物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于*d*维GHZ态的多方量子密钥协商

唐杰 石磊 魏家华 于惠存 薛阳 武天雄

Multi-party quantum key agreement based on *d*-level GHZ states

Tang Jie Shi Lei Wei Jia-Hua Yu Hui-Cun Xue Yang Wu Tian-Xiong

引用信息 Citation: Acta Physica Sinica, 69, 200301 (2020) DOI: 10.7498/aps.69.20200799
在线阅读 View online: https://doi.org/10.7498/aps.69.20200799
当期内容 View table of contents: http://wulixb.iphy.ac.cn

基于 d 维 GHZ 态的多方量子密钥协商*

唐杰 石磊 魏家华† 于惠存 薛阳 武天雄

(空军工程大学信息与导航学院, 西安 710077)

(2020 年 5 月 27 日收到; 2020 年 6 月 30 日收到修改稿)

提出了一个基于 d 维多粒子 GHZ (Greenberger-Horne-Zeilinger) 态作为量子信道的多方量子密钥协商协议. 该方案充分利用时移操作将密钥编码到量子态序列中, 通过 d 维 Z 基测量得到密钥. 除此之外, 本方案确保多个参与者是完全对等且公平的, 对最终密钥生成的贡献是平等的. 安全性分析表明本方案能够有效抵抗内部参与者和外部窃听者的攻击.

关键词: d 维, 多方量子密钥协商, 时移操作, 安全性分析

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.69.20200799

1 引 言

随着量子信息技术的发展, 量子密码也因其无条件安全性引起越来越多的关注. 不同于经典密码, 量子密码的安全性并非基于解决数学难题的复杂性, 而是基于量子物理学的基本原理, 从理论上讲具有无条件安全性. 量子密码技术包含很多分支, 如量子密钥分发, 量子安全直接通信, 量子秘密共享.

在开放式、动态化的网络中, 为了满足网络中的认证, 临时会话等需求, 实现保密通信, 在一个公开、不安全的信道中建立会话密钥, 两个端节点之间需要建立一个共享的密钥来实现基本的安全需求. 基于此, 量子密钥协商 (quantum key agreement, QKA) 则引起了研究者们广泛的关注. 不同于量子密钥分配, 量子密钥协商是一种双方或多方共同合作建立共享密钥的技术. 在协议中, 每个参与者均不能事先单独决定共享密钥, 且他们对于最终生成的密钥贡献相同. 在量子保密通信中, 需要建立临时通话, 满足网络中的认证等, 而量子密钥协商恰恰适应这个要求, 使我们可以安全地在分散型、无管理和动态网络结构中建立共享密钥. 因此, 量子密钥协商具有重要的研究意义.

自 2004 年 Zhou 等 [1] 利用量子隐形传态和最大纠缠态提出第一个 QKA 协议起, 人们陆续提出了很多 QKA 协议 [2–8]. 然而, 这些 QKA 协议仅仅只涉及两方, 并不适用于多个参与者. 自 Shi 和 Zhong[9] 基于 EPR 对和纠缠交换将两方 QKA 协议拓展到多方量子密钥协商 (multi-party quantum key agreement, MQKA) 协议时, 研究者们也将关注点放在了 MQKA 协议中. 随后 Liu 等 [10]指出 Shi 和 Zhong 提出的 MQKA 协议是不安全的, 证明了不诚实的参与者能够独自决定共享密钥, 同时他们提出了一种仅使用单光子进行编码的 MQKA 协议来抵抗参与者内部攻击. 然而, Liu 等的协议效率不是很高. Sun 等 [11] 添加了两个幺正操作改进了 Liu 的协议, 将量子比特效率提高到了 $1/[N(k+1)]$. 同年, Yin 等 [12] 基于两粒子纠缠态提出了三方 QKA 协议. 2014 年, Xu 等[13] 基于 GHZ (Greenberger-Horne-Zeilinger) 提出一个 MQKA 协议, 协议中的每个参与者仅仅只需执行单粒子测

* 国家自然科学基金 (批准号: 61971436) 和国家自然科学基金青年科学基金 (批准号: 61803382) 资助的课题.

