基于 Bell 态的三方量子密钥协商*

尹逊汝[1)2)†] 马文平[1)] 申冬苏[1)] 王丽丽[1)]

1) (西安电子科技大学综合业务网理论及关键技术国家重点实验室, 西安 710071)

2) (泰山学院数学与统计学院, 泰安 271000)

(2013 年 4 月 1 日收到; 2013 年 5 月 26 日收到修改稿)

提出了基于两粒子纠缠态的一个三方量子密钥协商协议. 方案中的三个参与者是完全对等的, 且对建立的共享密钥具有相同的贡献. 除此之外, 三方中的任何一方或两方都不能事先单独决定共享密钥. 安全分析表明本协议既能抵抗外部窃听者的攻击, 又能抵抗内部参与者攻击.

关键词: 量子密码学, 量子密钥协商, Bell 态

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.62.170304

1 引 言

不同于密钥分发, 密钥协商是一种双方或多方间根据各自贡献的信息来建立共享密钥的技术, 并且共享的密钥不能事先由任何一方来决定 [1,2]. 但是基于计算复杂度的经典密钥协商方案随着量子计算机的不断发展面临着严峻的安全性挑战, 特别是自 Shor [3] 在提出离散对数和因式分解两个量子算法后. 基于量子力学基本原理的量子密码学由于理论上的无条件安全性成为研究的热点. 该领域的主要目标就是利用量子效应提供无条件安全的信息交换. 自 1984 年 Bennett 和 Brassard [4] 提出了第一个量子密钥分发协议以来, 人们已经提出了多种量子密码协议 [5−23], 包括量子密钥分发 (QKD), 量子安全直接通信, 量子秘密共享, 及量子签名等. 基于此, 量子密钥协商 (QKA) 也成了一个值得研究的内容. 以量子效应实现的 QKA 一方面能使得共享的密钥满足 QKD 中的密钥安全性, 另一方面还要体现公平性这一基本属性, 因为协议中的参与者可以不需要信任其他各方, 并且建立通信方之间相互接受的共享密钥就要避免某一方在协商过程中具有比其他方更大的密钥贡献优势. 利用密钥协商的这种特性能够在一个公开, 不安全的信道中建立会话密钥, 同时也不需要预先共享密钥. 密钥协商在开放性网络中具有广泛的应用, 是实现保密通信的重要技术手段, 能够满足网络中的认证, 临时安全会话等需求, 这种分布式密钥管理方式尤其适用于分散型, 无管理中心, 及动态网络结构中. 因此 QKA 具有重要的研究意义.

2004 年, Zhou 等 [24] 基于量子隐形传态首次提出了一个 QKA 协议. 但该方案被 Tsai 等 [25] 指出其中一个参与者完全能够单独确定共享的密钥且不会被检测出. 2010 年, Chong 和 Hwang[26] 利用 BB84 协议提出了一个 QKA 方案, 该协议中的通信双方通过幺正操作和延迟测量技术来建立共享的密钥. 2011 年, Chong 等人 [27] 基于最大纠缠态对 Hsueh 等人的 QKA 协议 [28] 进行了改进. 以上这些 QKA 协议 [24−28] 均是在两方间建立共享密钥, 属于点对点的通信, 不涉及三方及多方.

目前多方 QKA 研究并不多见. 2013 年, Shi 和 Zhong[29] 首次提出了一个多方 QKA 协议, 该方案基于 Bell 态和 Bell 测量并利用纠缠变换技术来实现. 然而最近 Liu 等人 [30] 指出文献 [29] 中建立的共享密钥可以由不诚实的参与者单独决定从而不是一个安全的方案. 同时文献 [30] 基于单粒子提出

* 国家自然科学基金 (批准号: 61072140)、高等学校创新引智计划 (批准号: B08038)、高等学校博士学科点专项科研基金 (批准号: 20100203110003) 和山东省高等学校科技计划项目 (批准号: J13LN60) 资助的课题.

