\rangle\right)$$
$$\cdot\left(\beta_{00}|0\rangle_4|\xi_{00}\rangle+\beta_{01}|1\rangle_4|\xi_{01}\rangle\right)$$
$$\cdot\left(\beta_{00}|0\rangle_3|\xi_{00}\rangle+\beta_{01}|1\rangle_3|\xi_{01}\rangle\right)$$
$$\cdot\left(\beta_{00}|0\rangle_5|\xi_{00}\rangle+\beta_{01}|1\rangle_5|\xi_{01}\rangle\right)$$
$$+|0\rangle_1\left(\beta_{00}|0\rangle_2|\xi_{00}\rangle+\beta_{01}|1\rangle_2|\xi_{01}\rangle\right)$$
$$\cdot\left(\beta_{10}|0\rangle_4|\xi_{10}\rangle+\beta_{11}|1\rangle_4|\xi_{11}\rangle\right)$$
$$\cdot\left(\beta_{10}|0\rangle_3|\xi_{10}\rangle+\beta_{11}|1\rangle_3|\xi_{11}\rangle\right)$$
$$\cdot\left(\beta_{10}|0\rangle_5|\xi_{10}\rangle+\beta_{11}|1\rangle_5|\xi_{11}\rangle\right)$$
$$+|0\rangle_1\left(\beta_{10}|0\rangle_2|\xi_{10}\rangle+\beta_{11}|1\rangle_2|\xi_{11}\rangle\right)$$
$$\cdot\left(\beta_{10}|0\rangle_4|\xi_{10}\rangle+\beta_{11}|1\rangle_{24}|\xi_{11}\rangle\right)$$
$$\cdot\left(\beta_{00}|0\rangle_3|\xi_{00}\rangle+\beta_{01}|1\rangle_3|\xi_{01}\rangle\right)$$
$$\cdot\left(\beta_{10}|0\rangle_5|\xi_{10}\rangle+\beta_{11}|1\rangle_5|\xi_{11}\rangle\right)$$
$$+|1\rangle_1\left(\beta_{00}|0\rangle_2|\xi_{00}\rangle+\beta_{01}|1\rangle_2|\xi_{01}\rangle\right)$$
$$\cdot\left(\beta_{00}|0\rangle_4|\xi_{00}\rangle+\beta_{01}|1\rangle_4|\xi_{01}\rangle\right)$$
$$\cdot\left(\beta_{00}|0\rangle_3|\xi_{00}\rangle+\beta_{01}|1\rangle_3|\xi_{01}\rangle\right)$$
$$\cdot\left(\beta_{00}|0\rangle_5|\xi_{00}\rangle+\beta_{01}|1\rangle_5|\xi_{01}\rangle\right)$$
$$+|1\rangle_1\left(\beta_{00}|0\rangle_2|\xi_{00}\rangle+\beta_{01}|1\rangle_2|\xi_{01}\rangle\right)$$
$$\cdot\left(\beta_{00}|0\rangle_4|\xi_{00}\rangle+\beta_{11}|1\rangle_{54}|\xi_{11}\rangle\right)$$
$$\cdot\left(\beta_{00}|0\rangle_3|\xi_{00}\rangle+\beta_{01}|1\rangle_3|\xi_{01}\rangle\right)$$
$$\cdot\left(\beta_{10}|0\rangle_5|\xi_{10}\rangle+\beta_{11}|1\rangle_5|\xi_{11}\rangle\right)$$
$$+|1\rangle_1\left(\beta_{10}|0\rangle_2|\xi_{10}\rangle+\beta_{11}|1\rangle_2|\xi_{11}\rangle\right)$$
$$\cdot\left(\beta_{00}|0\rangle_4|\xi_{00}\rangle+\beta_{01}|1\rangle_4|\xi_{01}\rangle\right)$$
$$\cdot\left(\beta_{10}|0\rangle_3|\xi_{10}\rangle+\beta_{11}|1\rangle_3|\xi_{11}\rangle\right)$$
$$\cdot\left(\beta_{00}|0\rangle_5|\xi_{00}\rangle+\beta_{01}|1\rangle_5|\xi_{01}\rangle\right)$$
$$+|1\rangle_1\left(\beta_{10}|0\rangle_2|\xi_{10}\rangle+\beta_{11}|1\rangle_2|\xi_{11}\rangle\right)$$
$$\cdot\left(\beta_{10}|0\rangle_4|\xi_{10}\rangle+\beta_{11}|1\rangle_4|\xi_{11}\rangle\right)$$
$$\cdot\left(\beta_{10}|0\rangle_3|\xi_{10}\rangle+\beta_{11}|1\rangle_3|\xi_{11}\rangle\right)$$
$$\cdot\left(\beta_{10}|0\rangle_5|\xi_{10}\rangle+\beta_{11}|1\rangle_5|\xi_{11}\rangle\right)\Big]$$
$$=\frac{1}{2\sqrt{2}}\Big[|0\rangle_1\left(|00\rangle_{24}|00\rangle_{35}|E^0_{0000}\rangle+|00\rangle_{24}|01\rangle_{35}|E^0_{0001}\rangle\right.$$
$$+|00\rangle_{24}|10\rangle_{35}|E^0_{0010}\rangle+|00\rangle_{24}|11\rangle_{35}|E^0_{0011}\rangle$$
$$+|01\rangle_{24}|00\rangle_{35}|E^0_{0100}\rangle+|01\rangle_{24}|01\rangle_{35}|E^0_{0101}\rangle$$
$$+|01\rangle_{24}|10\rangle_{35}|E^0_{0110}\rangle+|01\rangle_{24}|11\rangle_{35}|E^0_{0111}\rangle$$
$$+|10\rangle_{24}|00\rangle_{35}|E^0_{1000}\rangle+|10\rangle_{24}|01\rangle_{35}|E^0_{1001}\rangle$$
$$+|10\rangle_{24}|10\rangle_{35}|E^0_{1010}\rangle+|10\rangle_{24}|11\rangle_{35}|E^0_{1011}\rangle$$
$$+|11\rangle_{24}|00\rangle_{35}|E^0_{1100}\rangle+|11\rangle_{24}|01\rangle_{35}|E^0_{1101}\rangle$$
$$\left.+|11\rangle_{24}|10\rangle_{35}|E^0_{1110}\rangle+|11\rangle_{24}|11\rangle_{35}|E^0_{1111}\rangle\right)$$
$$+|1\rangle_1\left(|00\rangle_{24}|00\rangle_{35}|E^1_{0000}\rangle+|00\rangle_{24}|01\rangle_{35}|E^1_{0001}\rangle\right.$$
$$+|00\rangle_{24}|10\rangle_{35}|E^1_{0010}\rangle+|00\rangle_{24}|11\rangle_{35}|E^1_{0011}\rangle$$
$$+|01\rangle_{24}|00\rangle_{35}|E^1_{0100}\rangle+|01\rangle_{24}|01\rangle_{35}|E^1_{0101}\rangle$$
$$+|01\rangle_{24}|10\rangle_{35}|E^1_{0110}\rangle+|01\rangle_{24}|11\rangle_{35}|E^1_{0111}\rangle$$
$$+|10\rangle_{24}|00\rangle_{35}|E^1_{1000}\rangle+|10\rangle_{24}|01\rangle_{35}|E^1_{1001}\rangle$$
$$+|10\rangle_{24}|10\rangle_{35}|E^1_{1010}\rangle+|10\rangle_{24}|11\rangle_{35}|E^1_{1011}\rangle$$
$$+|11\rangle_{24}|00\rangle_{35}|E^1_{1100}\rangle+|11\rangle_{24}|01\rangle_{35}|E^1_{1101}\rangle$$
$$\left.+|11\rangle_{24}|10\rangle_{35}|E^1_{1110}\rangle+|11\rangle_{24}|11\rangle_{35}|E^1_{1111}\rangle\right)\Big] \tag{24}$$

当 Alice 收到 TP 发送的 S_A 时，她随机选择 REFLECT 模式或 MEASURE 模式；当 Bob 收到 TP 发送的 S_B 时，他随机选择 REFLECT 模式或 MEASURE 模式. 然后，Eve 对 Alice 和 Bob 返回给 TP 的粒子以及自己的辅助粒子执行 U_F.