† 通信作者. E-mail: weijiahua@126.com

量. 后来, Sun 等[14,15]利用六粒子簇态提出两个 MQKA 协议. 2018 年, Cai 等[16]基于五粒子 brown 态和单粒子测量提出一个 MQKA 协议. 相比于其他协议, 此协议的效率更高, 并且也有着更好的操作灵活性. 2019 年, Lin 等[17]发现 Cai 等的协议不满足协议的公平性, 并提出了一个改进的协议. 同年, Liu 等[18]利用四粒子簇态作为量子源, 并对粒子执行 X 基操作, 提出了一个新的 MQKA 协议. 效率分析也说明此协议拥有着较高的效率. 2020 年, Zhou 等[19]以量子方 Charlie, 经典方 Alice 和 Bob 为参与方提出三方半量子密钥协商协议 (semi-QKA). 此协议能够减少量子设备的使用, 降低损耗. 随着对量子密钥协商协议的研究逐渐深入, 为了追求更好的安全性、公平性和高效率, 人们提出了许多 MQKA 协议[20–29].

"d 维"这个概念在量子密码的其他协议中出现过多次, 但在量子密钥协商中并未有人做过太多研究. 本文基于 d 维 k 粒子 GHZ 态提出了一个多方量子密钥协商协议. GHZ 态最早由 Greenberger-Horne-Zeilinger 三人联合提出. 1999 年, Bouwmeester 等[30]通过实验对其进行了观察与分析, 发现其显著的作用. 在后来的研究中, GHZ 态被广泛应用于多方量子密钥分发[31,32]、多方量子秘密共享[33]和多方量子安全直接通信[34]等方向. 本文所提的 d 维多粒子 GHZ 态是二维 GHZ 态的衍生, 能够携带更多的信息, 具有更高的信道容量. 除此之外, 在我们提出的多方协议中, 多个参与者是完全对等且公平的, 并利用时移操作将密钥编码到量子序列中, 最后通过 d 维 Z 基测量得到密钥. 安全性分析表明本方案能够有效地抵抗内部参与者和外部窃听者的攻击.

2 基于 d 维 GHZ 态的 MQKA 协议

2.1 理论基础

对于 d 维量子系统来说, k 粒子 GHZ 态可表示为

$$|\Phi\rangle = \frac{1}{\sqrt{d}}\left(\underbrace{|0\rangle|0\rangle\cdots|0\rangle}_{k}+\underbrace{|1\rangle|1\rangle\cdots|1\rangle}_{k} + \cdots+\underbrace{|d-1\rangle|d-1\rangle\cdots|d-1\rangle}_{k}\right). \tag{1}$$

两组正交基分别表示为

$$Z=\{|0\rangle,|1\rangle,|2\rangle,\cdots,|d-1\rangle\},$$

$$X=\{\mathrm{QFT}|0\rangle,\mathrm{QFT}|1\rangle,\mathrm{QFT}|2\rangle,\cdots,\mathrm{QFT}|d-1\rangle\}, \tag{2}$$

其中 QFT 是指作用在 d 维 Hilbert 空间的离散量子傅里叶变换, 它的作用是把一个单态转换到一个叠加态. QFT 的定义为

$$\mathcal{F}|u\rangle=\frac{1}{\sqrt{d}}\sum_{v=0}^{d-1}\mathrm{e}^{\frac{2\pi iuv}{dt}}|v\rangle \quad (u,v\in\{0,1,\cdots,d-1\}). \tag{3}$$

接下来, 引入时移操作:

$$U_r=\sum_{t=0}^{d-1}\exp\left(\frac{2\pi it(t\oplus r)}{d}\right)|t\oplus r\rangle\langle t|, \tag{4}$$

其中 $t\oplus r$ 表示 $t+r$ 模 d. 经过验算, 不难发现,

$$U_r(|s\rangle)=|s\oplus r\rangle,\ U_r(\mathrm{QFT}|s\rangle)=\mathrm{QFT}|s\oplus r\rangle \quad (s=0,1,2,\cdots,d-1)\,. \tag{5}$$

2.2 提出的 MQKA 协议

本节介绍提出的基于 d 维 k 粒子 GHZ 态的 MQKA 协议. 假设 $P_0,P_1,P_2,\cdots,P_{k-1}$是协议的 k 个参与者, 他们想通过量子信道建立共享密钥 K, 每个参与者 P_i随机产生各自的密钥信息为 $K_i=\left(K_i^0,K_i^1,\cdots,K_i^{d-1}\right)$, 其中 $K_i^n\in\{0,1,\cdots,l\}$; $d=2l+1$; $n=0,1,\cdots,k-1$; $j=0,1,\cdots,d-1$. 协议的具体步骤如下.