† 通讯作者. E-mail: xryin@outlook.com; yxr03@yahoo.com.cn

了一个多方 QKA 协议.

本文基于两粒子纠缠态利用稠密编码的思想提出了一个三方量子密钥协商协议. 三个参与者是完全对等的实体, 首先三方各自随机产生一个比特串作为自己的密钥, 然后每一方制备 Bell 态序列并分为两个单粒子序列分别传送给其余两方, 在经过编码操作后返回, 再通过 Bell 测量提取其余两方的密钥, 最后对三方的密钥进行异或运算来建立共享密钥. 安全分析表明本方案能够抵抗外部攻击和内部参与者的攻击.

2 提出的三方 QKA 协议

首先介绍两粒子最大纠缠态 Bell 基态, 也称为 EPR 纠缠对, 表现为四个形态. 即 $|\Psi^+\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)$, $|\Psi^-\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle)$, $|\Phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$, 以及 $|\Phi^-\rangle = 1/\sqrt{2}(|00\rangle - |11\rangle)$. 其中 $|0\rangle$ 和 $|1\rangle$ 表示二能级系统光子的两个相正交的偏振态, 也即 Pauli 算子 σ_z 的本征态. 分别令 $|+\rangle, |-\rangle$ 表示 $(|0\rangle + |1\rangle)/\sqrt{2}$, $(|0\rangle - |1\rangle)/\sqrt{2}$, 则 $|+\rangle$ 和 $|-\rangle$ 是 Pauli 算子 σ_x 的两个本征态. 记三个局域幺正操作 U_0, U_1, 和 U_2 分别表示 $U_0 \equiv I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $U_1 \equiv \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$, $U_2 \equiv \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$. 一个 EPR 对经过上面这三个幺正操作后可以转变为另一个 EPR 对. 更进一步, 如果以 $|\Psi^+\rangle$ 为初态, 对其第一个粒子施加幺正操作 U_0 或 U_1, 对第二个粒子施加 U_0 或 U_2 则变换后的终态总结在表 1 中.

表 1 态 $|\Psi^+\rangle$ 的转换规则

初态	幺正操作	终态
$\|\Psi^+\rangle$	$U_0 \otimes U_0$	$\|\Psi^+\rangle$
	$U_0 \otimes U_2$	$\|\Phi^+\rangle$
	$U_1 \otimes U_0$	$\|\Phi^-\rangle$
	$U_1 \otimes U_2$	$\|\Psi^-\rangle$

下面介绍三方量子密钥协商协议. 假定方案的三个参与者为 Alice, Bob 和 Charlie. 三方通过量子信道想要建立一个共享密钥 K. 首先 Alice 随机产生一个比特串 $K_A = \{a_1 a_2 \cdots a_n\}$ 作为她自己的密钥, Bob 随机产生一个比特串 $K_B = \{b_1 b_2 \cdots b_n\}$ 作为他自己的密钥, Charlie 随机产生一个比特串 $K_C = \{c_1 c_2 \cdots c_n\}$ 作为他自己的密钥. 这里 a_i, b_i, $c_i \in \{0,1\}$, $i = 1,2,\cdots,n$. 执行步骤如下.

1) Alice/Bob/Charlie 制备 n 个 Bell 态 $|\Psi^+\rangle$, 并从每一个纠缠对中取出两个粒子形成两个单粒子序列. 令 P_{A1} 和 P_{A2} 表示 Alice 的两个粒子序列, 这两个序列中的粒子分别由 $|\Psi^+\rangle$ 的第一个和第二个量子比特组成. 同样, 记 P_{B1}, P_{B2} 为 Bob 的两个单粒子序列; P_{C1}, P_{C2} 为 Charlie 的两个单粒子序列. 此外, 每一方均从 $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ 中随机选取足够的诱骗粒子并随机插入各自的两个单粒子序列中. 随后 Alice 把混合后的 P_{A1}, P_{A2} 分别发送给 Bob 和 Charlie. Bob 把混合后的 P_{B1}, P_{B2} 分别发送给 Charlie 和 Alice. Charlie 把混合后的 P_{C1}, P_{C2} 分别发送给 Alice 和 Bob.

