物理学报 Acta Physica Sinica

Chinese Physical Society
Institute of Physics, CAS

基于量子图态的量子秘密共享

梁建武 程资 石金晶 郭迎

Quantum secret sharing with quantum graph states

Liang Jian-Wu Cheng Zi Shi Jin-Jing Guo Ying

引用信息 Citation: Acta Physica Sinica, 65, 160301 (2016) DOI: 10.7498/aps.65.160301
在线阅读 View online: http://dx.doi.org/10.7498/aps.65.160301
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2016/V65/I16

基于量子图态的量子秘密共享*

梁建武 程资 石金晶[1)†] 郭迎

(中南大学信息科学与工程学院, 长沙 410000)

(2016 年 4 月 20 日收到; 2016 年 5 月 17 日收到修改稿)

本文基于量子图态的几何结构特征, 利用生成矩阵分割法, 提出了一种量子秘密共享方案. 利用量子图态基本物理性质中的稳定子实现信息转移的模式、秘密信息的可扩展性以及新型的组恢复协议, 为安全的秘密共享协议提供了多重保障. 更重要的是, 方案针对生成矩阵的循环周期问题和因某些元素不存在本原元而不能构造生成矩阵的问题提出了有效的解决方案. 在该方案中, 利用经典信息与量子信息的对应关系提取经典信息, 分发者根据矩阵分割理论获得子秘密集, 然后将子秘密通过酉操作编码到量子图态中, 并分发给参与者, 最后依据该文提出的组恢复协议及图态相关理论得到秘密信息. 理论分析表明, 该方案具有较好的安全性及信息的可扩展性, 适用于量子网络通信中的秘密共享, 保护秘密数据并防止泄露.

关键词: 量子秘密共享, 图态, 生成矩阵, 组恢复协议

PACS: 03.67.–a, 03.67.Ac, 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.65.160301

1 引 言

秘密共享是实现信息安全通信的一种重要途径, 其在信息安全领域里有着重要应用, 如: 数据安全、军事控制及财政管理. 所谓秘密共享, 就是多人共享某个秘密信息, 当其中的某些或者全部被授权的参与者合作时即可恢复原秘密. 秘密共享分为经典秘密共享和量子秘密共享. 1979 年, Shamir [1] 基于 LaGrange 内插多项式提出了经典的秘密共享理论, 可以实现有效且相对安全的密钥管理, 避免权利过分集中所带来的缺陷, 也称为门限密钥分散管理方案, 简称门限方案. 随着人类计算能力的逐步提升, 很多的研究逐步转向了量子信息领域, 如: 量子纠缠特性 [2–4] 的应用, 量子密钥分发 [5,6] 的研究, 量子安全直接通信 [7] 以及基于中国剩余定理 [8]、高效多方 [9] 量子秘密共享 (quantum secret sharing, QSS) 方案的提出. 这些量子方案很好地弥补了经典领域的不足, 保证了信息和秘密数据的绝对安全性. 随着纠错码理论与加密课题的结合, 开始考虑是否可以将纠错码理论用在秘密共享中. 1997 年, 李元兴和王新梅 [10] 提出了一种基于矩阵分割法的秘密共享方案, 并给出了构造一个成功的门限方案的一般化方法; 2008 年, 梅挺等 [11] 分析了利用最大距离可分 (maximum distance separable, MDS) 码构造门限方案的充要条件; 后来基于极小线性码 [12] 的秘密共享方案在 2013 年被提出, 该方案具有很好的接入结构. 进而考虑是否可以将基于线性分组码的算法应用到量子领域中, 这样就可以由量子力学来保证信息的完整性, 突破经典领域中基于计算复杂度的安全性的限制.

许多量子秘密共享方案中, 安全性大都是依赖于秘密拆分算法或者传输协议, 并没有考虑将初始秘密复杂化. 而在经典领域中, 矩阵分割法的应用可以实现秘密信息的可扩展性, 提高了编码多样性, 同时提高了破译难度, 因此, 引入矩阵分割算法是量子秘密共享方案设计的一种突破及趋势. 另外, 为了便于将量子态及访问结构图形化, 引入了

* 国家自然科学基金 (批准号: 61379153, 61401519, 61572529)、中国博士后科学基金 (批准号: 2013M542119, 2014T70772) 和湖南省科技计划 (批准号: 2015RS4032) 资助的课题.

