基于图态和中国剩余定理的量子秘密共享方案

梁建武，刘晓书，程资
（中南大学信息科学与工程学院，湖南 长沙 410083）

摘 要：受到量子图态几何结构和特性的启发，提出了一种基于图态和中国剩余定理的量子秘密共享方案。在该方案中，分发者在有限域内利用中国剩余定理分发秘密，秘密被编码到量子图态里并且通过酉正操作传送给合法参与者，合法参与者使用群恢复协议合作重建子秘密。该方案提供了一个简洁的方法，即通过使用纠缠图态的稳定子来传递信息，分析显示它能提供更好的信息安全性和性能。

关键词：量子信息；量子秘密共享；图态；中国剩余定理
中图分类号：TN918.1
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2018220

Quantum secret sharing with graph states based on Chinese remainder theorem

LIANG Jianwu, LIU Xiaoshu, CHENG Zi
Institute of Information Science and Engineering, Central South University, Changsha 410083, China

Abstract: Based on the topological features of quantum graph states, a quantum secret sharing scheme based on Chinese remainder theorem with a vivid graphic description was proposed. The dealer extracts sub-secrets according to Chinese remainder theorem over finite field, which were imbedded with quantum graph states and transmitted to the legal participants with unitary operations. Group-recovery protocols were used in the secret recovering processing through rebuilding sub-secrets among legal cooperative participants. Analysis shows that it could provide better security and capability of the information.

Key words: quantum information, quantum secret sharing, graph states, Chinese remainder theorem

1 引言

秘密共享是保证安全通信的一个重要途径，可以表示为一种理论上安全的密码协议，其中，一个秘密被多个参与者共享且可以通过授权参与者的合作被恢复。第一个经典秘密共享理论是由夏米尔提出的基于拉格朗日插值多项式的秘密共享方案[1]，它也被称为阈值的秘密共享方案，该方案可以避免权利过度集中。随着计算机计算能力的逐步发展，尤其是量子并行算法的兴起，许多研究者逐渐开始关注量子信息领域。量子的性质，如海森堡的不确定性原理和非克隆定理，在信息领域有着重要的作用。它可以打破经典信息系统在提高处理速度方面存在的局限性，保证信息安全，提高检测精度和信息容量。1999 年，马克等[2]首先提出了一种基于 GHZ（Greenberger-Horne-Zeilinger）态的量子秘密共享方案（QSS, quantum secret sharing），之后，利用中国剩余定理（CRT，Chinese remainder theorem）[3-4]，多方方案设计[5]和图态方案设计[6-7]一个个被提出。最近，Rahaman 等[8]利用本地分辨率分析提出了一种量子秘密共享方案，Tavakoli 等[9]提出了一种基于 d 维量子系统的秘密共享方案。目前，很多关于量子的研究已取得重大突破，例如，密钥分配[10-11]、多方通信[12]、签名[13-14]和秘密共享等。

现有的量子秘密共享方案大部分是基于 GHZ 态[15-16]或者 Bell 态[17]的，基于图态的方案比较少。

收稿日期：2017−07−01；**修回日期**：2018−06−22

本文结合量子图态和 CRT 的性质提出一种基于量子图态和 CRT 的秘密共享方案。该方案的物理机制采用量子图态，经典秘密分割利用中国剩余定理。量子图态的物理结构有利于该方案的图形表示，其转移特性可以保证方案的安全。CRT 是一种秘密分割的有效方法，提供了一种计算大量数据的方法，可以大大提高计算的速度和计算机的处理效率。如果一个秘密是利用 CRT 分割的，那么它只有通过所有参与者的合作才能被恢复。图态的转移特性、组恢复协议和 CRT 的高效计算性能，为通信的安全可靠提供了多重保护。

2　基本原理

2.1　图态的生成

图态可与数学图形对应，有良好的纠缠特性，且成熟的实验制备技术为其应用提供了条件。本方案是在一个有限域 F_d 中进行的，其中 d（d>2）是一个一阶素数。一个顶点数为 n 的加权无向图如式(1)所示。