2) 当确定 (Bob, Charlie)/(Charlie, Alice)/(Alice, Bob) 收到粒子序列后, Alice/Bob/Charlie 公布诱骗粒子的位置和相应的测量基 $\{|0\rangle, |1\rangle\}$ 或 $\{|+\rangle, |-\rangle\}$. 然后 Alice/Bob/Charlie 分别与其余两方通过比较测量结果来进行量子信道的安全检查. 如果错误率超过一定的阈值则放弃该协议, 否则继续进行下一步.

3) 挑选出诱骗粒子后, 各方按照如下规则进行编码操作. 对接收到 $P_{A1}/P_{B1}/P_{C1}$ 的 Bob/Charlie/Alice, 若 $b_i = 0/c_i = 0/a_i = 0$ ($i = 1,2,\cdots,n$), 则对序列中的第 i 个粒子执行操作 U_0; 否则执行 U_1. 执行幺正操作后的粒子序列记为 $P'_{A1}/P'_{B1}/P'_{C1}$. 对接收到 $P_{A2}/P_{B2}/P_{C2}$ 的 Charlie/Alice/Bob, 若 $c_i = 0/a_i = 0/b_i = 0$, 则对序列中的第 i 个粒子执行操作 U_0; 否则执行 U_2. 执行操作后序列记为 $P'_{A2}/P'_{B2}/P'_{C2}$. 另外, 接收到粒子序列的各方从 $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ 中随机选取足够的诱骗粒子并随机插入各自执行幺正操作后的单粒子序列中, 随后返还给原先的发送方.

4) 当确定 Alice/Bob/Charlie 收到粒子序列后, (Bob, Charlie)/(Charlie, Alice)/(Alice, Bob) 公布诱骗粒子的位置和相应的测量基, 然后他们通过比较测量结果进行第二次安全检查. 同样, 如果错误率超过一定的阈值, 通信方之间放弃该协议, 否则继续执行下一步.

5) 在挑选出诱骗粒子后, Alice 此时拥有粒子序列 P'_{A1} 和 P'_{A2}, Bob 拥有序列 P'_{B1} 和 P'_{B2}, 而 Charlie 拥有序列 P'_{C1} 和 P'_{C2}. 三方从各自两个序列中取出对应的粒子形成 n 个粒子对, 然后对这些粒子对执行 Bell 测量. 根据测量结果和表 1, 每一方能够提取其余两方的密钥, 从而三方建立共享密钥 $K = K_A \oplus K_B \oplus K_C$.

从以上所有步骤可看出, 三个参与者各自向其余两方传送单粒子序列的过程是同时进行的, 也即每一方既是序列的发送者同时也是接收者, 从

而形成了量子比特传送的一个回路. 为清楚起见, 忽略掉两次安全检查过程, 整个协议的执行步骤可以参见图 1, 其中步骤 Ⅱ 中, $U_{\mathrm{A1}}: P_{\mathrm{C1}} \to P'_{\mathrm{C1}}$ 表示 Alice 对序列 P_{C1} 执行幺正操作 U_{A1} 后形成新的序列 P'_{C1}, 其余类似; 操作 $U_{\mathrm{A1}}, U_{\mathrm{B1}}, U_{\mathrm{C1}} \in \{U_0, U_1\}$; $U_{\mathrm{A2}}, U_{\mathrm{B2}}, U_{\mathrm{C2}} \in \{U_0, U_2\}$; 步骤 Ⅳ 中 "BM" 表示 Bell 测量; 实线箭头表示量子比特的传送方向, 虚线表示三方同时执行程序.