（1）考虑 Alice 和 Bob 都选择 MEASURE 模式的情况. 为了使 Eve 在步骤 4 中不被发现，TP 对所选中的 P_1^l 的 Z 基测量结果、Alice 对所选中的 $P_2^lP_4^l$ 的 Z 基测量结果和 Bob 对所选中的 $P_3^lP_5^l$ 的 Z 基测量结果应满足式(14)，所以应当存在：

$$\begin{aligned}|E^0_{0000}\rangle&=|E^0_{0001}\rangle=|E^0_{0011}\rangle=|E^0_{0100}\rangle=|E^0_{0101}\rangle\\&=|E^0_{0110}\rangle=|E^0_{1001}\rangle=|E^0_{1010}\rangle=|E^0_{1011}\rangle\\&=|E^0_{1100}\rangle=|E^0_{1110}\rangle=|E^0_{1111}\rangle=0\end{aligned} \tag{25}$$

和

$$\begin{aligned}|E^1_{0001}\rangle&=|E^1_{0010}\rangle=|E^1_{0011}\rangle=|E^1_{0100}\rangle=|E^1_{0110}\rangle\\&=|E^1_{0111}\rangle=|E^1_{1000}\rangle=|E^1_{1001}\rangle=|E^1_{1011}\rangle\\&=|E^1_{1100}\rangle=|E^1_{1101}\rangle=|E^1_{1110}\rangle=0\end{aligned} \tag{26}$$

而且，TP 对 $P_2^lP_4^l$ 的 Z 基测量结果应和 Alice 对 $P_2^lP_4^l$ 的 Z 基测量结果一致，TP 对 $P_3^lP_5^l$ 的 Z 基测量结果应和 Bob 对 $P_3^lP_5^l$ 的 Z 基测量结果一致，所以应当存在

$$U_F\left(|0\rangle_1|00\rangle_{24}|10\rangle_{35}|E^0_{0010}\rangle\right)=|0\rangle_1|00\rangle_{24}|10\rangle_{35}|F^0_{0010}\rangle \tag{27}$$

$$U_F\left(|0\rangle_1|01\rangle_{24}|11\rangle_{35}|E^0_{0111}\rangle\right)=|0\rangle_1|01\rangle_{24}|11\rangle_{35}|F^0_{0111}\rangle \tag{28}$$

$$U_{\mathrm{F}}\left(|0\rangle_1|10\rangle_{24}|00\rangle_{35}|E^0_{1000}\rangle\right)=|0\rangle_1|10\rangle_{24}|00\rangle_{35}|F^0_{1000}\rangle \tag{29}$$

$$U_{\mathrm{F}}\left(|0\rangle_1|11\rangle_{24}|01\rangle_{35}|E^0_{1101}\rangle\right)=|0\rangle_1|11\rangle_{24}|01\rangle_{35}|F^0_{1101}\rangle \tag{30}$$

$$U_{\mathrm{F}}\left(|1\rangle_1|00\rangle_{24}|00\rangle_{35}|E^1_{0000}\rangle\right)=|1\rangle_1|00\rangle_{24}|00\rangle_{35}|F^1_{0000}\rangle \tag{31}$$

$$U_{\mathrm{F}}\left(|1\rangle_1|01\rangle_{24}|01\rangle_{35}|E^1_{0101}\rangle\right)=|1\rangle_1|01\rangle_{24}|01\rangle_{35}|F^1_{0101}\rangle \tag{32}$$

$$U_{\mathrm{F}}\left(|1\rangle_1|10\rangle_{24}|10\rangle_{35}|E^1_{1010}\rangle\right)=|1\rangle_1|10\rangle_{24}|10\rangle_{35}|F^1_{1010}\rangle \tag{33}$$

$$U_{\mathrm{F}}\left(|1\rangle_1|11\rangle_{24}|11\rangle_{35}|E^1_{1111}\rangle\right)=|1\rangle_1|11\rangle_{24}|11\rangle_{35}|F^1_{1111}\rangle \tag{34}$$

(2)考虑 Alice 选择 MEASURE 模式且 Bob 选择 REFLECT模式的情况. 当Alice对$P_2^lP_4^l$的Z基测量结果为$|00\rangle_{24}$时,式(24)的复合系统的状态被演化成

$$\begin{aligned}&|0\rangle_1|00\rangle_{24}|00\rangle_{35}|E^0_{0000}\rangle+|0\rangle_1|00\rangle_{24}|01\rangle_{35}|E^0_{0001}\rangle\\&+|0\rangle_1|00\rangle_{24}|10\rangle_{35}|E^0_{0010}\rangle+|0\rangle_1|00\rangle_{24}|11\rangle_{35}|E^0_{0011}\rangle\\&+|1\rangle_1|00\rangle_{24}|00\rangle_{35}|E^1_{0000}\rangle+|1\rangle_1|00\rangle_{24}|01\rangle_{35}|E^1_{0001}\rangle\\&+|1\rangle_1|00\rangle_{24}|10\rangle_{35}|E^1_{0010}\rangle+|1\rangle_1|00\rangle_{24}|11\rangle_{35}|E^1_{0011}\rangle;\end{aligned}$$

当Alice对$P_2^lP_4^l$的Z基测量结果为$|01\rangle_{24}$时,式(24)的复合系统的状态被演化成

$$\begin{aligned}&|0\rangle_1|01\rangle_{24}|00\rangle_{35}|E^0_{0100}\rangle+|0\rangle_1|01\rangle_{24}|01\rangle_{35}|E^0_{0101}\rangle\\&+|0\rangle_1|01\rangle_{24}|10\rangle_{35}|E^0_{0110}\rangle+|0\rangle_1|01\rangle_{24}|11\rangle_{35}|E^0_{0111}\rangle\\&+|1\rangle_1|01\rangle_{24}|00\rangle_{35}|E^1_{0100}\rangle+|1\rangle_1|01\rangle_{24}|01\rangle_{35}|E^1_{0101}\rangle\\&+|1\rangle_1|01\rangle_{24}|10\rangle_{35}|E^1_{0110}\rangle+|1\rangle_1|01\rangle_{24}|11\rangle_{35}|E^1_{0111}\rangle;\end{aligned}$$

当Alice对$P_2^lP_4^l$的Z基测量结果为$|10\rangle_{24}$时,式(24)的复合系统的状态被演化成

$$\begin{aligned}&|0\rangle_1|10\rangle_{24}|00\rangle_{35}|E^0_{1000}\rangle+|0\rangle_1|10\rangle_{24}|01\rangle_{35}|E^0_{1001}\rangle\\&+|0\rangle_1|10\rangle_{24}|10\rangle_{35}|E^0_{1010}\rangle+|0\rangle_1|10\rangle_{24}|11\rangle_{35}|E^0_{1011}\rangle\\&+|1\rangle_1|10\rangle_{24}|00\rangle_{35}|E^1_{1000}\rangle+|1\rangle_1|10\rangle_{24}|01\rangle_{35}|E^1_{1001}\rangle\\&+|1\rangle_1|10\rangle_{24}|10\rangle_{35}|E^1_{1010}\rangle+|1\rangle_1|10\rangle_{24}|11\rangle_{35}|E^1_{1011}\rangle;\end{aligned}$$

当Alice对$P_2^lP_4^l$的Z基测量结果为$|11\rangle_{24}$时,式(24)的复合系统的状态被演化成

$$\begin{aligned}&|0\rangle_1|11\rangle_{24}|00\rangle_{35}|E^0_{1100}\rangle+|0\rangle_1|11\rangle_{24}|01\rangle_{35}|E^0_{1101}\rangle\\&+|0\rangle_1|11\rangle_{24}|10\rangle_{35}|E^0_{1110}\rangle+|0\rangle_1|11\rangle_{24}|11\rangle_{35}|E^0_{1111}\rangle\\&+|1\rangle_1|11\rangle_{24}|00\rangle_{35}|E^1_{1100}\rangle+|1\rangle_1|11\rangle_{24}|01\rangle_{35}|E^1_{1101}\rangle\\&+|1\rangle_1|11\rangle_{24}|10\rangle_{35}|E^1_{1110}\rangle+|1\rangle_1|11\rangle_{24}|11\rangle_{35}|E^1_{1111}\rangle.\end{aligned}$$

首先,考虑Alice对$P_2^lP_4^l$的Z基测量结果为$|00\rangle_{24}$的情况. 在Eve对Alice和Bob返回给TP的粒子以及自己的辅助粒子执行U_F后,根据式(25)、式(26)、式(27)和式(31),复合系统的状态被演化为

$$\begin{aligned}&U_{\mathrm{F}}\left(|0\rangle_1|00\rangle_{24}|00\rangle_{35}|E^0_{0000}\rangle+|0\rangle_1|00\rangle_{24}|01\rangle_{35}|E^0_{0001}\rangle\right.\\&+|0\rangle_1|00\rangle_{24}|10\rangle_{35}|E^0_{0010}\rangle+|0\rangle_1|00\rangle_{24}|11\rangle_{35}|E^0_{0011}\rangle\\&+|1\rangle_1|00\rangle_{24}|00\rangle_{35}|E^1_{0000}\rangle+|1\rangle_1|00\rangle_{24}|01\rangle_{35}|E^1_{0001}\rangle\\&\left.+|1\rangle_1|00\rangle_{24}|10\rangle_{35}|E^1_{0010}\rangle+|1\rangle_1|00\rangle_{24}|11\rangle_{35}|E^1_{0011}\rangle\right)\\&=U_{\mathrm{F}}\left(|0\rangle_1|00\rangle_{24}|10\rangle_{35}|E^0_{0010}\rangle+|1\rangle_1|00\rangle_{24}|00\rangle_{35}|E^0_{0000}\rangle\right)\\&=\frac{1}{\sqrt{2}}\Big[|0\rangle_1|00\rangle_{24}\left(|\phi^+\rangle_{35}-|\phi^-\rangle_{35}\right)|F^0_{0010}\rangle\\&+|1\rangle_1|00\rangle_{24}\left(|\phi^+\rangle_{35}+|\phi^-\rangle_{35}\right)|F^1_{0000}\rangle\Big]\end{aligned} \tag{35}$$

为了使Eve在步骤4中不被检测到,TP对$P_2^lP_4^l$的Z基测量结果应和Alice对$P_2^lP_4^l$的Z基测量结果一致;而且,TP对P_1^l的基测量结果、对$P_2^lP_4^l$的Z基测量结果和对$P_3^lP_5^l$的Bell基测量结果应满足式(15). 根据式(35),这些要求自然满足.