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

其中，$V=v_i$，$E=e_{ij}=(v_i,v_j)$。每一个非零边的权重为 $A_{ij}\in F_d$，它们组成了邻接矩阵。权重为 0 意味着 2 个顶点之间不存在边。u（$u\in V$）的邻居数定义为度，记为 $N(u)$，计算式记为

$$deg=\left|N(u)\right| \tag{2}$$

d 维图态的计算基的初始定义如式(3)所示。

$$\left|G\right\rangle=\prod_{e_{i,j}\in E}C_{ij}^{A_{ij}}\left|\bar{0}\right\rangle^{\otimes n} \tag{3}$$

其中，

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

$$\left|\bar{i}\right\rangle=U^{-1}\left|i\right\rangle,i\in F_d \tag{5}$$

$$U\left|i\right\rangle=\sum_{j\in F_d}\omega^{ij}\left|j\right\rangle,\ j\in F_d \tag{6}$$

2.2　图态的编码过程

如果每个顶点 v_i 在有限域 F_d 内通过酉操作得到标签 $l_i=(z_i,x_i,s_i)$，其中，$z_i,x_i,s_i\in F_d$。那么标签图态可表示为

$$\left|G_l\right\rangle=\otimes_i S_i^{s_i}X_i^{x_i}Z_i^{z_i}\left|G\right\rangle \tag{7}$$

其中，广义泡利算符由式(8)给出。

$$\begin{aligned}Z\left|j\right\rangle&=\omega^j\left|j\right\rangle\\X\left|j\right\rangle&=\left|j+1\right\rangle\\S\left|j\right\rangle&=\omega^{j(j-1)/2}\left|j\right\rangle\end{aligned} \tag{8}$$

其中，$\omega=e^{\frac{2\pi i}{d}}$。

标签图态的稳定子模式表示如式(9)所示。

$$K_i=\left(XZ^{s_i}\right)Z^{A_i} \tag{9}$$

$\left|G_l\right\rangle$ 满足式(10)。

$$K_i\left|G_l\right\rangle=\omega^{-z_i}\left|G_l\right\rangle,i\in V \tag{10}$$

稳定子可以实现标签转移。但是转移标签的过程并不意味着物理上的操作或者改变图态本身，这个过程类似标签图态的重新标记，标签的变化满足定理 1[18]。

定理 1　假设参与者 i 和 j 是邻居。当用 $K_j^{-A_{ij}^{-1}z_i}$ 测量标签图态 $\left|G_l\right\rangle$ 时，$\left|G_l\right\rangle$ 转变成了标签图 $\left|G_{l'}\right\rangle$，其中，顶点 i 的标签重新标记为 $z_i'=0$，顶点 j 的标签重新标记为 $(z_j',x_j')=(z_j,-A_{ij}^{-1}z_i)$，$j$ 的每个邻居点 k 的标签重新标记为 $z_k'=z_k-A_{ij}^{-1}A_{jk}z_i$。

为了保证秘密恢复的安全性，引入了 group-recovery(GR)的概念[19]，为后续方案提供了理论基础。

定理 2　（n+1）GHZM 图态为 $\left|g_{(n+1)\mathrm{GHZM}}\right\rangle$，其中每个顶点满足

$$\left|g_{(n+1)\mathrm{GHZM}}\right\rangle=\left[V=v_1,v_j;E=v_1,v_{j\neq1}\right] \tag{11}$$