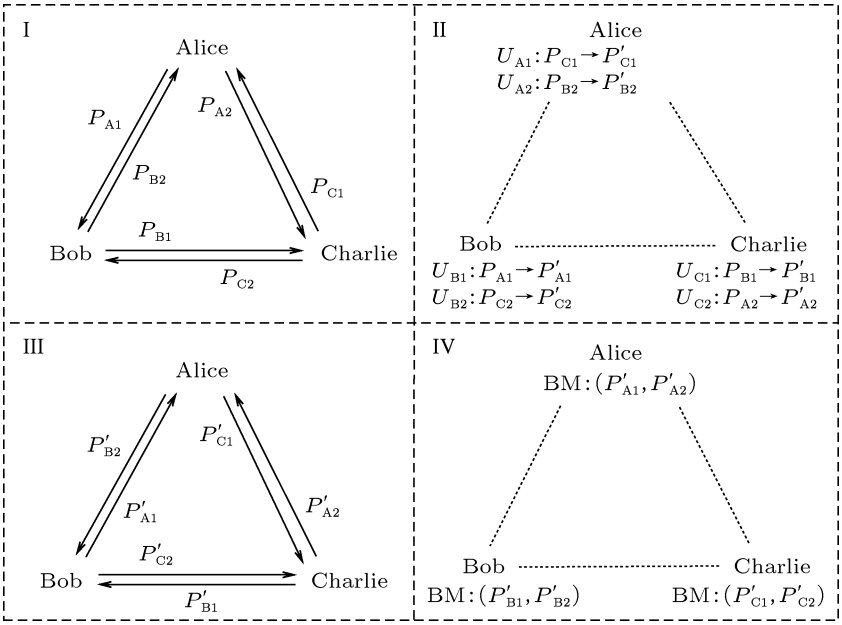

图 1 三方量子密钥协商协议图示

下面以 Alice 提取 Bob 和 Charlie 的密钥为例来说明三方如何来建立共享密钥 K. 不妨假设 Alice 的密钥是 $K_{\mathrm{A}} = 0$, Bob 的密钥是 $K_{\mathrm{B}} = 1$, Charlie 的密钥是 $K_{\mathrm{C}} = 1$. 首先 Alice 制备 Bell 态 $|\Psi^+\rangle_{12}$. 她把粒子 1 发送给 Bob, 粒子 2 发送 Charlie. 按照步骤 3) 的规则, Bob 对收到的粒子 1 根据自己的密钥比特值 K_{B} 采取幺正操作 U_1, Charlie 对收到粒子 2 根据自己的密钥 K_{C} 执行幺正操作 U_2, 此时态 $|\Psi^+\rangle_{12}$ 转换为 $U_1 \otimes U_2 |\Psi^+\rangle_{12} \to |\Psi^-\rangle_{12}$. Bob 和 Charlie 执行完幺正操作后分别把粒子 1 和 2 返回给 Alice. 当 Alice 收到两个粒子后执行 Bell 测量, 其测量结果必为 $|\Psi^-\rangle_{12}$. 由表 1, Alice 就可以提取 Bob 的密钥 1 和 Charlie 的密钥 1. 同样的方式, Bob 和 Charlie 也分别提取到其余两方的密钥比特. 于是三方建立了共享密钥 $K = K_{\mathrm{A}} \oplus K_{\mathrm{B}} \oplus K_{\mathrm{C}} = 0$.

3 安全分析

这一节我们来分析提出的三方 QKA 协议安全性. 一个安全的量子密钥协商协议要能阻止外部攻击者窃取共享密钥的相关信息, 同时也能够防止内部不诚实参与者的攻击, 即除全集以外全体参与者的任何子集都不能单独决定共享密钥的值. 下面就外部攻击和内部攻击分别进行分析.