† 通信作者. E-mail: shijinjing@csu.edu.cn

图态理论. 图态, 就是用图形来表示一个多粒子纠缠态[13], 其优势在于简单的图形表述、稳定子特性及其在计算[14]和纠错等[15]信息处理方面的实际应用. 结合这两方面的创新及优势, 提出了矩阵分割算法和图态相结合的秘密共享方案. 方案中, 定义了两种组恢复协议, 用来恢复子秘密信息, 并解决了生成矩阵的循环周期及其构造问题. 再者, 利用量子比特的测不准原理、不可克隆性及不可区分性等物理性质, 优化了基于计算复杂度的经典方案, 很大程度上确保通信是绝对安全的.

本方案利用酉操作从量子信息中获取经典信息, 进而通过生成矩阵分割法将其进行子秘密的划分; 子秘密的恢复过程采用所提出的门限组恢复, 通过可信中心和合法参与者的联合测量得到子秘密序列, 最后可信中心根据解密算法和对应关系将初始秘密恢复出来. 方案安全性和可靠性依赖于秘密信息的可扩展性、稳定子的转移特性及新型的秘密恢复策略. 第2部分介绍了量子图态理论及其信息转移算法; 第3部分介绍了整个方案的流程及详细步骤; 第4部分从算法和转移特性两个方面对方案的安全性及可行性进行了理论分析; 最后介绍了本方案的结论及可应用情景.

2 量子图态理论及其信息转移算法

图态是一种可以用数学图形来表述的态, 是一种纠缠态. 继量子计算出现以来, 人们越来越关注于制备图态的理论与实验. 在2004年, Nielsen[16]首次提出了关于制备图态的非确定性量子门理论. 之后, 专家们相继制备出光子簇态[17]及六原子GHZ态等[18]. 良好的纠缠特性和娴熟的实验制备技术是图态得以广泛应用的重要支撑. 图态是有很多种类的, 如: Bell态, GHZ态, 簇态及带有权值的图态等.

在本方案中, 采用带有权值的量子图态来进行信息的传递及恢复. 其中, 权值表示的是参与者之间的联系强度, 并且方案是在一个有限域 $GF(q)$ 中进行的, 其中 $q(q<2)$ 是一个素数, 一个带权值的无向图如下:

$$G=(V,E), \tag{1}$$

其中, $V=v_i$, $E=e_{ij}=(v_i,v_j)$. 每条边会被赋予权值 $A_{ij}(A_{ij}\in GF(q))$, 这些权值可以写成邻接矩阵的形式, 若权值为0, 则表示在两个顶点间不存在边.

这里引入了 q 维的图态及其对应的标签. 初始态的一般形式[19]为

$$|G\rangle=\prod_{e_{i,j}\in E}C_{ij}^{A_{ij}}|\bar{0}\rangle^{\otimes n}, \tag{2}$$

其中, $(|j\rangle|j\in GF_q)$, $|\bar{i}\rangle=U^{-1}|i\rangle, i\in GF_q$, 且酉操作满足

$$U|i\rangle=\sum_{j\in F_d}\omega^{ij}|j\rangle, \tag{3}$$

两粒子控制 Z 操作定义为

$$C_{ab}|j\rangle_a|k\rangle_b=\omega^{jk}|j\rangle_a|k\rangle_b, \tag{4}$$

图态被编码信息后称为标记图态. 在一个标记图态中, 每个顶点 v_i 带有一个标签 $l_i=(z_i,x_i,s_i)(z_i,x_i,s_i\in GF_q)$, 通过采用 $S_i^{m_i}X_i^{x_i}Z_i^{z_i}$ 操作来实现图态的编码操作. 标记图态可以写成

$$|G_l\rangle=\bigotimes_i S_i^{m_i}X_i^{x_i}Z_i^{z_i}|G\rangle. \tag{5}$$

一般化的泡利操作[20]是:

$$\begin{aligned}Z|j\rangle&=\omega^j|j\rangle,\\X|j\rangle&=|j+1\rangle,\\S|j\rangle&=\omega^{j(j-1)/2}|j\rangle,\end{aligned} \tag{6}$$

其中, $\omega=\mathrm{e}^{2\pi i/d}$. 标记图态可以表述成稳定子的形式, 每个顶点满足

$$K_i|G_l\rangle=\omega^{-z_i}|G_l\rangle, i\in V, \tag{7}$$

其中, 稳定子满足

$$K_i=(XZ^{m_i})_iZ^{A_i}. \tag{8}$$

量子图态性质中, 利用稳定子可以进行标记的转移. 值得注意的是, 标记的转移并不意味着执行任何操作或改变态的形式, 类似于对图态的重新标记, 标记的变化满足定理1[19].