第 1 步 每个参与者 P_i准备好 m 个形式如 (1) 式的 d 维 k 粒子 GHZ 态, 并将每一个 GHZ 态分成 k 个粒子序列: $S_0,S_1,\cdots,S_{k-1}$, 其中第 i 个序列 S_i $(i=0,1,\cdots,k-1)$由 GHZ 态的第 i 个粒子组成. 接下来, P_i从 (2) 式的 X 基和 Z 基随机挑选诱骗态分别插入到每个序列 S_i $(i=0,1,\cdots,k-1)$中得到新的序列 S_i' $(i=0,1,\cdots,k-1)$, 并将序列 S_j' $(j=0,1,\cdots,k-1)$发送给其他参与者 P_j.

第 2 步 在确认 P_j接收到序列 S_j'后, P_i将诱骗态的位置、采用的测量基及测量结果告知 P_j, 双方进行第一次安全检查. P_j用相应的测量基测量诱骗态粒子, 并根据测量结果对信道进行安全性检查, 若测量结果的错误率超过约定的阈值, 则认为协议中存在窃听者, 终止本次协议并重新开始; 若没有超过约定的阈值, 则 P_j从序列 S_j'挑选出诱骗粒子并舍弃, 将其恢复成 S_j.

第 3 步 每个参与者 P_j随机挑选一组序列 $r_j=(r_j^0,r_j^1,\cdots,r_j^{d-1}),(r_j^t\in\{0,1,\cdots,d-1\})$, 并对

序列 S_j 的第 t 个粒子进行如 (4) 式所示的时移操作 $U_{r_j^t}(|t\rangle)\,(t=1,2,\cdots,d-1)$ 得到新的粒子序列 S_j^*, P_j 随机挑选诱骗态插入到序列 S_j^* 中得到新的序列 $S_j^{*\prime}$, 并将其返还给 P_i.

第 4 步 在确认 P_i 收到序列 $S_j^{*\prime}$ 后, 双方进行第二次安全性检查, 检查过程与第 2 步类似. 若测量结果的错误率超过约定的阈值, 则认为协议中存在窃听者, 终止本次协议并重新开始; 若没有超过约定的阈值, P_i 舍弃其中的诱骗态恢复序列 S_j^*. 接下来, P_i 用 Z 基测量序列 S_j^* 中的每个粒子并得到 P_j 随机挑选的序列 r_j 的值.

第 5 步 P_j 将其密钥 $K_j=(K_j^0,K_j^1,\cdots,K_j^{d-1})$ 加密为 $K_j^*=(K_j^{0*},K_j^{1*},\cdots,K_j^{d-1*})$, 其中加密规则为 $K_j=K_j^*\oplus r_j$. 随后, P_j 通过认证信道将其发送给 P_i.

第 6 步 P_i 通过序列 r_j 的值和 P_j 发送过来的 K_j^*, 计算得到每个参与者 P_j 的密钥 K_j, 并计算出最终共享密钥 $K=K_0\oplus K_1\oplus\cdots\oplus K_{k-1}$.

2.3 MQKA 协议的一个例子

在本节中, 将给出上述协议的一个特例. 为了方便讲解, 在例子中并不考虑两次安全检查. 首先, 令 $k=3$, $l=3$, $d=2l+1=7$. 其次, 假设 3 个参与者 P_0, P_1, P_2 的密钥分别为 $K_0=(1,3,2,2,3,1,2)$, $K_1=(3,1,2,1,1,3,2)$, $K_2=(2,3,2,2,1,3,1)$, 以 P_0 为例.

第 1 步 P_0 准备好 m 个 7 维三粒子 GHZ 态 $|\Psi\rangle_{0,1,2}=\dfrac{1}{3}(|0\rangle|0\rangle|0\rangle+|1\rangle|1\rangle|1\rangle+\cdots|6\rangle|6\rangle|6\rangle)_{0,1,2}$, 并将其分成 3 个粒子序列: S_0, S_1, S_2. 随后, P_0 将 S_0 留在手中, 将 S_1 发送给 P_1, 将 S_2 发送给 P_2.