首先考虑外部攻击. 从协议的执行步骤可以看到, 每一个参与者通过量子信道向其他两方发送量子比特的过程是独立的. 三方间共享一个密钥的过程就是通过一方接收已经被其余方编码过的粒子并执行 Bell 测量从而提取到各方的私钥来建立的. 协议执行完毕后, 外部窃听者 Eve 是不可能得到共享密钥的相关信息的, 因此攻击者只能从每一个参与者的私钥和量子比特的传送来获取相关信息. 不失一般性, 假设 Alice 是 Bell 态 $|\Psi^+\rangle$ 的制备者, Bob 和 Charlie 是接收者为例来说明 Eve 的攻击策略. 量子比特的传送有两个并存的发送和返回两个过程. Eve 可能的一种攻击是拦截重发. 当 Alice 发送粒子序列给 Bob (Charlie) 时, Eve 俘获经过的粒子并存储起来, 然后替换成自己事先准备好的粒子再发送给接收方. 但是 Alice 是随机插入诱骗粒子到发送的序列中, 在她公布粒子位置和相应的测量基前, Eve 不可能知道诱骗粒子的相关信息. 由于诱骗粒子随机处于态 $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ 中, 假定制备的诱骗粒子数是 τ, 则 Eve 被检测出的概率是 $1/4^{\tau}$. 另一方面, Alice 是同时把两个粒子序列发送给 Bob 和 Charlie 的, Eve 还可以事先

准备好自己制备的态 $|\Psi^+\rangle$ 序列, 当俘获 Alice 发送的粒子后, 用自己的相应粒子序列代替 Alice 的再分别发送给 Bob 和 Charlie, 当返回时拦截编码后的粒子并测量. 如果 Eve 能够成功的通过安全检查她就能获得 Bob 和 Charlie 的密钥. 用类似的方法截获 Bob 和 Charlie 作为制备方分别发送的粒子后就可以窃取共享密钥. 下面来分析这种攻击是否能成功. Eve 如果把制备的两个粒子序列都发送出去, 她手中留下的是原先 Alice 制备的粒子, 这种情况下必然会引入错误通不过安全检查. 由于是确认接收方收到粒子后 Alice 才公布诱骗粒子的相关信息, 因此 Eve 可以采取各个延迟发送. 比如 Eve 把一个单粒子序列发送给 Bob, 当 Alice 公布诱骗粒子位置和测量基后, Eve 对手中对应的单粒子序列按照公布的结果进行测量. 由关联式 $|\Psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2} = (|++\rangle - |--\rangle)/\sqrt{2}$ 知无论采取哪个测量基, 每一次测量都会带来 50% 的出错率. Eve 还可能采取纠缠测量攻击, 即对截获的粒子不做测量, 而是和自己事先准备的光子 E 做一个幺正操作使二者纠缠. 不妨假定截获的一个粒子为 1, 并定义 Eve 的操作算符为 $\hat{U}$, 则

$$\hat{U} : |0\rangle|\varepsilon\rangle \to |0\rangle|\varepsilon_{00}\rangle + |1\rangle|\varepsilon_{01}\rangle, \tag{1}$$

$$|1\rangle|\varepsilon\rangle \to |0\rangle|\varepsilon_{10}\rangle + |1\rangle|\varepsilon_{11}\rangle, \tag{2}$$

其中 $|\varepsilon_{ij}\rangle$ $(i,j \in \{0,1\})$ 是由 $\hat{U}$ 确定的纯态. 于是整个量子系统处于态

$$\hat{U}|\Psi^+\rangle_{12}|\varepsilon\rangle_E \to \frac{1}{\sqrt{2}}(|1\rangle_1|u\rangle_{2E} + |0\rangle_1|v\rangle_{2E}). \tag{3}$$