第二,考虑Alice对$P_2^lP_4^l$的Z基测量结果为$|01\rangle_{24}$的情况. 在Eve对Alice和Bob返回给TP的粒子以及自己的辅助粒子执行U_F后,根据式(25)、式(26)、式(28)和式(32),复合系统的状态被演化为

$$\begin{aligned}&U_{\mathrm{F}}\left(|0\rangle_1|01\rangle_{24}|00\rangle_{35}|E^0_{0100}\rangle+|0\rangle_1|01\rangle_{24}|01\rangle_{35}|E^0_{0101}\rangle\right.\\&+|0\rangle_1|01\rangle_{24}|10\rangle_{35}|E^0_{0110}\rangle+|0\rangle_1|01\rangle_{24}|11\rangle_{35}|E^0_{0111}\rangle\\&+|1\rangle_1|01\rangle_{24}|00\rangle_{35}|E^1_{0100}\rangle+|1\rangle_1|01\rangle_{24}|01\rangle_{35}|E^1_{0101}\rangle\\&\left.+|1\rangle_1|01\rangle_{24}|10\rangle_{35}|E^1_{0110}\rangle+|1\rangle_1|01\rangle_{24}|11\rangle_{35}|E^1_{0111}\rangle\right)\\&=U_{\mathrm{F}}\left(|0\rangle_1|01\rangle_{24}|11\rangle_{35}|E^0_{0111}\rangle+|1\rangle_1|01\rangle_{24}|01\rangle_{35}|E^1_{0101}\rangle\right)\\&=\frac{1}{\sqrt{2}}\Big[|0\rangle_1|01\rangle_{24}\left(|\phi^+\rangle_{35}-|\phi^-\rangle_{35}\right)|F^0_{0111}\rangle\\&+|1\rangle_1|01\rangle_{24}\left(|\phi^+\rangle_{35}+|\phi^-\rangle_{35}\right)|F^1_{0101}\rangle\Big]\end{aligned} \tag{36}$$

为了使Eve在步骤4中不被检测到,TP对$P_2^lP_4^l$的Z基测量结果应和Alice对$P_2^lP_4^l$的Z基测量结果一致;而且,TP对P_1^l的Z基测量结果、对$P_2^lP_4^l$的Z基测量结果和对$P_3^lP_5^l$的Bell基测量结果应满足式(15). 根据式(36),这些要求自然满足.

第三,考虑Alice对$P_2^lP_4^l$的Z基测量结果为$|10\rangle_{24}$的情况. 在Eve对Alice和Bob返回给TP的粒子以及自己的辅助粒子执行U_F后,根据式(25)、式(26)、式(29)和(33),复合系统的状态被演化为

$$\begin{aligned}&U_{\mathrm{F}}\left(|0\rangle_1|10\rangle_{24}|00\rangle_{35}|E^0_{1000}\rangle+|0\rangle_1|10\rangle_{24}|01\rangle_{35}|E^0_{1001}\rangle\right.\\&+|0\rangle_1|10\rangle_{24}|10\rangle_{35}|E^0_{1010}\rangle+|0\rangle_1|10\rangle_{24}|11\rangle_{35}|E^0_{1011}\rangle\\&\left.+|1\rangle_1|10\rangle_{24}|00\rangle_{35}|E^1_{1000}\rangle+|1\rangle_1|10\rangle_{24}|01\rangle_{35}|E^1_{1001}\rangle\right.\end{aligned}$$

$$+|1\rangle_1|10\rangle_{24}|10\rangle_{35}|E^1_{1010}\rangle+|1\rangle_1|10\rangle_{24}|11\rangle_{35}|E^1_{1011}\rangle\big)$$
$$=U_{\mathrm{F}}\big(|0\rangle_1|10\rangle_{24}|00\rangle_{35}|E^0_{1000}\rangle+|1\rangle_1|10\rangle_{24}|10\rangle_{35}|E^1_{1010}\rangle\big)$$
$$=\frac{1}{\sqrt{2}}\Big[|0\rangle_1|10\rangle_{24}\big(|\phi^+\rangle_{35}+|\phi^-\rangle_{35}\big)|F^0_{1000}\rangle$$
$$+|1\rangle_1|10\rangle_{24}\big(|\phi^+\rangle_{35}-|\phi^-\rangle_{35}\big)|F^1_{1010}\rangle\Big] \tag{37}$$

为了使Eve在步骤4中不被检测到，TP对$P_2^lP_4^l$的Z基测量结果应和Alice对$P_2^lP_4^l$的Z基测量结果一致；而且，TP对P_1^l的Z基测量结果、对$P_2^lP_4^l$的Z基测量结果和对$P_3^lP_5^l$的Bell基测量结果应满足式(15). 根据式(37)，这些要求自然满足.

第四，考虑Alice对$P_2^lP_4^l$的Z基测量结果为$|11\rangle_{24}$的情况. 在Eve对Alice和Bob返回给TP的粒子以及自己的辅助粒子执行U_F后，根据式(25)、式(26)、式(30)和式(34)，复合系统的状态被演化为

$$U_{\mathrm{F}}\big(|0\rangle_1|11\rangle_{24}|00\rangle_{35}|E^0_{1100}\rangle+|0\rangle_1|11\rangle_{24}|01\rangle_{35}||E^0_{1101}\rangle$$
$$+|0\rangle_1|11\rangle_{24}|10\rangle_{35}|E^0_{1110}\rangle+|0\rangle_1|11\rangle_{24}|11\rangle_{35}||E^0_{1111}\rangle$$
$$+|1\rangle_1|11\rangle_{24}|00\rangle_{35}|E^1_{1100}\rangle+|1\rangle_1|11\rangle_{24}|01\rangle_{35}||E^1_{1101}\rangle$$
$$+|1\rangle_1|11\rangle_{24}|10\rangle_{35}|E^1_{1110}\rangle+|1\rangle_1|11\rangle_{24}|11\rangle_{35}||E^1_{1111}\rangle\big)$$
$$=U_{\mathrm{F}}\big(|0\rangle_1|11\rangle_{24}|01\rangle_{35}|E^0_{1101}\rangle+|1\rangle_1|11\rangle_{24}|11\rangle_{35}|E^1_{1101}\rangle\big)$$
$$=\frac{1}{\sqrt{2}}\Big[0\rangle_1|11\rangle_{24}\big(|\phi^+\rangle_{35}+|\phi^-\rangle_{35}\big)|F^0_{1101}\rangle$$
$$+|1\rangle_1|11\rangle_{24}\big(|\phi^+\rangle_{35}-|\phi^-\rangle_{35}\big)|F^1_{1111}\rangle\Big] \tag{38}$$

为了使Eve在步骤4中不被检测到，TP对$P_2^lP_4^l$的Z基测量结果应和Alice对$P_2^lP_4^l$的Z基测量结果一致；而且，TP对P_1^l的Z基测量结果、对$P_2^lP_4^l$的Z基测量结果和对$P_3^lP_5^l$的Bell基测量结果应满足式(15). 根据式(38)，这些要求自然满足.