其中，每个顶点的度为

$$N(u)=\begin{cases}n, & u=v_i\\1, & u=v_j,j\in(2,n+1)\end{cases} \tag{12}$$

其中，v_1 可以被视为可信中心，v_j 代表参与者。顶点 v、稳定子算符 K_j 和子秘密 z_j 满足式(13)。

$$v_1+v_j\xrightarrow{K_j}z_j,j\in(2,n+1) \tag{13}$$

即子秘密 z_j 可以通过可信中心和成员 j 合作进行联合测量获得，这就是组恢复协议。如图 1 所示，可信中心和成员 i 可以看成一个组。

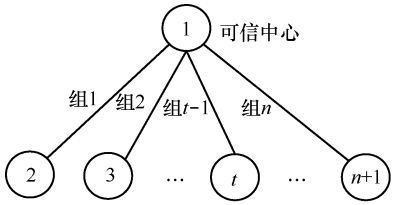

图 1 恢复秘密的组分布

当且仅当所有的子秘密都被可信中心知道时，秘密才可以通过 n 群组的相互合作恢复。这种情况称为全组恢复（FGR），记为 n-GR。

2.3 CRT 编码理论

中国剩余定理是由我国古代的著名数学家孙子提出的数论中的一个重要定理，又被称作孙子定理，用于求解线性同余方程组。其在经典信息通信、现代数学、现代密码学中有着巨大的作用。中国剩余定理的定义如定理 3 所示[20]。

定理 3 若 $n\geqslant 2$，$(m_1,\cdots,m_n)\geqslant 2$，且$(z_1,\cdots,z_n)\in Z$，且 $\gcd(m_1,m_n)=1$ 对任意 $1\leqslant i\leqslant n$，$1\leqslant j\leqslant n$ 都成立(m_j 与 m_i 互素)，那么下列方程组

$$\begin{cases} S=z_1 \bmod m_1 \\ \quad\vdots \\ S=z_n \bmod m_n \end{cases} \tag{14}$$

在整数空间 $Z_M=\{0,1,\cdots,M-1\}$ ($M=m_1\times m_2\times\cdots\times m_n$) 有解，解的形式为

$$S=\sum_{i-1}^{n} T_i M_i z_i \bmod M \tag{15}$$

其中，$M_i=\dfrac{M}{m_i}$，$T_i\times M_i\, M \bmod m_i=1$，且 $S\leqslant M$。

依据中国剩余定理的定义推知

$$\begin{cases} z_1=S \bmod m_1 \\ \quad\vdots \\ z_n=S \bmod m_n \end{cases} \tag{16}$$

分发者可以通过中国剩余定理将初始秘密拆分成 n 份（$z_1,\cdots,z_n$），然后分别分发给 n 个参与者。当所有合法参与者共同合作时，才能将初始秘密完整地恢复出来。鉴于该算法的计算便捷，可以提高计算速度，因此，很多方案都采用该算法，如数字指纹识别、群签名或者反追踪。实用性和普遍性是中国剩余定理的 2 个非常重要的特征。

3 方案描述

方案的主题思想是要共享经典秘密序列$\{S_r\}$ ($S_r\in F_d$)。对于每个秘密 S_r，首先，分发者通过中国剩余定理将秘密 S_r 拆分，$Z=z_i$ ($1\leqslant i\leqslant n+1$)表示子秘密集合，$n$+1 表示参与人数。分组的规则是：参与者 1 和 j($2\leqslant j\leqslant n+1$)为一组，进而所有的参与者可以被分成 n 组。其中，参与者 1 是一个可信中心，其他人为普通参与者，并且可以作为 1 的协助者。考虑到中国剩余定理算法和量子图态应用的空间维度，秘密的值受空间维度的限制，进行了下面的定义

$$d_j>\max m_i, d=\min d_j, 0<i<n+1 \tag{17}$$

其中，$d(d_j)$表示素数。为了便于分析，这里首先介绍基于 3 人的秘密共享方案，秘密为 S,方案流程如图 2 所示，鉴于其恢复子秘密的方式符合组恢复协议，所以又称其为 2-GR QSS。