这里 $|u\rangle \to |0\rangle|\varepsilon_{00}\rangle + |1\rangle|\varepsilon_{01}\rangle$, $|v\rangle \to |0\rangle|\varepsilon_{10}\rangle + |1\rangle|\varepsilon_{11}\rangle$. 如果 Eve 要避免引入错误, 必然要满足 $\langle 1|u\rangle = 0$ 及 $\langle 0|v\rangle = 0$, 于是可得 $\varepsilon_{01} = 0$, $\varepsilon_{10} = 0$. 另一方面, 安全检查时若采用的测量基为 $\{|+\rangle, |-\rangle\}$, 则

$$\hat{U} : |+\rangle|\varepsilon\rangle \to \frac{1}{2}(|+\rangle(|\varepsilon_{00}\rangle + |\varepsilon_{11}\rangle) + |-\rangle(|\varepsilon_{00} - |\varepsilon_{11}\rangle)), \tag{4}$$

$$|-\rangle|\varepsilon\rangle \to \frac{1}{2}(|+\rangle(|\varepsilon_{00}\rangle - |\varepsilon_{11}\rangle) + |-\rangle(|\varepsilon_{00} + |\varepsilon_{11}\rangle)). \tag{5}$$

此时整个量子系统 $\hat{U}\left(\frac{1}{\sqrt{2}}(|++\rangle - |--\rangle)_{12}\right)|\varepsilon\rangle_E$ 处于态

$$\begin{aligned}&\hat{U}|\Psi^+\rangle_{12}|\varepsilon\rangle_E\\ &\to \frac{1}{2\sqrt{2}}(|+\rangle_1(|+\rangle_2(|\varepsilon_{00}\rangle + |\varepsilon_{11}\rangle)_E\\ &\quad +|-\rangle_2(|\varepsilon_{00}\rangle - |\varepsilon_{11}\rangle)_E)\\ &\quad -|-\rangle_1(|+\rangle_2(|\varepsilon_{00}\rangle - |\varepsilon_{11}\rangle)_E\\ &\quad +|-\rangle_2(|\varepsilon_{00}\rangle + |\varepsilon_{11}\rangle)_E)).\end{aligned} \tag{6}$$

同样 Eve 要想避免引入错误, 上式中不能出现 $|+\rangle_1|-\rangle_2$ 和 $|-\rangle_1|+\rangle_2$ 这两项, 于是 $\varepsilon_{00} = \varepsilon_{11}$. 因此整个量子系统处于直积形式 $|\psi^+\rangle_{12}|\varepsilon_{00}\rangle_E$. 这样 Eve 不能通过观察附加粒子来获得任何有用的信息. 此外, 为避免不可见光子特洛伊木马攻击 [31,32] 针对对粒子往返传输窃取信息, 可应用滤波器和光子分离器. 综上所述, 提出的协议可以抵抗外部攻击.

接下来考虑三方中存在不诚实者的情况, 即参与者攻击 [33]. 这种攻击方式在量子密码协议中引起了深入而广泛的研究 [34−39], 已取得很多重要的结论. 方案中三方间共享的密钥是通过对参与者的私钥做异或操作建立的, 而三方的密钥 $K_{\rm A}$, $K_{\rm B}$ 以及 $K_{\rm C}$ 都是各自随机生成的, 因此除了他们自己外的其他任何两方都不能事先确定. 从协议的执行步骤可以看出三个参与者完全是对等的, 他们对共享密钥的建立具有相同的贡献. 这种共享密钥的建立过程和量子比特的传输模式类似于 Liu 等人基于单粒子提出的多方 QKA 协议 [30]. 不同之处在于本文中的粒子序列有一个往返过程, 下面针对这种情况进行安全分析. 不妨假定 Alice 是诚实的参与者, Bob 和 Charlie 双方联合起来欺骗 Alice, 他们打算独自决定共享的密钥. 要实现这一目的, Bob 和 Charlie 需要提取到 Alice 的密钥 $K_{\rm A}$. 因此 Alice 是粒子序列的接受方, 而 Bob 和 Charlie 都是粒子制备者. 对于 Bob, 他把制备的一个粒子序列发送给 Alice, 另一个粒子序列不经过 Charlie 而是自己保留在手中, 当 Alice 返回编码有她密钥信息的粒子序列后, Bob 通过 Bell 测量就可以获得 Alice 的密钥. 同样对于 Charlie, 他把制备的粒子序列发送给 Alice 后, 通过测量留在自己手中的粒子和返回的带有 Alice 密钥信息的编码粒子而提取密钥. 然而另一方面, 协议中三方间量子比特传送是一个回路, 每一方作为制备者是独立的且同时发送给其余两方, 当 Bob 和 Charlie 联合起来进行不诚实的操作的时候, Alice 不能获得 Bob 或 Charlie 的相应密钥, 从而会被她发觉而中止协议. 另外一种特殊的情况是存在一个不诚实的参与者, 比如 Alice 和 Bob 是诚实的, 不诚实的 Charlie 想独自确定共享的密钥. 此时 Charlie 需要获得 Alice 和 Bob 二者的密钥. 于是 Charlie 制备两个粒子序列并分别发送给 Alice

