重构者两粒子的量子秘密共享方案

夏红红,汪学明,杨万鑫
(贵州大学 计算机科学与技术学院,贵州 贵阳 550025)

摘 要:量子密码体制使它在多方秘密共享方面有很好的运用和发展,关于量子秘密共享的文章大都只考虑了参与者只分配一个粒子的情况。文中充分考虑了秘密重构者持有两个粒子的情况,构建了一个新的量子秘密共享方案,该方案是完全通过隐形传态来实现秘密共享的。在以往的方案中,重构者往往需要完全借助其他参与者的测量结果恢复秘密,自己不参与其他参与者的测量过程,存在一定的风险性。此方案不需要完全依靠其他参与者幺正变换即可恢复秘密,重构者拥有两个粒子,其中一个用于Bell测量,另一个参与幺正变换,在其他代理相互合作情况的下,秘密量子态也不会轻易转移到其他粒子上去,减轻了一定程度上的欺骗。在整个过程中粒子无太大损耗,最后对该方案进行了安全性分析,结果表明该方案是安全可靠的。

关键词:多方秘密共享;量子纠缠;幺正变换;量子隐形传态;Bell测量
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2020)06-0099-05
doi:10.3969/j.issn.1673-629X.2020.06.019

Reconstructing Quantum Secret Sharing Scheme of Two Particles

XIA Hong-hong, WANG Xue-ming, YANG Wan-xin
(School of Computer Science and Technology, Guizhou University, Guiyang 550025, China)

Abstract: Quantum cryptography makes it well used and developed in the aspect of multi-party secret sharing. Most articles about quantum secret sharing only consider the case that participants only allocate one particle. We give full consideration to the fact that the secret reconstructors hold two particles and construct a new quantum secret sharing scheme. In the previous schemes, the reconstructors often need to recover the secrets completely with the measurement results of other participants, and they do not participate in the measurement process of other participants, which has some risks. The proposed scheme does not need to depend entirely on other participants unitary transformation can restore the secret, refactoring has two particles, one is used for Bell, another to participate in the unitary transformation. Under the situation of other agents cooperation, secret quantum state will not be easily transferred to other particles, reducing the deception to some extent. In the whole process, there is no large loss of particles. Finally, the safety analysis shows that the proposed scheme is safe and reliable.

Key words: multi-party secret sharing; quantum entanglement; unitary operatuion; quantum teleportation; Bell-state measurement

0 引 言

随着科技的发展,在最初的经典密码学基础上,产生了量子密码,由于量子密码的安全性是由量子力学的基本原理做铺垫,成功解决了NP和RSA等问题。秘密共享则是量子密码学的一个方向。量子秘密共享的思想是:假设秘密发送者需要传递秘密信息给其他参与者,而仅仅一个或者部分参与者是恢复不了的,需要所有的参与者一起合作,才可以恢复。任何非法参与者与窃听者都不能重构出原始量子态,从一定程度上保证了秘密的安全性和完整性。

1979年Shamir和Blakley提出了秘密共享的概念,他们的方案分别基于拉格朗日内插多项式和摄影几何理论,由于基于插值多项式的方案实现简单代价小而得到了大量研究[1-2]。1994年,J. He和E. Dawson提出多方秘密共享的概念[3];秦素娟提出了一种基于Bell态纠缠交换的协议,参与方的量子信道构成一个环,通过在环上添加或删除节点可以构造任意多方协议,并且对其他参与方没有任何影响[4];2010年,符力平提出了基于重复使用W态的量子秘密共享来发送经典信息的方案,降低了信息被窃取或联手欺

收稿日期:2019-07-26 **修回日期**:2019-11-27
基金项目:国家自然科学基金([2011]61163049);贵州省自然科学基金资助项目(黔科合J字[2014]7641)
作者简介:夏红红(1995-),女,硕士研究生,研究方向为协议分析、密码学与信息安全;通讯作者:汪学明(1965-),男,教授,博士,CCF会员(E200036215M),研究方向为无线与移动通信、协议分析与模型检测、密码学与信息安全。