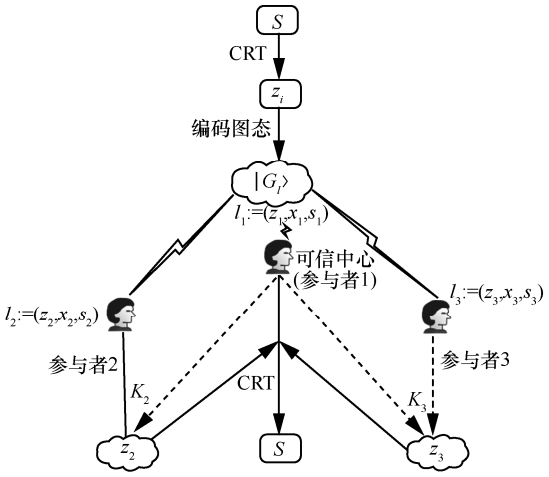

图 2 量子秘密共享方案流程

基于 3 人的秘密共享方案中参与者由分发者、可信中心 1、参与者 2 和参与者 3 组成，参与者 2 和 3 可以协助可信中心恢复子秘密集。

假设分发者想要在 3 个人之间共享一个秘密 S($S\in F_d$)，为了方便叙述和分析，令 S=5，模数 m_1=2, m_2=3，然后推知维度 d=5。具体的步骤如下。

1) 秘密的划分和标记。分发者拥有初始秘密 S=5，然后其通过 CRT 将 S 划分成子秘密 z_i，即

$$\begin{aligned} z_2&=5 \bmod 2=1 \\ z_3&=5 \bmod 3=2 \end{aligned} \tag{18}$$

则可以得到每个参与者的标签 l_1 =(0,0,0), l_2 =(1,0,0), l_3=(2,0,0)。

2) 量子图态的编码。分发者制备初始态

$$\left|G\right\rangle=\prod_{e_{i,j}\in E}C_{ij}^{A_{ij}}\left|\bar{0}\right\rangle^{\otimes n},i,j\in1,2,3;n=3 \tag{19}$$

这里 A_{ij} 是一个邻接矩阵。通过量子信道传输将初始图态的粒子 2 和 3 分发送给参与者 2 和参与者 3。传输过程的安全性由量子态的测不准原理和不可克隆性来保证的。然后，分发者将秘密编码到图态并采取与经典秘密相对应的酉操作将子秘密分发给参与者，得到的编码图态为

$$\left|G_l\right\rangle=\otimes_i Z_i^{z_i}\left|G\right\rangle,i=1,2,3 \tag{20}$$

基于 3 人的秘密共享方案中对应的稳定子为

$$\begin{aligned}K_1&=X_2Z_1Z_3\\K_2&=X_2Z_1\\K_3&=X_2Z_1\end{aligned} \tag{21}$$

最后将编码图态粒子 1 通过量子信道发送给可信中心。将发送给参与者 2 和参与者 3 的子秘密对应的模数通过经典信道发送给可信中心。

3) 量子图态测量和秘密的恢复。依据量子图态理论，子秘密的恢复可以通过联合测量得到。基于 3 人的秘密共享方案中，可信中心和 2 通过稳定子 K_2 测量量子态可以得到输出结果 ω^{-1}；可信中心和 3 通过稳定子 K_3 联合测量量子态可以得到结果 ω^{-2}。这样可信中心可以得到 2 个子秘密信息 $z_2=1$ 和 $z_3=2$，然后根据式(15)或 CRT 的解码规则如表 1 所示得到初始秘密 S。

表 1　　CRT 的解码规则

S	$z_2(m_1=2)$	$z_3(m_2=3)$
1	1	1
2	0	2
3	1	0
4	0	1
5	1	2

对于多人秘密共享的方案，其步骤跟上述基于 3 人的秘密共享方案类似。只是用到的量子图态计算式为

$$\left|G_l\right\rangle=\otimes_i Z_i^{z_i}\left|G\right\rangle,1\leqslant i\leqslant n+1 \tag{21}$$

相对应的稳定子为

$$\begin{aligned}K_1&=X_1\prod_{i=1}Z_i\\K_i&=X_iZ_i,i\neq1\end{aligned} \tag{22}$$

当恢复子秘密时，可信中心 1 和 $i(2\leqslant i\leqslant n+1)$ 通过稳定子 K_i 进行联合测量，得到输出结果 ω^{-z_i}，多人共享方案的子秘密分布如图 3 所示。