和 Bob, 当二者把各自的密钥通过幺正操作编码于粒子序列并返还时, Charlie 通过 Bell 测量获得了所需密钥信息, 按照协议 Charlie 已经确定了三方间的共享密钥. 但由于量子比特传输回路的特性, 其余两方同时也获得了 Charlie 的私钥. 即一个不诚实的参与者也不能事先独自确定所有通信者之间共享的密钥. 综上所述, 提出的协议能够抵抗参与者攻击.

4 结 论

本文基于 EPR 对提出了一个三方密钥协商方案. 共享密钥是通过每一方提取其余两方的密钥再对所有密钥进行异或操作建立的. 安全分析也表明我们的协议既能够抵抗外部窃听者的攻击也能够抵抗内部不诚实参与者的攻击. 方案中的量子资源在目前的技术下较为容易实现, 协议执行过程就有较高的可行性. 另一方面本文的讨论是建立在理想的量子信道上, 但实际物理环境中的噪声和损耗是不可忽略的, 噪声的存在能够降低量子通信的成功率, 因此在未来的研究中我们希望能够完善这类问题.

[1] Mitchell C J, Ward M, Wilson P 1998 *Electron. Lett.* **34** 980

[2] Ateniese G, Steiner M, Tsudik G 2000 *IEEE J. Sel. Areas Commun.* **18** 628

[3] Shor P W 1994 *Proceedings of 35th Annual Symposium on Foundations of Computer Science*, Los Alamitos p124

[4] Bennett C H, Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* Bangalore, India (New York: IEEE) p175

[5] Bennett C H, Brassard G, Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[6] Long G L, Liu X S 2002 *Phys. Rev.* A **65** 032302

[7] Gao F, Guo F Z, Wen Q Y, Zhu F C 2006 *Phys. Lett.* A **355** 172

[8] Zhang Z J, Man Z X 2005 *Chin. Phys. Lett.* **22** 1588

[9] Zeng G H, Keitel C 2002 *Phys. Rev.* A **65** 042312

[10] Deng F G, Long G L, Liu X S 2003 *Phys. Rev.* A **68** 042317

[11] Zeng G H, Lee M, Guo Y, He G Q 2007 *Int. J. Quantum Inf.* **5** 553

[12] Zhu C H, Pei C X, Quan D X, Gao J L, Chen N, Yi Y H 2010 *Chin. Phys. Lett.* **27** 090301

[13] Ding D, Yan F L 2013 *Acta Phys. Sin.* **62** 10302 (in Chinese) [丁东, 闫凤利 2013 物理学报 **62** 10302]

[14] Zhu J, He G Q, Zeng G H 2007 *Chin. Phys.* **16** 1364

[15] Yang Y G, Wen Q Y, Zhu F C 2006 *Acta Phys. Sin.* **55** 3255 (in Chinese) [杨宇光, 温巧燕, 朱甫臣 2006 物理学报 **55** 3255]

[16] Gao F, Guo F Z, Wen Q Y, Zhu F C 2008 *Sci. China Ser.* G **51** 559

[17] Yin X R, Ma W P, Liu W Y 2012 *Int. J. Theor. Phys.* **51** 455

[18] Nguyen B A 2004 *Phys. Lett.* A **328** 6

[19] Man Z X, Xia Y J, Zhang Z J 2006 *Int. J. Quantum Inf.* **4** 739

[20] Guo Y, Chen Z G, Zeng G H 2007 *Chin. Phys.* **16** 2549

[21] Li J, Jin H F, Jing Bo 2011 *Sci. China Ser.* G **54** 1612.