(3) 考虑Alice选择REFLECT模式且Bob选择MEASURE模式的情况. 当Bob对$P_3^lP_5^l$的Z基测量结果为$|00\rangle_{35}$时，式(24)的复合系统的状态被演化成

$$|0\rangle_1|00\rangle_{24}|00\rangle_{35}|E^0_{0000}\rangle+|0\rangle_1|01\rangle_{24}|00\rangle_{35}|E^0_{0100}\rangle$$
$$+|0\rangle_1|10\rangle_{24}|00\rangle_{35}|E^0_{1000}\rangle+|0\rangle_1|11\rangle_{24}|00\rangle_{35}|E^0_{1100}\rangle$$
$$+|1\rangle_1|00\rangle_{24}|00\rangle_{35}|E^1_{0000}\rangle+|1\rangle_1|01\rangle_{24}|00\rangle_{35}|E^1_{0100}\rangle$$
$$+|1\rangle_1|10\rangle_{24}|00\rangle_{35}|E^1_{1000}\rangle+|1\rangle_1|11\rangle_{24}|00\rangle_{35}|E^1_{1100}\rangle;$$

当Bob对$P_3^lP_5^l$的Z基测量结果为$|01\rangle_{35}$时，式(24)的复合系统的状态被演化成

$$|0\rangle_1|00\rangle_{24}|01\rangle_{35}|E^0_{0001}\rangle+|0\rangle_1|01\rangle_{24}|01\rangle_{35}|E^0_{0101}\rangle$$
$$+|0\rangle_1|10\rangle_{24}|01\rangle_{35}|E^0_{1001}\rangle+|0\rangle_1|11\rangle_{24}|01\rangle_{35}|E^0_{1101}\rangle$$
$$+|1\rangle_1|00\rangle_{24}|01\rangle_{35}|E^1_{0001}\rangle+|1\rangle_1|01\rangle_{24}|01\rangle_{35}|E^1_{0101}\rangle$$
$$+|1\rangle_1|10\rangle_{24}|01\rangle_{35}|E^1_{1001}\rangle+|1\rangle_1|11\rangle_{24}|01\rangle_{35}|E^1_{1101}\rangle;$$

当Bob对$P_3^lP_5^l$的Z基测量结果为$|10\rangle_{35}$时，式(24)的复合系统的状态被演化成

$$|0\rangle_1|00\rangle_{24}|10\rangle_{35}|E^0_{0010}\rangle+|0\rangle_1|01\rangle_{24}|10\rangle_{35}|E^0_{0110}\rangle$$
$$+|0\rangle_1|10\rangle_{24}|10\rangle_{35}|E^0_{1010}\rangle+|0\rangle_1|11\rangle_{24}|10\rangle_{35}|E^0_{1110}\rangle$$
$$+|1\rangle_1|00\rangle_{24}|10\rangle_{35}|E^1_{0010}\rangle+|1\rangle_1|01\rangle_{24}|10\rangle_{35}|E^1_{0110}\rangle$$
$$+|1\rangle_1|10\rangle_{24}|10\rangle_{35}|E^1_{1010}\rangle+|1\rangle_1|11\rangle_{24}|10\rangle_{35}|E^1_{1110}\rangle;$$

当Bob对$P_3^lP_5^l$的Z基测量结果为$|11\rangle_{35}$时，式(24)的复合系统的状态被演化成

$$|0\rangle_1|00\rangle_{24}|11\rangle_{35}|E^0_{0011}\rangle+|0\rangle_1|01\rangle_{24}|11\rangle_{35}|E^0_{0111}\rangle$$
$$+|0\rangle_1|10\rangle_{24}|11\rangle_{35}|E^0_{1011}\rangle+|0\rangle_1|11\rangle_{24}|11\rangle_{35}|E^0_{1111}\rangle$$
$$+|1\rangle_1|00\rangle_{24}|11\rangle_{35}|E^1_{0011}\rangle+|1\rangle_1|01\rangle_{24}|11\rangle_{35}|E^1_{0111}\rangle$$
$$+|1\rangle_1|10\rangle_{24}|11\rangle_{35}|E^1_{1011}\rangle+|1\rangle_1|11\rangle_{24}|11\rangle_{35}|E^1_{1111}\rangle.$$

第一，考虑Bob对$P_3^lP_5^l$的Z基测量结果为$|00\rangle_{35}$的情况. 在Eve对Alice和Bob返回给TP的粒子以及自己的辅助粒子执行U_F后，根据式(25)、式(26)、式(29)和式(31)，复合系统的状态被演化为

$$U_{\mathrm{F}}\big(|0\rangle_1|00\rangle_{24}|00\rangle_{35}|E^0_{0000}\rangle+|0\rangle_1|01\rangle_{24}|00\rangle_{35}|E^0_{0100}\rangle$$
$$+|0\rangle_1|10\rangle_{24}|00\rangle_{35}|E^0_{1000}\rangle+|0\rangle_1|11\rangle_{24}|00\rangle_{35}|E^0_{1100}\rangle$$
$$+|1\rangle_1|00\rangle_{24}|00\rangle_{35}|E^1_{0000}\rangle+|1\rangle_1|01\rangle_{24}|00\rangle_{35}|E^1_{0100}\rangle$$
$$+|1\rangle_1|10\rangle_{24}|00\rangle_{35}|E^1_{1000}\rangle+|1\rangle_1|11\rangle_{24}|00\rangle_{35}|E^1_{1100}\rangle\big)$$
$$=U_{\mathrm{F}}\big(|0\rangle_1|10\rangle_{24}|00\rangle_{35}|E^0_{1000}\rangle+|1\rangle_1|00\rangle_{24}|00\rangle_{35}|E^1_{0000}\rangle\big)$$
$$=\frac{1}{\sqrt{2}}\Big[|0\rangle_1\big(|\phi^+\rangle_{24}-|\phi^-\rangle_{24}\big)|00\rangle_{35}|F^0_{1000}\rangle$$
$$+|1\rangle_1\big(|\phi^+\rangle_{24}+|\phi^-\rangle_{24}\big)|00\rangle_{35}|F^1_{0000}\rangle\Big] \tag{39}$$

为了使Eve在步骤4中不被检测到，TP对$P_3^lP_5^l$的Z基测量结果应和Bob对$P_3^lP_5^l$的Z基测量结果一致；而且，TP对P_1^l的Z基测量结果、对$P_3^lP_5^l$的Z基测量结果和对$P_2^lP_4^l$的Bell基测量结果应满足式(16). 根据式(39)，这些要求自然满足.

第二，考虑Bob对$P_3^lP_5^l$的Z基测量结果为$|01\rangle_{35}$的情况. 在Eve对Alice和Bob返回给TP的粒子以及自己的辅助粒子执行U_F后，根据式(25)、式(26)、式(30)和式(32)，复合系统的状态被演化为

$$U_{\mathrm{F}}\big(|0\rangle_1|00\rangle_{24}|01\rangle_{35}|E^0_{0001}\rangle+|0\rangle_1|01\rangle_{24}|01\rangle_{35}|E^0_{0101}\rangle$$
$$+|0\rangle_1|10\rangle_{24}|01\rangle_{35}|E^0_{1001}\rangle+|0\rangle_1|11\rangle_{24}|01\rangle_{35}|E^0_{1101}\rangle$$
$$+|1\rangle_1|00\rangle_{24}|01\rangle_{35}|E^1_{0001}\rangle+|1\rangle_1|01\rangle_{24}|01\rangle_{35}|E^1_{0101}\rangle$$
$$+|1\rangle_1|10\rangle_{24}|01\rangle_{35}|E^1_{1001}\rangle+|1\rangle_1|11\rangle_{24}|01\rangle_{35}|E^1_{1101}\rangle\big)$$
$$=U_{\mathrm{F}}\big(|0\rangle_1|11\rangle_{24}|01\rangle_{35}|E^0_{1101}\rangle+|1\rangle_1|01\rangle_{24}|01\rangle_{35}|E^1_{0101}\rangle\big)$$

$$=\frac{1}{\sqrt{2}}\Big[|0\rangle_1\Big(|\phi^+\rangle_{24}-|\phi^-\rangle_{24}\Big)|01\rangle_{35}|F^0_{1101}\rangle +|1\rangle_1\Big(|\phi^+\rangle_{24}+|\phi^-\rangle_{24}\Big)|01\rangle_{35}|F^1_{0101}\rangle\Big] \tag{40}$$

为了使Eve在步骤4中不被检测到,TP对$P_3^lP_5^l$的Z基测量结果应和Bob对$P_3^lP_5^l$的Z基测量结果一致;而且,TP对P_1^l的Z基测量结果、对$P_3^lP_5^l$的Z基测量结果和对$P_2^lP_4^l$的Bell基测量结果应满足式(16). 根据式(40),这些要求自然满足.