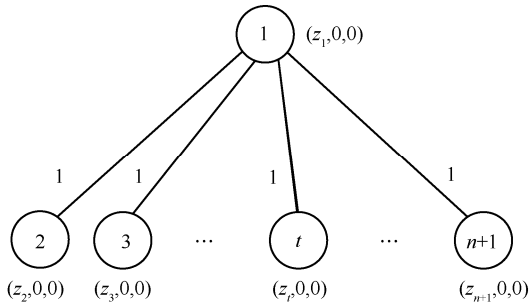

图 3　参与者关系和子秘密分布

4　安全性分析

量子图态、中国剩余定理、稳定子的信息转移机制以及组恢复协议，保证了所提方案的安全性。此外，参与者 1 是可信中心，是唯一有权利恢复秘密的人。这种机制可以有效地阻止攻击者和非诚信者非法获取信息。下面，详细分析该方案的安全性和性能。

4.1　截获–重发攻击

方案中产生的量子图态是一种特殊多粒子纠缠态，根据多粒子纠缠态的安全传输，任何方式的测量都会破坏量子图态的纠缠性，所以任何需要用到测量的监听都会被合法的参与者检测出来。假设攻击者 eve 采取截取重发攻击的方式，如果他想要获得秘密，必须对粒子进行测量，一旦 eve 粒子进行测量，就会破坏粒子的纠缠性，分发者和分发参与者之间的图态关系就会发生变化，eve 的攻击就会被检测出来。

4.2　纠缠攻击

假设攻击者 eve 纠缠附属粒子到 $\left|G_l\right\rangle$ 上，以便在后面通过观察辅助粒子的状态来获得秘密信息。$\left|G_l\right\rangle$ 纠缠附属粒子后得到 $\left|G_{l+\mathrm{e}}\right\rangle=\otimes_i Z_i^{z_i}\left|G_{+\mathrm{e}}\right\rangle$，$1\leqslant i\leqslant n+1$。当可信中心和合法参与者通过 K_i 进行联合测量时得到

$$K_i\left|G_{l+\mathrm{e}}\right\rangle = X_i Z_i \underset{i}{\otimes} Z_i^{z_i}\left|G_{+\mathrm{e}}\right\rangle, 1 \leqslant i \leqslant n+1 \quad (23)$$

由上可知，附属粒子的状态并没有改变，所以 eve 不能通过观察辅助粒子的状态获得秘密信息。

4.3　不诚实的参与者攻击

这里考虑不诚实的参与者想通过测量得到一些信息的情况。量子图态的应用便于图形化表示，在本方案中，稳定子的形式使得信息 z_k 与合法参与者 k+1 相互独立。根据图态的转移特性，单个不诚实的参与者不能通过测量获得任何信息。如图 4 所示，当不诚实的参与者进行测量时，子秘密标签会转移。在标签图态中，V' 通过 LOCC 可以获得子秘密 z_k，其中，V' 是 v_k 和它所有邻居的集合。值得注意的是，这种操作不改变态的本身，只是转移了标签。

以 3 个参与者的系统为例，设置初始化图态的标签 l_1 =(0,0,0)、l_2 =(1,0,0)、l_3 =(2,0,0)，权重都为 1。具体的分析如下。可信中心 1 不能获得秘密，因为它与秘密相互独立。参与者 2 不能获得秘密，因为通过稳定子操作 K_1^{-1} 秘密信息可能会转移到可信中心（参与者 1）或者参与者 3。那么图态被重新标记为 l_1 =(0,–1,0)、l_2 =(0,0,0)、l_3 =(1,0,0)。同样地，由于图态的转移特性，成员 3 也不能获得秘密。

$$\begin{aligned} z_2' &= 0 \\ x_1' &= -z_2 \\ z_i' &= z_i - z_2 (i \in (3,n)) \end{aligned} \quad (24)$$