骗的可能性[5]。2013 年,钱晓婕将无纠缠动态的量子秘密共享的思想具体应用到数字签名中去,免去了量子的制备,同时达到了与量子纠缠态相当的无条件安全的效果[6]。2015 年,吴君钦等人提出了使用 GHZ 的三粒子纠缠态作为量子信道来实现三个未知量子纠缠态的秘密共享方案[7]。2016 年,张建中等人提出了两种基于四粒子纠缠态的量子秘密共享方案,通过分析表明,提出的方案是高效且安全可靠的[8]。2018 年,高明提出了量子多方秘密共享方案,使得所有的对称纠缠态都可以通过隐形传态来完成秘密共享协议[9]。2019 年,张国帅适应任意类型 EPR 通道的单量子比特隐形传送通用线路,并推广到任意 N 比特量子隐形传送通用线路。

此后,经过多年的研究,量子秘密共享方案相继被提出[10-16]。这些方案主要是从秘密参与者手持 1 个粒子出发的。实际上,秘密重构者在某些情况下也会持有两个粒子。其中一个粒子参与 Bell 测量,而另一个粒子则根据最后的测量结果进行相应的幺正变换即可恢复秘密,不需要依靠其他参与者幺正变换即可恢复出秘密。在其他代理相互合作的情况下,秘密量子态也不会转移到其他的粒子上去,从一定程度上减小了欺骗的概率。秘密重构者的粒子除了进行幺正变换,还参与了 Bell 测量,保证了一定的安全性。

1 预备知识

1.1 幺正变换与量子逻辑门

幺正变换可分为以下操作:

(1)恒等操作:I,它保持量子比特状态不变,相对应的矩阵为:

$$\boldsymbol{I}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\quad \boldsymbol{I}=|0\rangle\langle 0|+|1\rangle\langle 1|$$

(2)非门操作 σ,进行非操作,对应矩阵为:

$$\boldsymbol{\sigma}_x=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

(3)Z 门 σ,对量子比特进行相位转换,相对应的矩阵为:

$$\boldsymbol{\sigma}_z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\quad \boldsymbol{\sigma}_z=|0\rangle\langle 0|-|1\rangle\langle 1|$$

(4)Y 门 σ_y,对量子比特做比特翻转,且相位调整 π/2,相对应的矩阵为:

$$i\boldsymbol{\sigma}_y=i\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}\quad i\boldsymbol{\sigma}_y=|0\rangle\langle 1|-|1\rangle\langle 0|$$

1.2 Bell 态与 Bell 测量

具体的 Bell 态有 4 个基底,可表示为:

$$|\varphi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$$

$$|\varphi^-\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)$$

$$|\psi^+\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)$$

$$|\psi^-\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)$$

2 四、五参与者量子秘密共享方案

2.1 四参与者量子秘密共享方案

假设由 Alex、Bess、Candy、Charlie 来进行量子秘密的共享,其中 Alex 是发送秘密消息者,其余三人是代理人。现在 Alex 准备发送给其中一人一个未知的单量子态:

$$|\varphi\rangle_n=\alpha|0\rangle_n+\beta|1\rangle_n \tag{1}$$

其中,α 和 β 满足 $|\alpha|^2+|\beta|^2=1$,且 Bess、Candy、Del 都不知道 α 和 β 的值。由于设定了其中的秘密重构者拥有两粒子,所以 Alex、Bess、Candy、Del 共享的是五粒子态:

$$|\psi\rangle_{12345}=\frac{1}{2}(|00000\rangle+|00110\rangle+|11001\rangle+|11111\rangle)_{12345} \tag{2}$$

量子态消息与 1 到 5 粒子组成系统状态直积可表示为:

$$|\tau\rangle_{n12345}=\frac{1}{2}(\alpha|0\rangle_n+\beta|1\rangle_n)\otimes(|00000\rangle+|00110\rangle+|11001\rangle+|11111\rangle)_{12345} \tag{3}$$