第 2 步 P_1, P_2 分别随机挑选一组序列 $r_1=(1,3,5,3,4,2,3)$, $r_2=(3,6,2,3,1,4,5)$, 并分别对其持有的粒子序列 S_1, S_2 的第 t 个粒子执行时移操作 $U_{r_1^t}(|t\rangle)$, $U_{r_2^t}(|t\rangle)$. 随后, 将操作后的粒子序列发给 P_0.

第 3 步 此时, P_0 拥有的 3 粒子 GHZ 态 $|\Psi\rangle_{0,1,2}$ 变为

$$\begin{aligned}|\Psi\rangle_{0,1,2}=&\frac{1}{3}(|0\rangle|0+r_1^0\rangle|0+r_2^0\rangle+|1\rangle|1+r_1^1\rangle|1+r_2^1\rangle\\&+\cdots|6\rangle|6+r_1^6\rangle|6+r_2^6\rangle)_{0,1,2}\\=&\frac{1}{3}(|0\rangle|1\rangle 3+|1\rangle|4\rangle|0\rangle+\cdots|6\rangle|2\rangle|5\rangle).\end{aligned}\tag{6}$$

P_0 用 Z 基测量 $|\Psi\rangle_{0,1,2}$ 中的每个粒子并得到序列 r_1 和 r_2 的值.

第 4 步 P_1, P_2 分别将其密钥 K_1, K_2 加密为 $K_1^*=(2,5,4,5,4,1,6)$, $K_2^*=(6,4,0,6,0,6,3)$, 通过认证信道将其发送给 P_0.

第 5 步 P_0 通过序列 r_1, r_2 的值和 P_j 发送过来的 K_1^*, K_2^*, 计算得到 P_1, P_2 的密钥 K_1, K_2, 并计算出最终共享密钥 $K=K_0\oplus K_1\oplus K_2=$ (6, 0, 6, 5, 5, 0, 5).

3 安全性分析

QKA 协议主要涉及两类攻击: 参与者攻击和外部攻击. 其中外部攻击又可以分为木马攻击、截取重发攻击. 为了证明这些协议的安全性, 将根据这两种攻击来讨论.

3.1 参与者攻击

假设参与者 P_0 为不诚实者, 想要获取其他参与者的密钥. 首先, P_0 需要得到序列 r_j. 然而, r_j 为 P_j 随机选择的序列, 故 P_0 只能够通过在协议的第 3 步进行截取重发攻击获得粒子序列 S_j^*. 此时, 参与者攻击可看成外部攻击, 并且其攻击将会在协议的第二次安全检查中被发现, 造成协议的失败. 而在第 5 步中, 其传输是通过认证的量子信道, 故 P_0 不能获得任何关于 r_j 的信息. 此协议可以抵抗内部参与者攻击.

3.2 外部攻击

假设 Eve 是外部攻击者, 她需要窃听 r_j 和 K_j^* 的信息来获得共享密钥. 可能的主要攻击方法有特洛伊木马攻击、拦截重发攻击和纠缠测量攻击.

特洛伊木马攻击. 由于这个改进的协议是一个单向的 QKA 协议, 所有的粒子序列只在信道中传输一次, 特洛伊木马攻击者没有机会从粒子序列中提取出间谍光子. 也就是说, 改进的协议可以不需要使用任何特定的检测设备, 从而能够抵抗两种类型的攻击特洛伊木马攻击[35,36].

拦截重发攻击. 若 Eve 想要对在信道中传输的粒子序列 S_j' 和 $S_j^{*\prime}$ 执行拦截重发攻击, 则她必须对此序列进行拦截并发送伪随机序列. 然而, Eve 在窃听检查之前并不知道诱骗逻辑粒子的位置和相应的测量基, 因此 Eve 仅有 $1/d$ 的机率能够正确测量出诱骗态的值, 假定每次序列制备的诱骗

粒子数是τ, 则其被发现的概率为$1-(1/d)^{\tau}$, 可知当τ足够大时, 参与者可以轻易地发现窃听者的存在. 而一旦发现了窃听者, 便终止本次协议并重新开始. 所以 Eve 是几乎不可能通过截取重发攻击获得最终密钥.