[22] Liu W, Wang Y B 2011 *Acta Phys. Sin.* **60** 30305 (in Chinese) [刘文, 王永滨 2011 物理学报 **60** 30305]

[23] Liu B, Gao F, Wen Q Y 2011 *IEEE J. Quant. Electron.* **47** 1383

[24] Zhou N, Zeng G, Xiong J 2004 *Electron. Lett.* **40** 1149

[25] Tsai C W, Hwang T 2009 *Technical Report*, *C-S-I-E, NCKU*, Taiwan, R.O.C.

[26] Chong S K, Hwang T 2010 *Opt. Commun.* **283** 1192

[27] Chong S K, Tsai C W, Hwang T 2011 *Int. J. Theor. Phys*. **50** 1793

[28] Hsueh C C, Chen C Y 2004 *Proceedings of the 14th Information Security Conference, National Taiwan University of Science and Technology*, Taipei p236

[29] Shi R H, Zhong H 2013 *Quantum Inf. Process.* **12** 921

[30] Liu B, Gao F, Huang W, Wen Q Y 2013 *Quantum Inf. Process.* **12** 1797

[31] Cai Q Y 2006 *Phys. Lett.* A **351** 23

[32] Li X H, Deng F G, Zhou H Y 2006 *Phys. Rev.* A **74** 054302

[33] Gao F, Qin S J, Wen Q Y, Zhu F C 2007 *Quantum Inf. Comput.* **7** 329

[34] Qin S J, Gao F, Wen Q Y, Zhu F C 2007 *Phys. Rev.* A **76** 062324

[35] Gao F, Wen Q Y, Zhu F C 2007 *Phys. Lett.* A **360** 748

[36] Gao F, Guo F Z, Wen Q Y, Zhu F C 2008 *Phys. Rev. Lett.* **101** 208901

[37] Song T T, Zhang J, Gao F, Wen Q Y, Zhu F C 2009 *Chin. Phys.* B **18** 1333

[38] Guo F Z, Qin S J, Gao F, Liu S, Wen Q Y, Zhu F C 2010 *Eur. Phys. J.* D **56** 445

[39] Gao F, Qin S J, Wen Q Y, Zhu F C 2010 *Opt. Commun.* **283** 192

Three-party quantum key agreement with Bell states*

Yin Xun-Ru[1)2)†] Ma Wen-Ping[1)] Shen Dong-Su[1)] Wang Li-Li[1)]

1) (*State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an* 710071, *China*)

2) (*School of Mathematics and Statistics, Taishan University, Tai'an* 271000, *China*)

(Received 1 April 2013; revised manuscript received 26 May 2013)

Abstract

A three-party quantum key agreement protocol based on EPR pairs is proposed, in which the three participants have equal status in the protocol and each participant is capable of contributing to the shared secret key in the same degree. In addition, any one or two parties cannot predetermine the value of shared key alone. The security analysis shows that our protocol can resist the outside attack and the dishonest participants attack.

Keywords: quantum cryptography, quantum key agreement, Bell states

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.62.170304

* Project supported by the National Natural Science Foundation of China (Grant No. 61072140), the 111 Project (Grant No. B08038), the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20100203110003), the Project of Shandong Province Higher Educational Science and Technology Program, China (Grant No. J13LN60).

† Corresponding author. E-mail: xryin@outlook.com; yxr03@yahoo.com.cn