第三,考虑Bob对$P_3^lP_5^l$的Z基测量结果为$|10\rangle_{35}$的情况. 在Eve对Alice和Bob返回给TP的粒子以及自己的辅助粒子执行U_F后,根据式(25)、式(26)、式(27)和式(33),复合系统的状态被演化为

$$\begin{aligned}&U_F\Big(|0\rangle_1|00\rangle_{24}|10\rangle_{35}|E^0_{0010}\rangle+|0\rangle_1|01\rangle_{24}|10\rangle_{35}|E^0_{0110}\rangle\\&+|0\rangle_1|10\rangle_{24}|10\rangle_{35}|E^0_{1010}\rangle+|0\rangle_1|11\rangle_{24}|10\rangle_{35}|E^0_{1110}\rangle\\&+|1\rangle_1|00\rangle_{24}|10\rangle_{35}|E^1_{0010}\rangle+|1\rangle_1|01\rangle_{24}|10\rangle_{35}|E^1_{0110}\rangle\\&+|1\rangle_1|10\rangle_{24}|10\rangle_{35}|E^1_{1010}\rangle+|1\rangle_1|11\rangle_{24}|10\rangle_{35}|E^1_{1110}\rangle\Big)\\=&U_F\Big(|0\rangle_1|00\rangle_{24}|10\rangle_{35}|E^0_{0010}\rangle+|1\rangle_1|10\rangle_{24}|10\rangle_{35}|E^1_{1010}\rangle\Big)\\=&\frac{1}{\sqrt{2}}\Big[|0\rangle_1\Big(|\phi^+\rangle_{24}+|\phi^-\rangle_{24}\Big)|10\rangle_{35}|F^0_{0010}\rangle\\&+|1\rangle_1\Big(|\phi^+\rangle_{24}-|\phi^-\rangle_{24}\Big)|10\rangle_{35}|F^1_{1010}\rangle\Big]\end{aligned} \tag{41}$$

为了使Eve在步骤4中不被检测到,TP对$P_3^lP_5^l$的Z基测量结果应和Bob对$P_3^lP_5^l$的Z基测量结果一致;而且,TP对P_1^l的Z基测量结果、对$P_3^lP_5^l$的Z基测量结果和对$P_2^lP_4^l$的Bell基测量结果应满足式(16). 根据式(41),这些要求自然满足.

第四,考虑Bob对$P_3^lP_5^l$的Z基测量结果为$|11\rangle_{35}$的情况. 在Eve对Alice和Bob返回给TP的粒子以及自己的辅助粒子执行U_F后,根据式(25)、式(26)、式(28)和式(34),复合系统的状态被演化为

$$\begin{aligned}&U_F\Big(|0\rangle_1|00\rangle_{24}|11\rangle_{35}|E^0_{0011}\rangle+|0\rangle_1|01\rangle_{24}|11\rangle_{35}|E^0_{0111}\rangle\\&+|0\rangle_1|10\rangle_{24}|11\rangle_{35}|E^0_{1011}\rangle+|0\rangle_1|11\rangle_{24}|11\rangle_{35}|E^0_{1111}\rangle\\&+|1\rangle_1|00\rangle_{24}|11\rangle_{35}|E^1_{0011}\rangle+|1\rangle_1|01\rangle_{24}|11\rangle_{35}|E^1_{0111}\rangle\\&+|1\rangle_1|10\rangle_{24}|11\rangle_{35}|E^1_{1011}\rangle+|1\rangle_1|11\rangle_{24}|11\rangle_{35}|E^1_{1111}\rangle\Big)\\=&U_F\Big(|0\rangle_1|01\rangle_{24}|11\rangle_{35}|E^0_{0111}\rangle+|1\rangle_1|11\rangle_{24}|11\rangle_{35}|E^1_{1111}\rangle\Big)\\=&\frac{1}{\sqrt{2}}\Big[|0\rangle_1\Big(|\phi^+\rangle_{24}+|\phi^-\rangle_{24}\Big)|11\rangle_{35}|F^0_{0111}\rangle\\&+|1\rangle_1\Big(|\phi^+\rangle_{24}-|\phi^-\rangle_{24}\Big)|11\rangle_{35}|F^1_{1111}\rangle\Big]\end{aligned} \tag{42}$$

为了使Eve在步骤4中不被检测到,TP对$P_3^lP_5^l$的Z基测量结果应和Bob对$P_3^lP_5^l$的Z基测量结果一致;而且,TP对P_1^l的Z基测量结果、对$P_3^lP_5^l$的Z基测量结果和对$P_2^lP_4^l$的Bell基测量结果应满足式(16). 根据式(42),这些要求自然满足.

(4)考虑Alice和Bob都选择REFLECT模式的情况. 将式(25)和(26)代入式(24)得到:

$$\begin{aligned}&U_E\Big(|\vartheta_1\rangle_{123}\otimes|\phi^+\rangle_{45}\Big)\\=&\frac{1}{2\sqrt{2}}\Big(|0\rangle_1|00\rangle_{24}|10\rangle_{35}|E^0_{0010}\rangle+|0\rangle_1|01\rangle_{24}|11\rangle_{35}|E^0_{0111}\rangle\\&+|0\rangle_1|10\rangle_{24}|00\rangle_{35}|E^0_{1000}\rangle+|0\rangle_1|11\rangle_{24}|01\rangle_{35}|E^0_{1101}\rangle\\&+|1\rangle_1|00\rangle_{24}|00\rangle_{35}|E^1_{0000}\rangle+|1\rangle_1|01\rangle_{24}|01\rangle_{35}|E^1_{0101}\rangle\\&+|1\rangle_1|10\rangle_{24}|10\rangle_{35}|E^1_{1010}\rangle+|1\rangle_1|11\rangle_{24}|11\rangle_{35}|E^1_{1111}\rangle\Big)\end{aligned} \tag{43}$$

在Eve对Alice和Bob返回给TP的粒子以及自己的辅助粒子执行U_F后,根据式(27)~(34),复合系统的状态被演化为

$$\begin{aligned}&U_F\Big[U_E\Big(|\vartheta_1\rangle_{123}\otimes|\phi^+\rangle_{45}\Big)\Big]\\=&\frac{1}{2\sqrt{2}}U_F\Big(|0\rangle_1|00\rangle_{24}|10\rangle_{35}|E^0_{0010}\rangle\\&+|0\rangle_1|01\rangle_{24}|11\rangle_{35}|E^0_{0100}\rangle+|0\rangle_1|10\rangle_{24}|00\rangle_{35}|E^0_{1000}\rangle\\&+|0\rangle_1|11\rangle_{24}|01\rangle_{35}|E^0_{1101}\rangle+|1\rangle_1|00\rangle_{24}|00\rangle_{35}|E^1_{0000}\rangle\\&+|1\rangle_1|01\rangle_{24}|01\rangle_{35}|E^1_{0101}\rangle+|1\rangle_1|10\rangle_{24}|10\rangle_{35}|E^1_{1010}\rangle\\&+|1\rangle_1|11\rangle_{24}|11\rangle_{35}|E^1_{1111}\rangle\Big)\\=&\frac{1}{4\sqrt{2}}\Big[|0\rangle_1|\phi^+\rangle_{24}|\phi^+\rangle_{35}\Big(|F^0_{0010}\rangle+|F^0_{1101}\rangle\Big)\\&+|0\rangle_1|\phi^+\rangle_{24}|\phi^-\rangle_{35}\Big(|F^0_{1101}\rangle+|F^0_{0010}\rangle\Big)\\&+|0\rangle_1|\phi^-\rangle_{24}|\phi^+\rangle_{35}\Big(|F^0_{0010}\rangle+|F^0_{1101}\rangle\Big)\\&-|0\rangle_1|\phi^-\rangle_{24}|\phi^-\rangle_{35}\Big(|F^0_{1101}\rangle+|F^0_{0010}\rangle\Big)\\&+|0\rangle_1|\phi^+\rangle_{24}|\phi^+\rangle_{35}\Big(|F^0_{0111}\rangle+|F^0_{1000}\rangle\Big)\\&-|0\rangle_1|\phi^+\rangle_{24}|\phi^-\rangle_{35}\Big(|F^0_{0111}\rangle+|F^0_{1000}\rangle\Big)\\&+|0\rangle_1|\phi^-\rangle_{24}|\phi^+\rangle_{35}\Big(|F^0_{0111}\rangle+|F^0_{1000}\rangle\Big)\\&-|0\rangle_1|\phi^-\rangle_{24}|\phi^-\rangle_{35}\Big(|F^0_{0111}\rangle+|F^0_{1000}\rangle\Big)\\&+|1\rangle_1|\phi^+\rangle_{24}|\phi^+\rangle_{35}\Big(|F^1_{0000}\rangle+|F^1_{1111}\rangle\Big)\\&+|1\rangle_1|\phi^+\rangle_{24}|\phi^-\rangle_{35}\Big(|F^1_{0000}\rangle-|F^1_{1111}\rangle\Big)\\&+|1\rangle_1|\phi^-\rangle_{24}|\phi^+\rangle_{35}\Big(|F^1_{0000}\rangle-|F^1_{1111}\rangle\Big)\\&+|1\rangle_1|\phi^-\rangle_{24}|\phi^-\rangle_{35}\Big(|F^1_{0000}\rangle+|F^1_{1111}\rangle\Big)\\&+|1\rangle_1|\phi^+\rangle_{24}|\phi^+\rangle_{35}\Big(|F^1_{0101}\rangle+|F^1_{1010}\rangle\Big)\end{aligned}$$

$$+|1\rangle_1|\phi^+\rangle_{24}|\phi^-\rangle_{35}\left(|F^1_{0101}\rangle-|F^1_{1010}\rangle\right)$$
$$+|1\rangle_1|\phi^-\rangle_{24}|\phi^+\rangle_{35}\left(|F^1_{0101}\rangle-|F^1_{1010}\rangle\right)$$
$$+|1\rangle_1|\phi^-\rangle_{24}|\phi^-\rangle_{35}\left(|F^1_{0101}\rangle+|F^1_{1010}\rangle\right)\Big] \tag{44}$$