如果要达到重构出秘密的目的,则需利用两次 Bell 测量最终剩余单量子态。因为每次 Bell 测量会“消去”两个粒子。两次 Bell 测量消去四个粒子。在秘密重构者的两个粒子中,一个粒子参与 Bell 测量,剩余一个参与者对自己所持有的粒子进行 X 基测量,将最后的测量结果告知秘密重构者,重构者的另一个粒子进行幺正变换即可。首先把 Alex 的粒子 1 与 n 粒子进行 Bell 测量,得到:

$$n_1<\varphi^+|\tau>_{n12345}=\frac{1}{2\sqrt{2}}(\alpha|0000\rangle+\alpha|0110\rangle+\beta|1001\rangle+\beta|1111\rangle)_{2345} \tag{4}$$

$$n_1<\varphi^-|\tau>_{n12345}=\frac{1}{2\sqrt{2}}(\alpha|0000\rangle+\alpha|0110\rangle-\beta|1001\rangle-\beta|1111\rangle)_{2345} \tag{5}$$

$$n_1<\psi^+|\tau>_{n12345}=\frac{1}{2\sqrt{2}}(\alpha|1001\rangle+\alpha|1111\rangle+\beta|0000\rangle+\beta|0110\rangle)_{2345} \tag{6}$$

$$n_1 < \psi^- | \tau >_{n12345} = \frac{1}{2\sqrt{2}}(\alpha | 1001\rangle + \alpha | 1111\rangle - \beta | 0000\rangle - \beta | 0110\rangle)_{2345} \quad (7)$$

2.1.1　Bess 为秘密重构者

Bess 作为秘密重构者时,Bess 拥有两个粒子,粒子 2 和粒子 3。需保留 2 粒子,将自己的 3 粒子与 Charlie 的 5 粒子进行 Bell 测量,最后 Candy 对持有的粒子 4 进行 X 基测量即可。把结果告诉 Bess,Bess 利用手中的 2 粒子进行相应幺正变换重构出秘密,见表 1。

表 1　四参与者量子秘密共享 Bess 重构秘密结果汇总

Charlie 和 Bess 测量结果	Candy 的 X 基测量	Bess 的粒子状态	Bess 采取的幺正变换
$\|\varphi^+\rangle$	$\|+x\rangle$	$\alpha\|0\rangle+\beta\|1\rangle$	I
	$\|-x\rangle$	$\alpha\|0\rangle-\beta\|1\rangle$	σ_z
$\|\varphi^-\rangle$	$\|+x\rangle$	$\alpha\|0\rangle-\beta\|1\rangle$	σ_z
	$\|-x\rangle$	$\alpha\|0\rangle+\beta\|1\rangle$	I
$\|\psi^+\rangle$	$\|+x\rangle$	$\alpha\|1\rangle+\beta\|0\rangle$	σ_x
	$\|-x\rangle$	$\alpha\|1\rangle-\beta\|0\rangle$	$i\sigma_y$
$\|\psi^-\rangle$	$\|+x\rangle$	$\alpha\|1\rangle-\beta\|0\rangle$	$i\sigma_y$
	$\|-x\rangle$	$\alpha\|1\rangle+\beta\|0\rangle$	σ_x

$$\begin{aligned}|\gamma\rangle_{2345} = \frac{1}{4\sqrt{2}}\{&|\varphi^+\rangle_{35}[|+x\rangle_4(\alpha|0\rangle+\beta|1\rangle)_2 + |-x\rangle_4(\alpha|0\rangle-\beta|1\rangle)_2] + |\varphi^-\rangle_{35}[|+x\rangle_4|(\alpha|0\rangle-\beta|1\rangle)_2 + |-x\rangle_4(\alpha|0\rangle+\beta|1\rangle)_2] \\ &+|\psi^+\rangle_{35}[|+x\rangle_4|(\alpha|1\rangle+\beta|0\rangle)_2 + |-x\rangle_4(\alpha|1\rangle-\beta|0\rangle)_2] + |\psi^-\rangle_{34}[|+x\rangle_4(\alpha|1-\beta|0\rangle\rangle)_2 + |-x\rangle_4(\alpha|1\rangle+\beta|0\rangle)_2]\}\end{aligned} \quad (8)$$