纠缠测量攻击. 在两个协议中, 假设 Eve 想要利用自己事先准备的辅助光子$|\varepsilon\rangle_{\mathrm{E}}$对 QKA 协议进行纠缠测量攻击, 则她需要对截获的量子态执行幺正操作U_{E}使之与辅助光子产生纠缠. 以免疫集体退相位噪声的 QKA 协议为例, 结果如下.

$$\begin{aligned} U_{\mathrm{E}}|0\rangle|\varepsilon\rangle_{\mathrm{E}} &= a|0\rangle|\varepsilon_{00}\rangle_{\mathrm{E}} + b|1\rangle|\varepsilon_{01}\rangle_{\mathrm{E}}, \\ U_{\mathrm{E}}|1\rangle|\varepsilon\rangle_{\mathrm{E}} &= c|0\rangle|\varepsilon_{10}\rangle_{\mathrm{E}} + d|1\rangle|\varepsilon_{11}\rangle_{\mathrm{E}}, \end{aligned} \tag{7}$$

$$\begin{aligned} &U_{\mathrm{E}}(|+\rangle|\varepsilon\rangle_{\mathrm{E}}) = \\ &\frac{1}{2}\left[|+\rangle(a|\varepsilon_{00}\rangle_{\mathrm{E}} + b|\varepsilon_{01}\rangle_{\mathrm{E}} + c|\varepsilon_{10}\rangle_{\mathrm{E}} + d|\varepsilon_{11}\rangle_{\mathrm{E}})\right] \\ &+ \frac{1}{2}\left[|-\rangle(a|\varepsilon_{00}\rangle_{\mathrm{E}} - b|\varepsilon_{01}\rangle_{\mathrm{E}} + c|\varepsilon_{10}\rangle_{\mathrm{E}} - d|\varepsilon_{11}\rangle_{\mathrm{E}})\right], \end{aligned} \tag{8}$$

$$\begin{aligned} &U_{\mathrm{E}}(|-\rangle|\varepsilon\rangle_{\mathrm{E}}) = \\ &\frac{1}{2}\left[|+\rangle(a|\varepsilon_{00}\rangle_{\mathrm{E}} + b|\varepsilon_{01}\rangle_{\mathrm{E}} - c|\varepsilon_{10\mathrm{E}} - d|\varepsilon_{11}\rangle_{\mathrm{E}})\right] \\ &+ \frac{1}{2}\left[|-\rangle(a|\varepsilon_{00}\rangle_{\mathrm{E}} - b|\varepsilon_{01}\rangle_{\mathrm{E}} - c|\varepsilon_{10\mathrm{E}} + d|\varepsilon_{11}\rangle_{\mathrm{E}})\right], \end{aligned} \tag{9}$$

其中$|a|^2+|b|^2=1$, $|c|^2+d^2=1$. Eve 为了避免引入错误, 必须满足

$$\begin{aligned} a|\varepsilon_{00}\rangle_{\mathrm{E}} + c|\varepsilon_{10}\rangle_{\mathrm{E}} &= b|\varepsilon_{01}\rangle_{\mathrm{E}} + d|\varepsilon_{11}\rangle_{\mathrm{E}}, \\ a|\varepsilon_{00}\rangle_{\mathrm{E}} - c|\varepsilon_{10}\rangle_{\mathrm{E}} &= b|\varepsilon_{01}\rangle_{\mathrm{E}} + d|\varepsilon_{11}\rangle_{\mathrm{E}}. \end{aligned} \tag{10}$$

(10) 式必须满足三个条件: $a=d=1$, $b=c=0$, $|\varepsilon_{00}\rangle_{E}=|\varepsilon_{11}\rangle_{E}$. 则 (7) 式变为

$$\begin{aligned} U_{\mathrm{E}}(|0\rangle|\varepsilon\rangle_{\mathrm{E}}) &= |0\rangle|\varepsilon_{00}\rangle_{\mathrm{E}}, \\ U_{\mathrm{E}}(|1\rangle|\varepsilon\rangle_{\mathrm{E}}) &= |1\rangle|\varepsilon_{11}\rangle_{\mathrm{E}}. \end{aligned} \tag{11}$$

显然, 仅当辅助状态和目标粒子$\{|0\rangle, |1\rangle\}$是乘积状态时, Eve 不会引入任何错误. 因此, 此协议可以抵抗外部攻击.

从本节的分析可以得出, 我们的协议不但能够抵抗内部参与者的攻击, 还能够抵抗外部窃听者的攻击. 而当内部攻击与外部攻击同时发生时, 协议能够通过进程及时知晓, 并及时止损, 不造成任何信息的泄露.