定理1 假设参与者 i, j 是邻居, 当对标记态 $|G_l\rangle$ 执行 $K_j^{-A_{ij}^{-1}z_i}$ 测量时, $|G_l\rangle$ 将重新标记为 $|G_{l'}\rangle$. 其中, 顶点 i 重新标记为 $z_i'=0$, 顶点 j 重新标记为 $(z_j',x_j')=(z_j,-A_{ij}^{-1}z_i)$, 并且任意一个顶点 j 的邻居 k 将标记为 $z_k'=z_k-A_{ij}^{-1}A_{jk}z_i$.

为确保子秘密恢复的安全性, 在 nGHZM 态[21]的基础上进一步提出了 Group-Recovery (GR) 的概念, 为方案提供理论基础.

定理2 $(n+1)$GHZM图态记为$|g_{(n+1)\mathrm{GHZM}}\rangle$, 每个顶点$v_i$满足

$$|g_{(n+1)\mathrm{GHZM}}\rangle=[V=v_1,v_j,E=v_1,v_{j\neq1}], \quad (9)$$

并且各个顶点的度为

$$N(u)=\begin{cases}n, & u=v_1,\\ 1, & u=v_j, \quad j\in(2,n+1).\end{cases} \quad (10)$$

其中, v_1可以看作一个可信中心, v_j代表参与者. 当顶点v, 稳定子K_j及子秘密z_j满足

$$v_1+v_j\to K_jz_j, \quad j\in(2,n+1), \quad (11)$$

上式表述了当参与者1和参与者j通过K_j为一组, 进行联合测量时, 可以获得子秘密z_j. 为了更加形象和便捷地表示子秘密的获取方式, 定义了组恢复协议的概念.

1) 全组恢复(full-group-recovery, FGR). 可信中心必须获取到所有的子秘密, 并且通过对应的解密算法才可以将初始秘密恢复出来的情形, 称之为全组恢复, 也可称为n-GR.

2) 门限组恢复(threshold-group-recovery, TGR)当且仅当可信中心获取任意m个子秘密, 就可以恢复出原秘密的情形, 称之为门限组恢复, 也可以记为(m,n)-GR.

3 秘密共享方案

本方案首次将矩阵分割法与图态相结合的思想应用到量子领域中. 为了便于分析与表述, 以$(3,6)$门限方案为例来进行方案描述, 见图1. 基于图态和矩阵分割法有限域的限制, 取$q=7$, 即, 协议在有限域$GF(7)$中进行.

1) 子秘密的产生. 分发者dealer想要共享的量子态秘密为

$$|\varphi_m\rangle=\alpha|0\rangle+\beta|1\rangle. \quad (12)$$

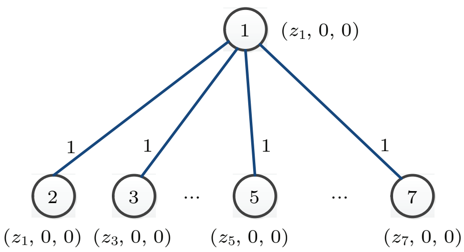

图1 参与者及其“持有”的子秘密分布图

Fig. 1. The distribution of secrets held by participants.

其通过采用三种酉操作来实现对秘密态的加密, 即$\delta_x,\delta_y,\delta_z$, 见表1(加密算符的编码规则: 选择该操作则编码为1, 不选择对应操作则编码为0, 显然有八种状态. 因为实例方案是基于6人参与的, 所以给出了六种状态下的二进制编码). 假设分发者随机使用001(十进制为1)这组对应的操作来加密秘密态, 即采用了δ_z来加密信息$|\varphi_m\rangle$, 则加密后的秘密态为

$$|\psi_m\rangle=\delta_z|\varphi_m\rangle=\alpha|0\rangle-\beta|1\rangle. \quad (13)$$

然后将加密后的量子态进行安全的存储, 并将001对应的十进制数值1作为要共享的经典秘密, 即$s=1$.