2.1.2　Candy 作为秘密重构者

Candy 作为秘密重构者时,Candy 拥有两个粒子,粒子 2 和粒子 5。需保留 2 粒子,将自己持有的粒子 5 与 Charlie 的粒子 3 进行 Bell 测量,最后 Bess 对粒子 4 进行 X 基测量,将测量结果公布给 Candy,Candy 利用手中的 2 粒子进行相应幺正变换重构出秘密。当 Bess 作为秘密重构者时进行的是粒子 3 和粒子 5,现在 Candy 也是。因此,对于 2.1.2 情况的讨论,可参照 2.1.1。

2.1.3　Charlie 作为秘密重构者

Charlie 作为秘密重构者时,Charlie 拥有两个粒子,粒子 4 和粒子 5。需保留 5 粒子,将自己的 4 粒子与 Bess 的 2 粒子进行 Bell 测量,最后 Candy 对持有的粒子 3 进行用 X 基测量持有的粒子 3,把结果告诉 Charlie,Charlie 对持有的 5 粒子进行相应的幺正变换即可重构出原始消息,见表 2。

表 2　四参与者量子秘密共享 Del 重构秘密结果汇总

Bess 和 Charlie 测量结果	Candy 的 X 基选择	Charlie 的粒子状态	Charlie 采取的幺正变换
$\|\varphi^+\rangle$	$\|+x\rangle$	$\alpha\|0\rangle+\beta\|1\rangle$	I
	$\|-x\rangle$	$\alpha\|0\rangle-\beta\|1\rangle$	σ_z
$\|\varphi^-\rangle$	$\|+x\rangle$	$\alpha\|0\rangle-\beta\|1\rangle$	σ_z
	$\|-x\rangle$	$\alpha\|0\rangle+\beta\|1\rangle$	I
$\|\psi^+\rangle$	$\|+x\rangle$	$\beta\|1\rangle+\alpha\|0\rangle$	I
	$\|-x\rangle$	$\beta\|1\rangle-\alpha\|0\rangle$	$-\sigma_z$
$\|\psi^-\rangle$	$\|+x\rangle$	$\beta\|1\rangle-\alpha\|0\rangle$	$-\sigma_z$
	$\|-x\rangle$	$\beta\|1\rangle+\alpha\|0\rangle$	σ_x

$$\begin{aligned}|\gamma\rangle_{2345} = \frac{1}{4\sqrt{2}}\{&|\varphi^+\rangle_{24}|[|+x\rangle_3(\alpha|0\rangle+\beta|1\rangle)_5 + |-x\rangle_3(\alpha|0\rangle-\beta|1\rangle)_5] + |\varphi^-\rangle_{24}[|+x\rangle_3(\alpha|0\rangle-\beta|1\rangle)_5 + |-x\rangle_3(\beta|1\rangle+\alpha|0\rangle)_5] + |\psi^+\rangle_{24}[|+x\rangle_3(\alpha|0\rangle+\beta|1\rangle)_5 + |-x\rangle_2(\alpha|0\rangle-\beta|1\rangle)_5] + |\psi^-\rangle_{24}[|+x\rangle_3(\alpha|0\rangle-\beta|1\rangle)_5 + |-x\rangle_2(\beta|1\rangle+\alpha|0\rangle)_5]\}\end{aligned} \quad (9)$$