4 效率分析

正如 Cabello 在文献 [37] 中所述, QKA 协议的量子比特效率可以定义为$\eta=\dfrac{c}{q+b}$. 其中, c是最终密钥的长度, q是所用量子比特的数目, b是用于生成最终密钥所用经典比特的数目. 在本方案中, 准备了 m个 d维 k粒子 GHZ 态, 在每次量子序列的传输过程中插入 d个诱骗粒子. 因此本方案的量子比特效率$\eta=\dfrac{md}{mdk+2mdk}=\dfrac{1}{3k}$. 同时, 我们的协议与其他多方 QKA 协议的比较如表 1 所列. 相比于其他协议, 我们的协议也有着较高的量子比特效率.

表 1 本文协议和其他协议比较

Table 1. Comparison between our protocols and the other protocols.

QKA protocol	Quantum resource	Qubit efficiency
Liu et al.'s protocols[10]	GHZ states	$1/[2k(k-1)]$
Xu et al.'s protocols[12]	Single photons	$1/[2k(k-1)]$
Sun et al.'s protocols[14]	Six-qubit states	$1/(2k)$
Our protocol	GHZ states	$1/(3k)$

5 结 论

本文基于 d维 k粒子 GHZ 态提出了一个多方量子密钥协商方案. 通过时移操作将密钥编码到序列中, 并以 d维 Z基测量得到序列中的密钥, 最后对所有参与者的密钥进行异或操作建立共享密钥. 安全性分析表明我们的方案能够有效地抵抗内部参与者和外部窃听者的攻击. 然而, 我们的协议提出的前提是基于理想环境下的量子信道. 在实际应用中, 粒子在有噪量子信道传输过程中, 通常会受到噪声的影响. 因此, 在将来如何使本协议适应更加复杂的环境是我们研究的重点.

参考文献

[1] Zhou N, Zeng G, Xiong J 2004 *Electron. Lett.* **40** 1149
[2] Chong S K, Hwang, T 2010 *Opt. Commun.* **283** 1192
[3] Huang W, Su Q, Wu X, Li Y B, Sun L 2014 *Int. J. Theor. Phys.* **53** 2891
[4] Shen D S, Ma W P, Wang L L 2014 *Quantum Inf. Process.* **13** 2313
[5] He Y F, Ma W P 2015 *Quantum Inf. Process.* **14** 3483
[6] He Y F, Ma W P 2017 *Int. J. Quantum Inf.* **3** 1750018
[7] Yang Y G, Li B R, Li D, Zhou Y H, Shi W M 2019 *Quantum Inf. Process.* **18** 322
[8] Zhou Y H, Wang M F, Shi W M, Yang Y G, Zhang J 2020 *Quantum Inf. Process.* **19** 100
[9] Shi R H, Zhong H 2013 *Quantum Inf. Process* **12** 921