多个不诚实的参与者也不能获得秘密。假设 n 个成员分享秘密 S，通过 CRT，S 被分割成子秘密 $z_i\left(i \in (2,n)\right)$。其他的标签值设为 0，权重为 1。如图 5 所示，子秘密 z_2 可以从成员 2 转移到成员 1 处。

由此可知，如果除了可信中心 1 的 n–1 个成员合作，他们只能获得 $z_i - z_2$，由于他们不知道 z_2，所以他不能得到秘密 $z_i\left(i \in (2,n)\right)$。那么初始秘密 S 就不能被恢复。但是他们知道模数 m，所以解密的概率为

$$P = \prod_{i=1}^{n} \frac{1}{m_i} = \frac{1}{M} \quad (25)$$

其中，n 是所有的成员，M= $m_2 \times \cdots \times m_n$ 熵为

$$H\left(S\middle|z_1\right) = \mathrm{lb}\frac{1}{P} = \mathrm{lb}\frac{1}{M} = H\left(S\right) \quad (26)$$

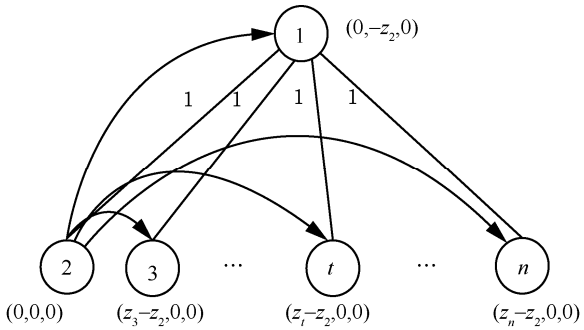

图 5　标记 z_2 的转移状态

4.4　破译分析

假设存在一个长为 R 的秘密序列$\{S_{\mathrm{r}}\}, r \in (1,R)$，攻击者 eve 通过一定的方法从 S_{r} 分割的子秘密序列中获得了 k 个子秘密，那么秘密 S_{r} 的破译概率为

$$P = \frac{\prod_{i=2}^{k} m_{\mathrm{eve}i}}{M_{\mathrm{r}}} \quad (27)$$

则秘密序列的破译概率为

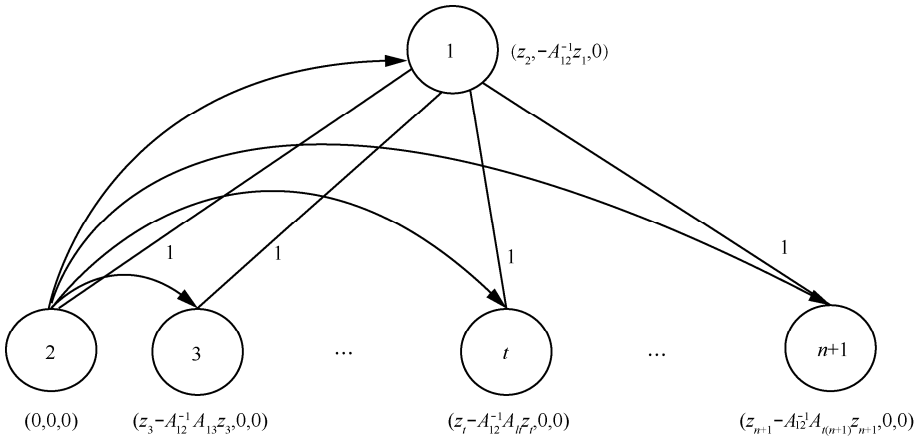

图 4　参与者 2 执行 $K_1^{-A_{12}^{-1}z_2}$ 测量，标记 z_2 的转移状态

$$P=\prod_{r=1}^{R}\frac{\prod_{i=2}^{k}m_{\mathrm{eve}i}}{M_{\mathrm{r}}} \tag{28}$$

其中，$m_{\mathrm{eve}i}$ 是 eve 获取的子秘密 $m_{\mathrm{eve}i}$ 相对应的模数，M_{r} 是秘密 S_{r} 对应的 M 值。