2.2　五参与者量子秘密共享方案

设 Alex 需要传递的未知单量子态为:

$$|\varphi\rangle_m = \alpha|0\rangle_m + \beta|1\rangle_m \quad (10)$$

由于设定了其中的秘密重构者拥有两粒子,所以 Alex、Bess、Candy、Del、Bob 共享一个六粒子态未知量子与 1 到 6 粒子组成系统状态直积为:

$$\begin{aligned}|\tau\rangle_{m123456} = \frac{1}{2}(\alpha|0\rangle_m+\beta|1\rangle_m)\otimes(&|000000\rangle + |001001\rangle + |001111\rangle + |000100\rangle + |110000\rangle + |110110\rangle + |111111\rangle + |111011\rangle)_{123456}\end{aligned} \quad (11)$$

2.2.1　Candy 为秘密重构者

而此五参与者方案由于是六粒子结构,实际上无需 X 单基测量,每次 Bell 测量会“消去”两个粒子,因此方案需要进行三次的 Bell 测量。Candy 拥有两个粒子,粒子 5 和 2,粒子 2 与其余粒子 3,4,6 进行 Bell 测量,最后剩余的单量子态经过相应的幺正变换就能得到 Alex 发送的未知态。

Candy 为秘密重构者时,设三次测量结果均为 $|\varphi^+\rangle$,则三次 Bell 测量过程为:

$$\begin{aligned}\langle\varphi^+|\tau\rangle = \frac{1}{4}[&\alpha(|00000\rangle+|01001\rangle+|01111\rangle+|00100\rangle)+\beta(|10000\rangle+|10110\rangle+|11111\rangle+|11011\rangle)]_{23456}\end{aligned} \quad (12)$$

$$\langle\varphi^+|\gamma\rangle_{23456} = \frac{1}{4\sqrt{2}}[(\alpha|000\rangle+\alpha|010\rangle+$$

$$\beta|111\rangle+\beta|101\rangle)_{345} \quad (13)$$

$$\langle\varphi^+|\zeta\rangle_{345}=\frac{1}{8}(\alpha|0\rangle+\beta|1\rangle)_5 \quad (14)$$

$$\langle\varphi^-|\zeta\rangle_{345}=\frac{1}{8}(\alpha|0\rangle-\beta|1\rangle)_5 \quad (15)$$

$$\langle\psi^+|\zeta\rangle_{345}=\frac{1}{8}(\alpha|0\rangle+\beta|1\rangle)_5 \quad (16)$$

$$\langle\psi^-|\zeta\rangle_{345}=\frac{1}{8}(\alpha|0\rangle-\beta|1\rangle)_5 \quad (17)$$

最后将测量结果告诉 Candy,Candy 进行相应的幺正变换重构出秘密,见表 3。

2.2.2 Del 为重构者

Del 拥有两个粒子,粒子 5 和 4,粒子 4 与其余粒子 2,3,6 进行 Bell 测量,Candy 进行 Bell 测量的粒子组合是(2,3,4,6),现在 Del 进行 Bell 测量的粒子组合是(4,2,3,6),Bell 测量具有无序性,所以他们测量的结果是一样的。对于其他重构者,重构者的两粒子需要有 2,3,4,6 的其中一个粒子即可,剩余的一个粒子进行相应的幺正变换即可恢复初始秘密。

表 3 五参与者量子秘密共享 Candy 重构秘密结果汇总

Alex 测量结果	Bess 和 Bob 幺正变换	粒子 23456 状态	Bess 和 Bob 测量结果	Del 和 Candy 幺正变换	粒子 345 状态	Del 和 Candy 测量结果	Candy 幺正变换
$\|\varphi^+\rangle$	$I\otimes I$	$\|\lambda\rangle_{23456}$	$\|\varphi^+\rangle$	$I\otimes I$	$\|\zeta\rangle_{345}$	$\|\varphi^+\rangle$	I
$\|\varphi^-\rangle$	$\sigma_z\otimes I$		$\|\varphi^-\rangle$	$\sigma_z\otimes I$		$\|\varphi^-\rangle$	σ_z
$\|\psi^+\rangle$	$\sigma_z\otimes\sigma_x$		$\|\psi^+\rangle$	$\sigma_z\otimes\sigma_x$		$\|\psi^+\rangle$	I
$\|\psi^-\rangle$	$i\sigma_y\otimes\sigma_z$		$\|\psi^-\rangle$	$i\sigma_y\otimes\sigma_z$		$\|\psi^-\rangle$	σ_z