表1 操作算符的二进制和十进制码

Table 1. Binary and decimal codes of operators.

DEC	1	2	3	4	5	6
δ_x	0	0	0	1	1	1
δ_y	0	1	1	0	0	1
δ_z	1	0	1	0	1	0

根据矩阵分割算法[10]:

$$\boldsymbol{V}=\boldsymbol{U}\boldsymbol{P}, \quad (14)$$

其中, 生成矩阵$\boldsymbol{P}_{k\times n}=[\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_n]$, 信息矢量$\boldsymbol{U}=[u_0,u_1,\cdots,u_{k-1}]$, 秘密矢量$\boldsymbol{V}=[v_1,v_2,\cdots,v_k]$. 因为是$(3,6)$门限方案, 有$k=3$, 则秘密矩阵$\boldsymbol{U}_{1\times k}=[u_0,u_1,\cdots,u_k]=[u_0,u_1,u_2]$, 令$\boldsymbol{A}_0^{\mathrm{T}}=(100)$, 由$s=\boldsymbol{U}\boldsymbol{A}_0=u_0$, $s=1$, 则u_0应该设置为1, u_1, u_2可在1—6的数值中任意选取, 只要满足三个数值互不相同即可, 这里假定分发者选择的$\boldsymbol{U}=[u_0,u_1,u_2]=[1,2,3]$. 在$GF(7)$域中, 构造$(3,6)$RS码的生成矩阵$\boldsymbol{P}$, $GF(7)$的一个n次本原元是3, 则生成矩阵可以写成

$$\boldsymbol{P}=\begin{pmatrix}1 & 1 & 1 & 1\\ \alpha & \alpha^2 & \cdots & \alpha^n\\ \alpha^2 & \alpha^4 & \cdots & \alpha^{2n}\\ \vdots & \vdots & \vdots & \vdots\\ \alpha^{k-1} & \alpha^{2(k-1)} & \cdots & \alpha^{2n(k-1)}\end{pmatrix}$$
$$=\begin{pmatrix}1&1&1&1&1&1\\3&2&6&4&5&1\\2&4&1&2&4&1\end{pmatrix}, \quad (15)$$

其中, α 为此有限域中的 n 次本原根. 由 $\boldsymbol{V}=\boldsymbol{UP}$, 则子秘密矩阵为

$$\begin{aligned}\boldsymbol{V}&=[v_1,v_2,v_3,v_4,v_5,v_6]\\&=[6,3,2,1,2,6].\end{aligned}\tag{16}$$

2) 编码图态. 分发者得到子秘密矩阵 $\boldsymbol{V}$ 后, 需要将其编码在图态 $|G_l\rangle$ 上. 分发者将子秘密信息通过标记的形式, 对图态实现编码的操作, 如 $v_1=6$ 时, $l_2=(6,0,0)$, 即将子秘密 v_k 编码在 z_{k+1} 的位置上. 通过类似的操作得到其他的标签, 同时可信中心的标签为 $l_1=(0,0,0)$, 进而通过对应的泡利操作得到标记图态:

$$|G_l\rangle=\otimes_i Z_i^{z_i}|G\rangle,\quad i\in(1,n),\quad n=7.\tag{17}$$

图态的稳定子可以写成

$$K_1=X_1\prod_{i\neq1}Z_i,\quad K_i=X_iZ_1,\quad i\neq1.\tag{18}$$

3) 传输过程及恢复过程. 通过量子信道, 将量子态分发给参与者, 如图1所示. 传输过程的安全性是量子态的测不准原理和不可克隆性保证的. 通过定理2中定义的门限组恢复协议可知: 可信中心1与任意3个其他参与者合作可以得到3个子秘密信息, 如: 根据(7)式, 当可信中心1与参与者2合作时, 两者需要通过稳定子 $K_2=X_2Z_1$ 进行联合测量, 并得到测量结果 ω^{-6}. 假设可信中心1获取到三个子秘密为 $\boldsymbol{V}'=[v_1,v_2,v_3]=[6,3,2]$, 此时对应的满秩矩阵为