[10] Liu B, Gao F, Huang W, Wen Q Y 2013 *Quantum Inf. Process.* **12** 1797
[11] Sun Z, Zhang C, Wang B H, Li Q, Long D Y 2013 *Quantum Inf. Process.* **12** 3411
[12] Yin X R, Ma W P, Shen D S, Wang L L 2013 *Acta Phys. Sin.* **62** 170304 (in Chinese) [尹逊汝, 马文平, 申冬苏, 王丽丽 2013 物理学报 **62** 170304]
[13] Xu G B, Wen Q Y, Gao F, Qin S J 2014 *Quantum Inf. Process.* **13** 2587
[14] Sun Z, Zhang C, Wang P, Yu J P, Zhang Y, Long D Y 2016 *Int. J. Theor. Phys.* **55** 1920
[15] Sun Z, Yu J, Wang P 2016 *Quantum Inf. Process.* **15** 373
[16] Cai T, Jiang M, Cao G 2018 *Quantum Inf. Process.* **17** 103
[17] Lin S, Guo G D, Chen A M, Liu X F 2019 *Quantum Inf. Process.* **18** 1
[18] Liu H N, Liang X Q, Jiang D H, Zhang Y H, Xu G B 2019 *Quantum Inf. Process.* **18** 242
[19] Zhou N R, Zhu K N, Wang Y Q 2020 *Int. J. Theor. Phys.* **59** 663
[20] Huang W, Wen Q Y, Liu B, Su Q, Gao F 2014 *Quantum Inf. Process.* **13** 1651
[21] Cai B B, Guo G D, Lin S 2017 *Int. J. Theor. Phys.* **56** 1039
[22] Min S Q, Chen H Y, Gong L H 2018 *Int. J. Theor. Phys.* **57** 1811
[23] Wang S S, Xu G B, Liang X Q 2018 *Int. J. Theor. Phys.* **57** 3716
[24] Zhao X Q, Zhou N R, Chen H Y, Gong L H 2019 *Int. J. Theor. Phys.* **58** 436
[25] Liu H N, Liang X Q, Jiang D H, Zhang Y H, Xu G B 2019 *Int. J. Theor. Phys.* **58** 1659
[26] Yin X R, Ma W P 2019 *Int. J. Theor. Phys.* **58** 631
[27] Zhou Y H, Zhang J, Shi W M, Yang Y G 2020 *Mod. Phys. Lett. B* **4** 2050083
[28] Wang W, Zhou B M, Zhang L 2020 *Int. J. Theor. Phys.* **59** 1944
[29] Tang J, Shi L, Wei J H 2020 *Mod. Phys. Lett. B* **49** 2050201
[30] Bouwmeester D, Pan J W, Daniell M, Weinfurte H, Zeilinger A 1999 *Phys. Rev. Lett.* **82** 1345
[31] Zhou N R, Chong S H, Gong L H, Liu Y 2012 *Acta Phys. Sin.* **61** 214203 (in Chinese) [周南润, 宋汉冲, 龙黎华, 刘晔 2012 物理学报 **61** 214203]
[32] Zhang Z J, Man Z X, Shi S H 2005 *Int. J. Quantum Inf.* **03** 555
[33] Hwang T, Hwang C C, Li C M 2011 *Phys. Scripta* **83** 045004
[34] Kao S H, Tsai C W, Tzonelih H 2011 *Commun. Theor. Phys.* **55** 1007
[35] Cai Q Y 2006 *Phys. Lett. A* **351** 23
[36] Deng F G, Li X H, Zhou H Y, Zhang Z J 2005 *Phys. Rev. A* **72** 044302
[37] Cabello A 2000 *Phys. Rev. Lett.* **85** 5633

Multi-party quantum key agreement based on *d*-level GHZ states*

Tang Jie Shi Lei Wei Jia-Hua† Yu Hui-Cun
Xue Yang Wu Tian-Xiong

(*Institute of Information and Navigation, Air Force Engineering University, Xi'an* 710077, *China*)

(Received 27 May 2020; revised manuscript received 30 June 2020)

Abstract

A multi-party quantum key agreement protocol based on *d*-level multi-particle GHZ states is proposed. The "*d*-level" is common in other quantum cryptographic protocols, but there are few researches in the field of quantum key agreement. In our scheme, we introduce two indistinguishable orthogonal bases, i.e. the quantum Fourier transform and shift operation, into a *d*-level quantum system. In addition, we make full use of shift operation to encode the key into the sequence of quantum states, and the key can be measured by the *d*-level *Z*-basis. By decoding and calculating, each participant can equally extract other participants' key and obtain the final shared key $K = K_0 \oplus K_1 \oplus \cdots \oplus K_{k-1}$. The protocol resists external eavesdropping by inserting decoy states and conducting two security checks. Furthermore, we present an example by assigning certain values to parameters for illustrative purpose. Finally, QKA protocol mainly involves two types of attacks: participant attack and external attack. The external attack can be divided into Trojan attack, intercept-resend attack, and entangle-measure attack. To demonstrate the security of the scheme, we analyze the two types of attacks. The results show that the scheme can effectively resist the attack from internal participants and external eavesdroppers. However, the premise of our protocol is based on the ideal quantum channel. In practical applications, particles are usually affected by noise in the process of quantum channel transmission. Therefore, how the agreement adapts itself to a more complicated environment is our main work in the future.

Keywords: *d*-level, multi-party quantum key agreement, shift operation, security analysis

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.69.20200799

* Project supported by the National Natural Science Foundation of China (Grant No. 61971436) and the Young Scientists Fund of the National Natural Science Foundation of China (Grant No. 61803382).

† Corresponding author. E-mail: weijiahua@126.com