为了使Eve在步骤4中不被检测到，TP对P_1^l的Z基测量结果、对$P_2^lP_4^l$的Bell基测量结果和对$P_3^lP_5^l$的Bell基测量结果应满足式(17). 因此，根据式(17)和式(44)，应当存在：

$$\begin{aligned}&|F^0_{1101}\rangle=|F^0_{0010}\rangle,\ |F^0_{0111}\rangle=|F^0_{1000}\rangle,\\&|F^1_{0000}\rangle=|F^1_{1111}\rangle,\ |F^1_{0101}\rangle=|F^1_{1010}\rangle\end{aligned} \tag{45}$$

将式(45)代入式(44)可得：

$$\begin{aligned}&U_F\Big[U_E\left(|\vartheta_1\rangle_{123}\otimes|\phi^+\rangle_{45}\right)\Big]\\&=\frac{1}{4}\Big\{|001\rangle_{123}\Big[|\phi^+\rangle_{45}\left(|F^0_{0010}\rangle+|F^0_{0111}\rangle\right)\\&\quad+|\phi^-\rangle_{45}\left(|F^0_{0010}\rangle-|F^0_{0111}\rangle\right)\Big]\\&\quad+|010\rangle_{123}\Big[|\phi^+\rangle_{45}\left(|F^0_{0010}\rangle+|F^0_{0111}\rangle\right)\\&\quad+|\phi^-\rangle_{45}\left(|F^0_{0111}\rangle-|F^0_{0010}\rangle\right)\Big]\\&\quad+|100\rangle_{123}\Big[|\phi^+\rangle_{45}\left(|F^1_{0000}\rangle+|F^1_{0101}\rangle\right)\\&\quad+|\phi^-\rangle_{45}\left(|F^1_{0000}\rangle-|F^1_{0101}\rangle\right)\Big]\\&\quad+|111\rangle_{123}\Big[|\phi^+\rangle_{45}\left(|F^1_{0000}\rangle+|F^1_{0101}\rangle\right)\\&\quad+|\phi^-\rangle_{45}\left(|F^1_{0101}\rangle-|F^1_{0000}\rangle\right)\Big]\Big\}\end{aligned} \tag{46}$$

为了使Eve在步骤4中不被检测到，TP对$P_1^lP_2^lP_3^l$的Z基测量结果、对$P_4^lP_5^l$的Bell基测量结果都应满足式(13). 因此，根据式(13)和式(46)，应当存在：

$$|F^0_{0010}\rangle=|F^0_{0111}\rangle,\ |F^1_{0000}\rangle=|F^1_{0101}\rangle \tag{47}$$

将式(47)代入式(46)可得到

$$\begin{aligned}&U_F\Big[U_E\left(|\vartheta_1\rangle_{123}\otimes|\phi^+\rangle_{45}\right)\Big]\\&=\frac{1}{2}\Big(|001\rangle_{123}|F^0_{0010}\rangle+|010\rangle_{123}|F^0_{0010}\rangle\\&\quad+|100\rangle_{123}|F^1_{0000}\rangle+|111\rangle_{123}|F^1_{0000}\rangle\Big)|\phi^+\rangle_{45}\\&=\frac{1}{2}\Big[|\vartheta_1\rangle_{123}\left(|F^0_{0010}\rangle+|F^1_{0000}\rangle\right)\\&\quad+|\vartheta_7\rangle_{123}\left(|F^0_{0010}\rangle-|F^1_{0000}\rangle\right)\Big]|\phi^+\rangle_{45}\end{aligned} \tag{48}$$

为了使Eve在步骤4中不被检测到，TP对$P_1^lP_2^lP_3^l$的类GHZ基测量结果、对$P_4^lP_5^l$的Bell基测量结果都应满足式(13). 因此，根据式(13)和式(48)，应当存在：

$$|F^0_{0010}\rangle=|F^1_{0000}\rangle \tag{49}$$

根据式(45)、式(47)和式(49)可得：

$$\begin{aligned}|F^0_{1101}\rangle&=|F^0_{0010}\rangle=|F^0_{0111}\rangle=|F^0_{1000}\rangle=|F^1_{0000}\rangle\\&=|F^1_{1111}\rangle=|F^1_{0101}\rangle=|F^1_{1010}\rangle=|F\rangle\end{aligned} \tag{50}$$

(5)将式(50)代入式(27)~(42)、式(44)和式(48)可知，为了在步骤4中不引入错误，Eve的探测态的最终状态不仅要独立于Alice、Bob和TP的操作，而且还要独立于她们的测量结果. 因此，Eve无法获得关于C_A或C_B的任何有用信息.

5 针对内部参与者攻击的安全性

文献[30]指出，与外部攻击者相比，内部参与者的攻击往往更具破坏性. 接下来将分析来自半忠诚TP的攻击和来自Alice或Bob的攻击.

(1)来自半忠诚TP的攻击

TP是半忠诚的，也就是说，她可以执行任何不当的行为，但不能与其他任何人合谋. 在所提出的SQPC协议中，TP很容易地分别从Alice和Bob获得R_A和R_B. 另外，根据协议流程，TP自然会知道K_A和K_B. 但是，由于K_{AB}是通过文献[27]的SQKD协议被Alice和Bob共享，TP无法得到K_{AB}. 因此，根据式(18)，TP没有办法得到M_A；根据式(19)，TP没有办法得到M_B.

(2)来自不忠诚Alice或Bob的攻击

在所提出的SQPC协议中，Alice的角色与Bob的角色类似. 不失一般性，这里假设Alice是不忠诚的，尝试用各种手段去得到M_B. 首先，如果Alice对TP发送给Bob的S_B的粒子以及Bob返回给TP的粒子发起各种攻击，这时Alice实际上扮演着外部窃听者的角色，那么根据第4部分的证明，Alice要想攻击不被TP和Bob检测到就无法得到K_B. 其次，Alice可能会收到TP传送给Bob的R_B. 但是由于无法知道K_B，根据式(19)，Alice没有办法得到M_B.

6 基于IBM Qiskit的仿真

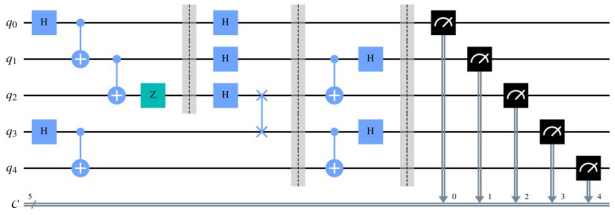
这里使用IBM公司的Qiskit来对本文协议进行实验仿真. 需要指出的是，窃听攻击被忽略，且以下所有仿真实验均被执行1 024次.

在本文协议中，TP需制备$|\vartheta_1\rangle$和$|\phi^+\rangle$. 图2~图4中的q_0、q_1、q_2、q_3和q_4为初始状态都为$|0\rangle$的5个量子比特，分别对应于粒子P_1^l、P_2^l、P_3^l、P_4^l和P_5^l. 对q_0执行一个Hadamard门(即H门)，接着以q_0为控制量子比特和q_1为目标量子比特执行一个CNOT门，然后以q_1为控制量子比特和q_2为目标量子比特执行一个CNOT门，然后对q_2执行Z门(即Z=$|0\rangle\langle0|-|1\rangle\langle1|$)，最后分别在$q_0$、$q_1$和$q_2$上执行H门，就可以制备出$|\vartheta_1\rangle$. 对$q_3$执行一个H门，然后以$q_3$为控制量子比特和$q_4$为目标量子比特执行一个CNOT门，就可以制备出$|\phi^+\rangle$. 对$q_2$和$q_3$执行SWAP门

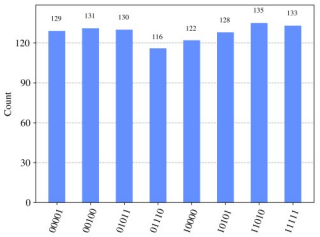
可以实现纠缠交换操作. 实现Bell基测量,只需先执行一个CNOT门和一个H门,然后进行测量;实现对类GHZ态$|\vartheta_1\rangle$的测量,需先执行三个H门和一个Z门,接着执行两个CNOT门和一个H门,再然后进行测量. 测量结果$|00\rangle$、$|01\rangle$、$|10\rangle$和$|11\rangle$分别对应00、01、10和11;测量结果$|000\rangle$、$|001\rangle$、$|010\rangle$、$|011\rangle$、$|100\rangle$、$|101\rangle$、$|110\rangle$和$|111\rangle$分别对应000、001、010、011、100、101、110和111;测量结果$|\phi^+\rangle$、$|\phi^-\rangle$、$|\varphi^+\rangle$、$|\varphi^-\rangle$分别对应00、01、10、11;测量结果$|\vartheta_1\rangle$对应000.