$$\boldsymbol{P}'=\begin{pmatrix}1&1&1\\3&2&6\\2&4&1\end{pmatrix},\tag{19}$$

则可以得到秘密矩阵为

$$\boldsymbol{U}=\boldsymbol{V}'\boldsymbol{P}'^{-1}=[1,2,3].\tag{20}$$

其中关于 $\boldsymbol{P}'^{-1}$ 的运算, 注意是要遵循有限域中的运算规则. 得到秘密矩阵 $\boldsymbol{U}$ 后, 可知 $s=\boldsymbol{UA}_0=1$. 通过表1, 可知选择的对应酉操作是 δ_z^*, 则通过酉操作的性质 $\delta_z\delta_z^*=\boldsymbol{I}$, 可知

$$\begin{aligned}|\varphi\rangle=&\delta_z^*|\psi_m\rangle=\delta_z^*\delta_z|\varphi_m\rangle=|\varphi_m\rangle\\=&\alpha|0\rangle+\beta|1\rangle.\end{aligned}\tag{21}$$

这样就实现了秘密的恢复过程. 此方案还可以实现同时共享两个秘密的情况, 根据纠错码及扩展校验理论[10]可知: $[s_1,s_2]=\boldsymbol{UA}_0=[u_0,u_{k-1}]$, 然后通过该协议就可以实现双秘密的共享过程.

4 协议的安全性分析

4.1 算法的安全性分析

4.1.1 门限方案的可行性及破译分析

在本方案中, 将初始秘密设置在秘密矩阵 $\boldsymbol{U}$ 的第一个位置, 即 u_0. 假设不诚信者或者攻击者Eve想要窃取秘密信息, 且截获到了 $k-1$ 份子秘密时, 通过 $\boldsymbol{V}=\boldsymbol{UP}$ 来求解秘密矩阵 $\boldsymbol{U}$, 此时相当于求解 $k-1$ 个 k 元一次线性方程组, 很显然初始秘密 u_0 是关于某个 u_i 的函数, 因为方案是限定在有限域 $GF(q)$(q 为有限域的阶) 中, 即 u_i 有 q 种取值, 则 u_0 可能存在 q 个解, 则信息熵[10]为

$$\begin{aligned}&H(s=u_0|v_{i_1},v_{i_2},\cdots,v_{i_{k-1}})\\&=\log q=H(u_0),\end{aligned}\tag{22}$$

即当获取到 $k-1$ 份子秘密时, 信息的不确定性仍为其本身, 因此通过所获得信息得不到任何关于秘密的信息量. 另一方面, 当攻击者Eve成功截获到 k 份子秘密的时候, 相当于求解 k 个 k 元一次线性方程组, 此时始秘密 u_0 有惟一确定解, 即

$$H(s=u_0|v_{i_1},v_{i_2},\cdots,v_{i_k})=0,\tag{23}$$

综上, 方案满足成功门限方案的必要条件[10], 因此是一个成功的门限方案.

方案解决了生成矩阵的循环周期及本原元不存在问题. 在伽罗华域 $GF(q)$ 中, 当 q 是素数的时候, 满足 $T=q-1$, T 表示循环周期, 此时可以构造任何满足 $k\leqslant n\leqslant T$ 的 (k,n) 门限方案; 当 q 不是素数的时候, 此时的 $T\neq q-1$, 但是可以找到比 q 大的素数, 再进行类似构造, 构造完成后可以将多余的子秘密丢弃, 不参与分配即可, 这样可以解决当某些数据不存在本原元而不能构造生成矩阵的漏洞. 然后确定 $GF(q)$, 进而计算出其 n 次本原根 α 的值.

为了使得攻击者难于采取穷尽搜索法破解到秘密, 需要将 q 尽量取得大一些. 更重要的是方案中应用的门限组恢复协议, 进一步确保方案的安全性. 可信中心是惟一的生成矩阵和子秘密位置的掌控者, 两者均不对外公布. 因此, 倘若攻击者通过某种方式取得了 k 份子秘密 (在各种安全措施下, 可能性微乎其微), 但其并不知晓解密的生成矩阵. 由 $\boldsymbol{V}=[v_1,v_2,\cdots,v_k]=\boldsymbol{UP}'_{k\times k}$, 可知解密的关键

就在于构造解密生成矩阵, 攻击者任意在生成矩阵 G 中抽取 k 列且正好是对应解密矩阵的概率为

$$\frac{1}{A_n^k}\left(A\text{表示排列数, 满足}A_n^k=\frac{n!}{k!}\right),$$

破译完成后, 得到真实秘密的位置的概率为 $1/k$, 因两事件相互独立, 即有破译概率为 $1/(k\times A_n^k)$, 即当 n 和 k 的值越大, 此时的破译可能性越低. 值得注意的是, 如果经典秘密被破译, 但其因得不到加密后的量子态, 也就无法得到真正的秘密.