为了便于仿真和直观的分析，m_i 取值为素数，并且攻击者仅仅从一个子秘密集中获取了一个 qudit($z_{\mathrm{eve}i}$ =1, $m_{\mathrm{eve}i}$ =2)，仿真结果如图 6 所示。

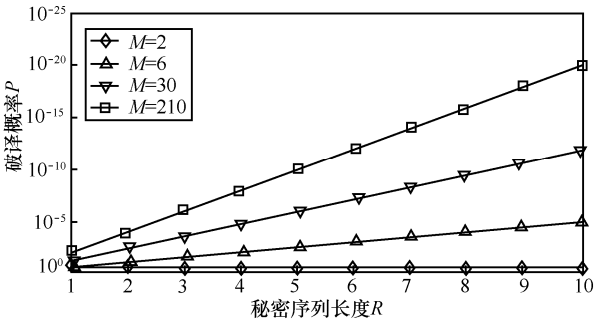

图 6　破译概率的仿真结果

从图 6 可以看到在 M 变换的情况下，R 与 P 在呈负相关，这意味着序列长度越长，破译概率就会越小。从另一方面来看，在 R 变换的情况下，随着 m 的增加，破译概率会随之降低。另外，菱形线表示当 R=1，M=2 时，破译概率一直为 1。因此，适当地增加秘密长度或模数会使得网络通信更安全。

4.5　性能分析

量子比特传输实现的经典比特传输的比特数越多，方案的性能越好。比特比值用 Q 表示，即

$$Q=\frac{q_{\mathrm{b}}}{q_{\mathrm{t}}} \tag{29}$$

其中，q_{t} 为传输的量子比特数，q_{b} 为传输 q_{t} 量子比特实现经典比特传输的比特数。Q 越大，效率越高。提出的方案 Q 值和选择的模数 m 有关，对于 2-GR QSS，当模数 m_1=2, m_2 =3 时，根据 CRT 定理，秘密 S 最大为 6，即 q_{t}=3 时 q_{b}=2，$Q=\frac{2}{3}$。模数 m 越大，秘密 S 的最大值越大，传输 3 量子比特可实现经典秘密的传输的比特数越大，即 q_{b} 越大。所以提出方案的比特比值 $Q\geqslant\frac{2}{3}$。文献[21]中，Q 值均为 $\frac{1}{2}$，所以提出的方案量子比特传输实现的经典比特传输的比特数比已有的类似方案高。

5　结束语

本文依据中国剩余定理和量子图态的结构特征，介绍了一种新型的量子秘密共享方案。方案中的编解码依赖于量子图态独有的纠缠特性及中国剩余定理。图态的结构特性使得方案得以更加清晰且具有图形表述。在方案设计中，分发者是通过中国剩余定理获取子秘密，然后编码信息到量子图态上，进而通过合适的酉操作分发粒子给合法的参与者。引用了组恢复协议，目的是更加清楚明了的表述子秘密的恢复流程及方式。通过对该方案合理的理论分析，可以看出方案具有良好的安全性及可行性。其中，秘密共享方案的安全性是由中国剩余定理、稳定子的信息转移机制以及新型的秘密恢复策略来保障的。中国剩余定理的便捷性和高效性及图态的转移特性使该方案可应用于量子网络密码共享及量子签名、认证。

参考文献：

[1] SHAMIR A. How to share a secret[J]. Communication of ACM, 1979, 22(11):621-613.

[2] HILLERY M, BU˙ZEK V, BERTHIAUME A. Quantum secret sharing[J]. Physical Review A, 1999, 59(3):1829-1834.

[3] SHI R H, SU Q, GUO Y, et al. Quantum secret sharing based on Chinese remainder theorem[J]. Communications in Theoretical Physics, 2011, 55 (4):573-578.

[4] GUO Y, ZHAO Y. High efficient quantum secret sharing based o-n the Chinese remainder theorem via the orbital angular momentum entanglement analysis[J]. Quantum Information Processing, 2013, 12 (2):1125-1139.