(1)Alice和Bob都选择REFLECT模式. 这种情况相应的量子线路及仿真结果如图2所示.

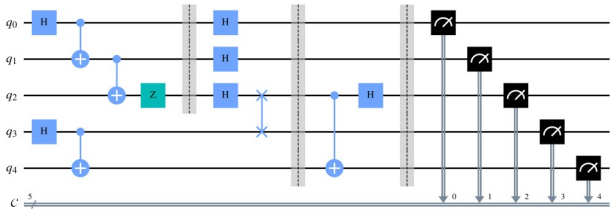
根据图2(a),TP使用Z基测量P_1^l并使用Bell基分别测量$P_2^lP_4^l$和$P_3^lP_5^l$. 从图2(b)中不难看出,00001、00100、01011、01110、10000、10101、11010、11111分别对应TP的测量结果$|1\rangle|\phi^+\rangle|\phi^+\rangle$、$|0\rangle|\phi^+\rangle|\phi^+\rangle$、$|1\rangle|\phi^-\rangle|\phi^-\rangle$、$|0\rangle|\varphi^-\rangle|\phi^-\rangle$、$|0\rangle|\phi^+\rangle|\varphi^+\rangle$、$|1\rangle|\varphi^+\rangle|\varphi^+\rangle$、$|0\rangle|\phi^-\rangle|\varphi^-\rangle$、$|1\rangle|\varphi^-\rangle|\varphi^-\rangle$. 根据图2($c$),TP使用Z基测量$P_1^lP_2^lP_3^l$且使用Bell基测量$P_4^lP_5^l$. 从图2($d$)中不难看出,00001、00010、01000、01011分别对应TP的测量结果$|100\rangle|\phi^+\rangle$、$|010\rangle|\phi^+\rangle$、$|001\rangle|\phi^+\rangle$和$|111\rangle|\phi^+\rangle$.



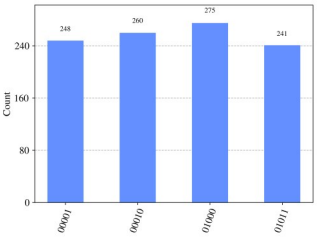
(a) TP使用Z基测量P_1^l并使用Bell基测量$P_2^lP_4^l$和$P_3^lP_5^l$时的量子线路



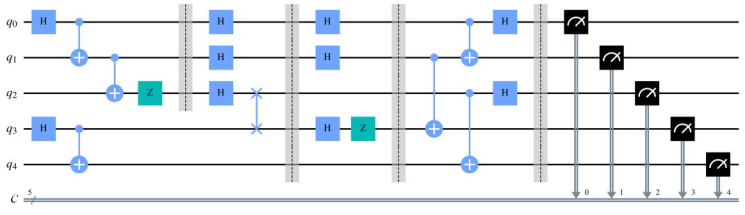
(b) (a)的仿真结果



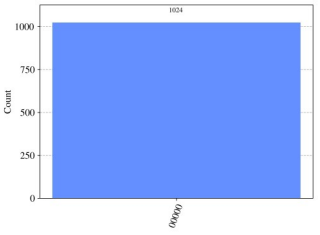
(c) TP使用Z基测量$P_1^lP_2^lP_3^l$且使用Bell基测量$P_4^lP_5^l$时的量子线路



(d) (c)的仿真结果

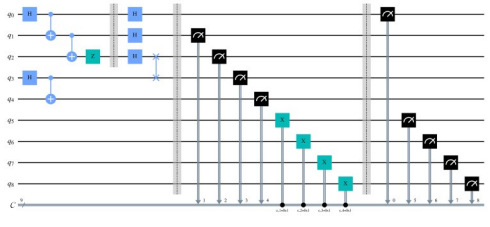


(e) TP用类GHZ基测量并用Bell基测量时的量子线路

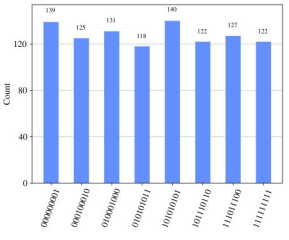


(f) (e)的仿真结果

图2　Alice和Bob都选择REFLECT模式的相应量子线路及仿真结果

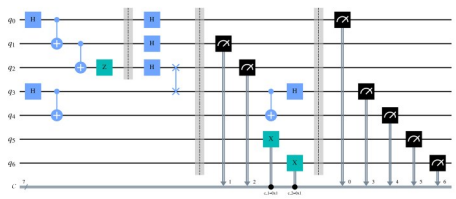


(a) Alice和Bob都选择MEASURE模式的量子线路

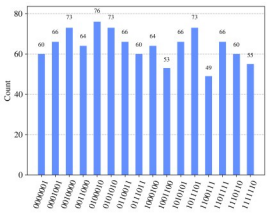


(b) (a)的仿真结果

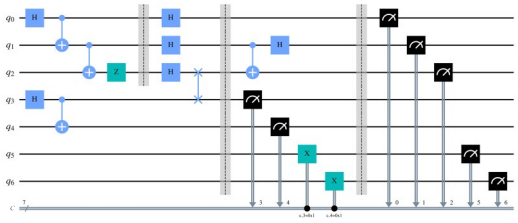
图3　Alice和Bob都选择MEASURE模式的相应量子线路及仿真结果



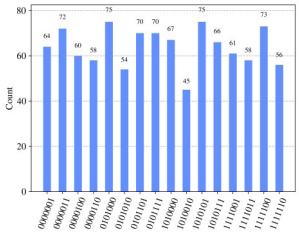
(*a*) Alice选择MEASURE模式且Bob选择REFLECT模式的量子线路



(*b*) (*a*)的仿真结果



(*c*) Alice选择REFLECT模式且Bob选择MEASURE模式的量子线路



(*d*) (*c*)的仿真结果

图4 Alice或Bob其中一方选择MEASURE模式的相应量子线路及仿真结果

根据图2(*e*),TP使用类GHZ基测量$P_1^lP_2^lP_3^l$且使用Bell基测量$P_4^lP_5^l$. 从图2(*f*)中不难看出,00000对应TP的测量结果$|\vartheta_1\rangle|\phi^+\rangle$,从而满足式(13).

因此,这种情况下的仿真结果与本文协议的理论结果一致.

(2)Alice和Bob都选择MEASURE模式. 这种情况相应的量子线路及仿真结果如图3所示. 这里,q_5和q_6表示Alice根据自己对q_1和q_3的测量结果重新制备的量子比特,q_7和q_8表示Bob根据自己对q_2和q_4的测量结果重新制备的量子比特,X门表示根据测量结果重新制备一个量子态. 从图3(*b*)中可以看出,TP的测量结果对应于000000001、000100010、010001000、010101011、101010101、101110110、111011100和111111111. 这意味着TP的测量结果与Alice、Bob的测量-重发态相同,且满足式(14). 因此,这种情况下的仿真结果与本文协议的理论结果一致.

(3)Alice或Bob其中一方选择MEASURE模式. 这种情况相应的量子线路和仿真结果如图4所示. 在图4(*a*)中,q_5和q_6表示Alice根据自己对q_1和q_3的测量结果重新制备的量子比特;由图4(*b*)可知,TP的测量结果有16种,这意味着TP的测量结果与Alice的测量-重发态相同,且满足式(15). 在图4(*c*)中,q_5和q_6表示Bob根据自己对q_2和q_4的测量结果重新制备的量子比特;由图4(*d*)可知,TP的测量结果有16种,这意味着TP的测量结果与Bob的测量-重发态相同,且满足式(16). 因此,这种情况下的仿真结果与本文协议的理论结果一致.

7 讨论与结论

文献[31]定义量子通信协议的量子比特效率为

$$\eta=\frac{c}{q+b} \tag{51}$$

其中,c、q和b分别表示隐秘信息的长度、所消耗的量子比特的数量和经典通信消耗的经典比特的数量. 这里忽略窃听检测消耗的经典资源.

在本文协议中,为了比较长度为L的隐秘信息,TP需制备$8L$个类GHZ态和$8L$个Bell态,并分别将S_A和S_B发送给Alice和Bob;接着,Alice和Bob分别从S_A和S_B中选择一半的粒子进入MEASURE模式;然后,Alice和Bob通过认证经典信道分别向TP发送R_A和R_B;此外,Alice和Bob利用文献[27]的SQKD协议预先共享K_{AB}需消耗$24L$个量子比特. 因此,有$c=L$,$q=(3+2)\times 8L+2\times 2\times 4L+24L=80L$,$b=2\times L=2L$,从而得到$\eta=\frac{L}{80L+2L}=\frac{1}{82}$.