4.1.2　秘密信息的可扩展性分析

生成矩阵分割法应用的前提是构造一个秘密矩阵 $\boldsymbol{U}$, 而这种前提条件恰恰使得秘密信息可扩展, 秘密矩阵多样化, 并且成为其他量子秘密共享方案所不具备的创新点和优势. 假设初始秘密 $s=1$, 并设定其位置为 u_0, 根据构造规则, 其他位置上的 $u_1,u_2,\cdots,u_{k-1}$ 的值可以设定为有限域中的任意互不重复的数值. 因此秘密矩阵的构造种类满足排列数 A_{n-1}^{k-1}, 其中 n 表示参与者人数, k 为恢复秘密的最少的合法参与者人数. 事实上, 当伽罗华域越大 (可以对应表现在 n 的大小上) 或者恢复秘密的人数 k 越大, 其不确定性就越大, 即传输真实秘密可选取的 u_i 值就越多, 传输相同秘密所构造的秘密矩阵的种类就越多, 自然而然地增加了破译的难度. 下面通过立体树状图的形式, 直观给出了三种门限方案的情况, 如图2所示.

除了特殊取值外, 当参与者总数 n 一定的时候, k 越大, 树状图就越复杂; k 一定的时候, n 越大, 树状图也越复杂. 此时可构造的秘密矩阵 $\boldsymbol{U}$ 的种类就越多. 所以, 提高参与者总数或者合法恢复者人数, 会增加窃取者的破译难度, 从而在一定程度上保证了方案的安全性.

4.2　转移特性的安全性分析

图态的应用, 不仅仅使得方案更利于图形化表述, 更重要的是其中的稳定子形式使得参与者 $k+1$ 与信息 z_k 之间是相互独立的, 即当个人进行测量时, 并不能够获取到自己手中的信息, 因为子秘密信息会随着测量, 通过稳定子操作将秘密转移出去. 值得注意的是, 秘密信息的转移并不意味着任意的物理上的操作或者改变态的本身, 其仅仅是对物理态的重新标记.

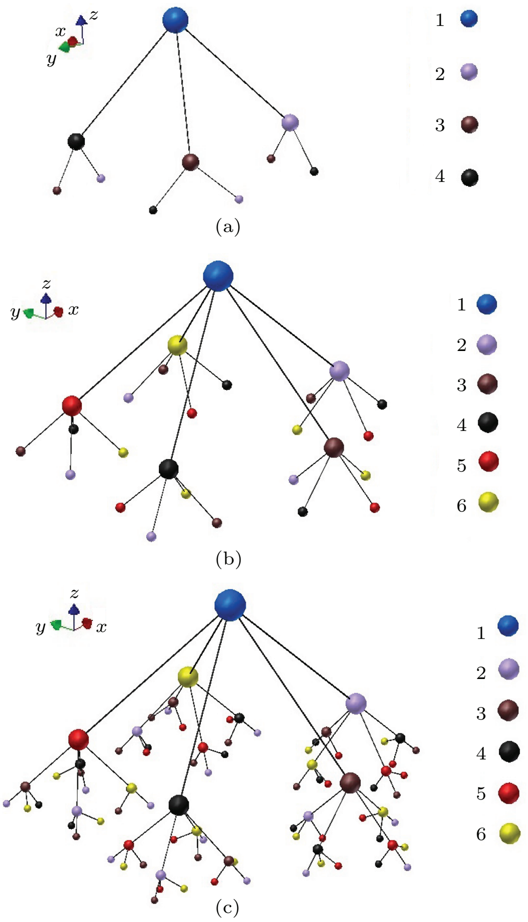

图2　(网刊彩色) 门限方案中所有可能的构造结果 (a) (3, 4) 门限方案; (b) (3, 6) 门限方案; (c) (4, 6) 门限方案

Fig. 2. (color online) All possible matrices in threshold scheme: (a) (3, 4) threshold scheme; (b) (3, 6) threshold scheme; (c) (4, 6) threshold scheme.