[5] GUO Y, HUANG D Z, ZENG G H. Multiparty quantum secret s-haring of quantum states using entanglement states[J]. Chinese Physics Letters, 2008, 25 (1):16-19.

[6] MARKHAM D, SANDERS B C. Graph states for quantum secret sharing[J]. Physical Review A, 2008, 78 (4): 042309.

[7] KEET A, FORTESCUE B, MARKHAM D, et al. Quantum secret sharing with qudit graph states[J]. Physical Review A, 2010, 82 (6):062315.

[8] RAHAMAN R, PARKER M G. Quantum scheme for secret sharing based on local distinguish ability[J]. Physical Review A, 2015, 91 (2): 022330.

[9] TAVAKOLI A, HERBAUTS I, ZUKOWSKI M, et al. Secret sharing with a single dlevelquantum system[J]. Physical Review A, 2015, 92 (3): 030302.

[10] LIANG J W, ZHOU J, SHI J J, et al. Improving continuous variable quantum key distribution using the heralded noiseless linear amplifier with source in the middle[J]. International Journal of Theoretical Physics, 2015, 55 (2):1156-1166.

[11] WANG C, HUANG P, HUANG D, et al. Practical security of continuous variable quantum key distribution with finite sampling bandwidth

effects[J]. Physical Review A, 2016, 93 (2): 022315.
[12] WU Y D, ZHOU J, GONG X B, et al. Continuous variable measurement device independent multipartite quantum communication[J]. Physical Review A, 2016, 93 (2): 022325.
[13] AMIRI R, WALLDEN P, KENT A, et al. Secure quantum signatures using insecure quantum channels[J]. Physical Review A, 2016, 3 (3): 032325.
[14] QIN H W, DAI Y W. An efficient (*t*, *n*) threshold quantum secret sharing without entanglement Quantum error correcting codes using qudit graph states[J]. Modern Physics Letters B, 2016, 30 (12):1650138.
[15] QIN H, ZHU X, DAI Y. A proactive quantum secret sharing scheme based on GHZ state[J]. Modern Physics Letters B, 2015, 29 (27): 1550165.
[16] HE X L, YANG C P. Deterministic transfer of multi-qubit GHZ entangled states and quantum secret sharing between different cavityes[J]. Quantum Information Processing, 2015, 14 (12): 4461-4474.
[17] QIN H, DAI Y. Verifiable (*t*, *n*) threshold quantum secret sharing using d-dimensional Bellstate[J]. Information Processing Letters, 2016, 116 (5): 351-355.
[18] KEET A, FORTESCUE B, MARKHAM D, et al. Quantum sec-ret sharing with qudit graph states[J]. Physical Review A, 2010, 82(6): 4229-4231.
[19] 梁建武, 程资, 石金晶, 等. 基于量子图态的量子秘密共享[J]. 物理学报, 2016, 65(16):35-41.
LIANG J W, CHEGN Z, SHI J J, et al. Quantum secret sharing based on quantum graph States[J]. Acta Physica Sinica, 2016, 65(16):35-41.
[20] KONDRACKI A. The Chinese remainder theorem[J]. Formalized Mathematics, 1997, 6(4): 573-577.
[21] 佟鑫, 温巧燕, 朱甫臣. 基于 GHZ 态纠缠交换的量子秘密共享[J]. 北京邮电大学学报, 2007, 30(1):44-48.
TONG X, WEN Q Y, ZHU F C. Quantum secret sharing based on GHZ state entanglement swapping[J]. Journal of Beijing University of Posts and Telecommunications, 2007, 30(1):44-48.

[作者简介]

梁建武（1964−），男，湖南长沙人，中南大学副教授，主要研究方向为量子通信和无线通信。

刘晓书（1994−），女，湖南衡阳人，中南大学硕士生，主要研究方向为量子通信和无线通信。

程资（1990−），女，河北晋州人，中南大学硕士生，主要研究方向为量子通信和无线通信。