接下来将所提出的SQPC协议与目前现有的基于量子纠缠交换的SQPC协议进行比较,并将比较结果总结在表1中. 根据表1,在量子资源方面,由于类GHZ态比四粒子团簇态更容易被制备,所提出的SQPC协议超过了文献[19]的协议;在粒子传输模式方面,所提出的SQPC协议采用树型传输模式,相比于文献[21]协议采用的环形传输模式,更能保证半量子方的独立性;在量子比特效率方面,所提出的SQPC协议高于文献[19]的协议;在量子仿真方面,文献[5]和文献[19]的协议并未对协议流程和输出正确性进行量子仿真,而所提出的SQPC协议对协议流程和输出正确性进行了量子仿真.

综上所述,本文提出一种基于类GHZ态与Bell态纠缠交换的SQPC协议,在不泄露两个半量子通信者隐秘信息的前提下借助半忠诚TP正确地比较出隐秘信息的相等性. 本文详细证明了该协议针对外部窃听者的

表1　所提出的SQPC协议与目前现有的基于量子纠缠交换的SQPC协议的对比

协议	文献[5]	文献[19]	文献[21]	本文协议
特征	测量-重发	测量-重发	测量-重发	测量-重发
量子资源	Bell态	四粒子团簇态和Bell态	Bell态	类GHZ态和Bell态
半量子用户的数量	2	2	2	2
粒子传输模式	树型传输	树型传输	环形传输	树型传输
TP的类型	半忠诚	半忠诚	半忠诚	半忠诚
TP的量子测量	Bell基测量和Z基测量	Bell基测量和Z基测量	Bell基测量和Z基测量	类GHZ基测量、Bell基测量和Z基测量
半量子通信者的量子测量	Z基测量	Z基测量	Z基测量	Z基测量
纠缠交换的使用	是	是	是	是
酉操作的使用	否	否	否	否
半量子方延迟线的使用	否	否	否	否
预共享密钥的使用	否	是	否	是
TP是否知道比较结果	是	是	是	是
量子比特效率	$\frac{1}{82}$	$\frac{1}{98}$	$\frac{1}{18}$	$\frac{1}{82}$
量子仿真的使用	否	否	是	是

攻击具备完全鲁棒性,并且分析了该协议针对内部参与者的攻击具备安全性. 本文除了从理论上分析该协议的输出是正确的之外,还通过IBM的Qiskit进行实验仿真验证了其输出正确性.

本文只研究在系统不存在噪声且器件完美的情况下利用类GHZ态与Bell态纠缠交换来进行SQPC协议的理论上的设计. 由于在系统存在噪声或器件并非完美情况下,设计安全的半量子隐私比较设计会比较复杂,我们将其留待将来进一步研究.

参考文献

[1] YAO A C. Protocols for secure computations[C]//23rd Annual IEEE Symposium on Foundations of Computer Science. Piscataway: IEEE, 1982: 160-164.

[2] YANG Y G, WEN Q Y. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement[J]. Journal of Physics A Mathematical General, 2009, 42(5): 055305.

[3] BOYER M, KENIGSBERG D, MOR T. Quantum key distribution with classical bob[J]. Physical Review Letters, 2007, 99(14): 140501.

[4] BOYER M, GELLES R, KENIGSBERG D, et al. Semi-quantum key distribution[J]. Physical Review A, 2009, 79(3): 032341.

[5] CHOU W H, HWANG T, GU J. Semi-quantum private comparison protocol under an almost-dishonest third pa-rty[EB/OL]. (2016-08-23)[2024-02-27]. https://arxiv.org/abs/1607.07961v2.

[6] YE T Y, YE C Q. Measure-resend semi-quantum private comparison without entanglement[J]. International Journal of Theoretical Physics, 2018, 57(12): 3819-3834.

[7] LIN P H, HWANG T, TSAI C W. Efficient semi-quantum private comparison using single photons[J]. Quantum Information Processing, 2019, 18(7): 207.

[8] YE C Q, LI J, CHEN X B, et al. Efficient semi-quantum private comparison without using entanglement resource and pre-shared key[J]. Quantum Information Processing, 2021, 20(8): 262.

[9] GENG M J, XU T J, CHEN Y, et al. Semiquantum private comparison of size relationship based on d-level single-particle states[J]. Scientia Sinica Physica, Mechanica & Astronomica, 2022, 52(9): 290311.

[10] YE T Y, LIAN J Y. A novel multi-party semiquantum private comparison protocol of size relationship with d-dimensional single-particle states[J]. Physica A: Statistical Mechanics and its Applications, 2023, 611: 128424.

[11] THAPLIYAL K, SHARMA R D, PATHAK A. Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment[J]. International Journal of Quantum Information, 2018, 16(5): 1850047.

[12] 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.

[13] JIANG L Z. Semi-quantum private comparison based on Bell states[J]. Quantum Information Processing, 2020, 19: 180.

[14] TSAI C W, LIN J, YANG C W. Cryptanalysis and im-

provement in semi-quantum private comparison based on Bell states[J]. Quantum Information Processing, 2021, 20: 120.
[15] XIE L, LI Q, YU F, et al. Cryptanalysis and improvement of a semi-quantum private comparison protocol based on Bell states[J]. Quantum Information Processing, 2021, 20: 244.
[16] SUN Y H, YAN L L, SUN Z B, et al. A novel semi-quantum private comparison scheme using bell entangle states[J]. Computers, Materials & Continua, 2021, 66(3): 2385-2395.
[17] GENG M J, CHEN Y, XU T J, et al. Single-state semi-quantum private comparison based on Bell states[J]. EPJ Quantum Technology, 2022, 9(1): 36.
[18] LI Z X, LIU T H, ZHU H F. Private comparison protocol for multiple semi-quantum users based on Bell states[J]. International Journal of Theoretical Physics, 2022, 61(6): 177.
[19] TIAN Y, LI J, LI C Y, et al. An efficient semi-quantum private comparison protocol based on entanglement swapping of four-particle cluster state and Bell state[J]. International Journal of Theoretical Physics, 2022, 61(3): 67.
[20] LIAN J Y, LI X, YE T Y. Multi-party semiquantum private comparison of size relationship with d-dimensional Bell states[J]. EPJ Quantum Technology, 2023, 10(1): 10.
[21] YE C Q, LI J, CHEN X B, et al. A feasible semi-quantum private comparison based on entanglement swapping of Bell states[J]. Physica A: Statistical Mechanics and Its Applications, 2023, 625: 129023.
[22] TIAN Y, LI J, YE C Q, et al. W-state-based semi-quantum private comparison[J]. International Journal of Theoretical Physics, 2022, 61(2): 18.
[23] YAN L L, CHANG Y, ZHANG S B, et al. Measure-resend semi-quantum private comparison scheme using GHZ class states[J]. Computers, Materials & Continua, 2019, 61(2): 877-887.
[24] YAN L L, ZHANG S B, CHANG Y, et al. Semi-quantum private comparison protocol with three-particle G-like states[J]. Quantum Information Processing, 2021, 20(1): 17.
[25] DÜR W, VIDAL G, CIRAC J I. Three qubits can be entangled in two inequivalent ways[J]. Physical Review A, 2000, 62(6): 062314.
[26] YANG Y G, XIA J, JIA X, et al. Comment on quantum private comparison protocols with a semi-honest third party[J]. Quantum Information Processing, 2013, 12(2): 877-885.
[27] KRAWEC W O. Mediated semiquantum key distribution[J]. Physical Review A, 2015, 91(3): 032323.
[28] DENG F G, ZHOU P, LI X H, et al. Robustness of two-way quantum communication protocols against Trojan horse attack[EB/OL].(2005-08-23)[2024-02-27].https://arxiv.org/abs/quant-ph/0508168.
[29] 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.
[30] GAO F, QIN S J, WEN Q Y, et al. A simple participant attack on the Brádler-Dušek protocol[J]. Quantum Information & Computation, 2007, 7(4): 329-334.
[31] CABELLO A. Quantum key distribution in the Holevo limit[J]. Physical Review Letters, 2000, 85(26): 5635-5638.

作者简介

徐 欣 女,1999年3月出生于浙江省丽水市. 分别于2021年和2024年在浙江工商大学获得工学学士和工学硕士学位. 主要研究方向为量子与半量子密码.

甘志刚 男,1979年1月出生于江西省抚州市. 现为浙江工商大学讲师. 主要研究方向为量子信息、量子计算、量子人工智能.
E-mail: ganzhigang@mail.zjgsu.edu.cn

叶天语 男,1982年8月出生于浙江省温州市. 现为浙江工商大学教授、硕士生导师. 主要研究方向为量子信息、量子计算、量子与半量子密码. 中国电子学会会员编号:E190010253M.
E-mail: yetianyu@zjgsu.edu.cn