假设某个参与者不诚信, 单独进行测量想要获得秘密时, 由定理1可以知: 子秘密信息将会被转移, 量子态将被重新标记, 测量者手中的标记为 $l=(0,0,0)$, 所以该参与者获取不到任何信息, 也称为信息的转移特性. 在如图1所示的标记态中, 信息 z_k 可以通过可信中心1和第 k 参与者的联合测量获得. 以本方案实际参数为例, 给出了当存在不诚信者进行单独测量时信息的转移结果.

假设参与者2为不诚信者, 子秘密信息 $z_2=6$. 不诚信者通过稳定子 K_1^{-6} 测量量子态时, 图态将会被重新标记为 $l_2=(0,0,0)$, $l_1=(0,1,0)$, $l_3=(3,0,0)$, $l_4=(2,0,0)$, $l_5=(1,0,0)$, $l_6=(2,0,0)$, $l_7=(0,0,0)$, 此时, 参与者2手中是没有信息的, 该信息被直接或者间接地转移到其他参与者手中, 其他情况也是类似于这种情形的, 如图3所示. 信息的转移特性使得方案更加安全和可靠.

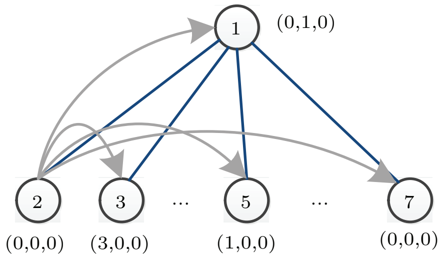

图 3 标记 z_2 的转移

Fig. 3. The transfer of the label z_2.

5 结 论

本文提出了一种基于生成矩阵的图态量子秘密共享方案. 在该方案中, 利用经典信息与量子信息的对应关系提取经典信息, 分发者通过矩阵分割法实现秘密的划分, 然后将子秘密通过酉操作编码到量子图态中, 并分发给参与者. 最后, 秘密重构是基于量子图态理论及门限组恢复协议实现. 秘密信息的可扩展性, 图态中稳定子的转移特性及提出的组恢复协议是方案的最大创新点, 保障了量子通信的安全可靠. 该方案解决了在经典领域中有些元素的本原元不存在而不能构造生成矩阵的问题, 并提出了根据循环周期来限制参与者人数, 使得方案更加严谨. 矩阵分割法的编码多样性以及图态的简单图形表示和稳定子性质使得该方案在量子网络中的密码共享及信息安全领域具备较好的应用前景. 更重要的是这些理论都可以进一步应用在量子签名、认证及密钥分发等量子密码协议中, 可以为安全、多样、扩展性强的量子安全通信协议的设计提供科学的理论方法.

参考文献

[1] Shamir A 1979 *Commun. ACM* **22** 612

[2] Feng L J, Zhang Y J, Zhang L, Xia Y J 2015 *Chin. Phys. B* **24** 103

[3] Zhou N R, Cheng H L, Tao X Y, Gong L H 2014 *Quantum Inf. Process.* **13** 513

[4] Tang S Q, Yuan J B, Wang X W, Kuang L M 2015 *Chin. Phys. Lett.* **32** 040303

[5] Gong L H, Song H C, He C S, Liu Y, Zhou N R 2014 *Phys. Scr.* **89** 240

[6] Sun W, Yin H L, Sun X X, Chen T Y 2016 *Acta Phys. Sin.* **65** 080301 (in Chinese) [孙伟, 尹华磊, 孙祥祥, 陈腾云 2016 物理学报 **65** 080301]

[7] Gong L H, Liu Y, Zhou N R 2013 *Int. J. Theor. Phys.* **52** 3260

[8] Guo Y, Zhao Y 2013 *Quantum Inf. Process.* **12** 1125

[9] Gao G 2014 *Int. J. Theor. Phys.* **53** 2231

[10] Li Y X, Wang X M 1993 *J. Commun.* **14** 22 (in Chinese) [李元兴, 王新梅 1993 通信学报 **14** 22]

[11] Mei T, Dai Q, Zhang M 2008 *Commun. Tech.* **11** 288 (in Chinese) [梅挺, 代群, 张明 2008 通信技术 **11** 288]

[12] Song Y, Li Z H, Li Y M 2013 *Acta Electr. Sin.* **02** 220 (in Chinese) [宋云, 李志慧, 李永明 2013 电子学报 **02** 220]

[13] Briegel H J, Raussendorf R 2001 *Phys. Rev. Lett.* **86** 910

[14] Raussendorf R, Briegel H J 2001 *Phys. Rev. Lett.* **86** 5188

[15] Looi S Y, Li Y, Gheorghiu V, Griffiths R B 2008 *Phys. Rev. A* **78** 042303

[16] Nielsen M A 2004 *Phys. Rev. Lett.* **93** 040503

[17] Kiesel N, Schmid C, Weber U, Tóth G, Gühne O, Ursin R, Weinfurter H 2005 *Phys. Rev. Lett.* **95** 210502

[18] Leibfried D, Knill E, Seidelin S, Britton J, Blakestad R B, Chiaverini J, Hume D B, Itano W M, Jost J D, Langer C, Ozeri R, Reichle R, Wineland D J 2005 *Nature* **438** 639

[19] Keet A, Fortescue B, Markham D, Sander B C 2010 *Phys. Rev. A* **82** 062315

[20] Bartlett S D, de Guise H, Sanders B C 2002 *Phys. Rev. A* **65** 052316

[21] Markham D, Sanders B C 2008 *Phys. Rev. A* **78** 042309

Quantum secret sharing with quantum graph states*

Liang Jian-Wu Cheng Zi Shi Jin-Jing† Guo Ying

(*School of Information Science and Engineering, Central South University, Changsha 410000, China*)

(Received 20 April 2016; revised manuscript received 17 May 2016)

Abstract

Quantum secret sharing is an important way to achieve secure communications, which has critical applications in the field of information security for its physical properties. According to the perspective of the practical applications, improving the confidentiality and integrity of secret sharing schemes is a good method to increase the security and reliability of communications. In this paper, we propose a quantum secret sharing scheme based on generator matrix segmentation and the structural features of quantum graph states. The security of the secure secret sharing scheme is guaranteed by the pattern of transferring information by stabilizers, scalability of the information and new recovery strategy provided by the entanglement of the related graph states. It puts forward an effective solution to the problem of matrix cycle period, where some numbers without the primitive element cannot construct the generation matrix.

First of all, the physical properties of quantum bits (qubits), such as uncertainty principle, no-cloning theorem and indistinguishability, not only optimize the classical schemes but also ensure the absolute safety of communication. Secondly, the application of matrix segmentation makes secret information has better scalability. It improves the coding diversity and the difficulty in deciphering. Thirdly, the favorable entanglement properties and mature experiment preparation techniques of graph states provide an approach to the practical applications. The superiority of the yielded graph states is described in graphical fashion with an elegant stabilizer. Fourthly, the shuffling operation can ensure the independence of the message among participants. Therefore, Eve can not obtain any useful information by measuring randomly. Two group-recovery protocols are proposed to show the secret recovering processing through rebuilding sub-secrets among legal cooperative participants.

In the scheme design, the dealer extracts the classical secret information according to the corresponding principle between the classical and quantum information, and divides the classical secret through generated matrix which is produced with the primitive elements in finite domain satisfying the linear independence for any k column vectors. Then the dealer encodes information into graph states and distributes particles to the legal participants with unitary operations. Subsequently, the credible center obtains sub-secrets by the theory of graph states and the group recovery protocol. He can achieve the initial classical secret via the inverse algorithm of matrix segmentation. After getting the classical secret, he recovers quantum secret according to the relationship between classical information and quantum information.

Theoretical analysis shows that this scheme can provide better security and scalability of the information. It is appropriate to realize the secret sharing in the quantum network communication to protect secrets from eavesdropping. Also, it can provide an approach to designing diverse and scalable quantum secure communication schemes based on quantum graph states, the algorithm of matrix segmentation, and group-recovery protocol.

Keywords: quantum secret sharing, graph states, generated matrix, group-recovery protocol

PACS: 03.67.–a, 03.67.Ac, 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.65.160301

---

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61379153, 61401519, 61572529), the China Postdoctoral Science Foundation (Grant Nos. 2013M542119, 2014T70772), and the Science and Technology Planning Project of Hunan Province, China (Grant No. 2015RS4032).

† Corresponding author. E-mail: shijinjing@csu.edu.cn