2.3 方案总结

该方案秘密重构者持有两个粒子的情况,这样一来,其中一个粒子参与 Bell 测量,而另一个粒子则根据最后的测量结果进行相应的幺正变换即可恢复秘密。不需要依靠其他参与者幺正变换即可恢复秘密。也不用担心参与者数目的增多有所影响,已有文章解决了 n 个代理的方案。实际上,秘密重构者持有两个粒子,实际上就是参与者的情况。假设有 n 个参与者,在这种情况下就变成了 $n+1$ 个参与者的情况,唯一不同之处就是可以参与了 Bell 测量。而其他参与者进行幺正变换,那么秘密量子态就会转移到其他的量子上去,很容易受到欺骗。而秘密重构者自己幺正变换,秘密量子态还是在自己这里,不会转移。

整个过程是基于量子秘密共享、Bell 测量、幺正变换、单粒子测量等的幺正变换,使量子态在粒子间相互转换来重构秘密,具备正确性。

当重构者手持两个粒子时,一样可以扩展为 n 参与者方案,仍然是在对称纠缠信道的基础上,由于重构者多了一个粒子,所以变为 $n+1$,两者只是奇偶性的差别。如现方案的四参与者的步骤,实际上就是原方案的五参与者的步骤。

2.4 安全性分析

上述方案采取了量子隐形传输的方式,即秘密量子态在传输过程中不会被任何参与方所知,大大地提高了秘密重构的安全性。方案中无粒子损耗,利用率得到了提高,理论上成功率高达 100%。该方案从外部攻击和内部攻击两个方面进行分析。

2.4.1 外部攻击

对于外部攻击者 Eve 来说,由于对消息一无所知,常常采用的攻击方式是可复制或者截取重发。由量子不可克隆原理可知,不可能克隆一个未知的量子状态,所以复制无作用。由 Heisenberg 测不准原理可知,通信过程也会受到相应影响。

窃听者 Eve 在其中引入一个辅助粒子,无论 Eve 是否获取到秘密信息,都可以被发现。这个粒子会影响原来方案的步骤,由于多了一个粒子,会使得所需要的 Bell 态测量的次数异常,甚至秘密无法被重构。即使没有给量子系统引入任何错误,仍然不会影响原有的未知单粒子态和纠缠粒子复合系统的状态直积。

假设 Eve 纠缠的辅助粒子为 $|0\rangle_e$,若假设测量结果为 $\langle\varphi^+|\gamma\rangle_{23456}$,则剩余粒子所组合的态变为:

$(\alpha|000\rangle+\alpha|010\rangle+\beta|111\rangle+\beta|101\rangle)_{345}\otimes|0\rangle_e=(\alpha|0000\rangle+\alpha|0100\rangle+\beta|1110\rangle+\beta|1010\rangle)_{345e}$

对粒子 3 和粒子 4 作 Bell 测量,若测量结果为 $|\varphi^+\rangle_{34}$,则剩余粒子将会塌缩到 $(\alpha|0\rangle+\beta|1\rangle)_5|0\rangle_e$,可以看出 Eve 并未获取到任何有用的信息。

同样假设 Eve 纠缠的辅助粒子为 $|1\rangle_e$,则剩余粒子所组合的态变为:

$(\alpha|000\rangle+\alpha|010\rangle+\beta|111\rangle+\beta|101\rangle)_{345}\otimes|1\rangle_e=(\alpha|000\rangle+\alpha|010\rangle+\beta|111\rangle+\beta|101\rangle)_{345e}$

同样的对粒子 3 和粒子 4 作 Bell 测量,若测量结果为 $|\psi^-\rangle_{34}$,则剩余粒子将会塌缩到 $(\alpha|0\rangle-\beta|1\rangle)_5|0\rangle_e$,Eve 仍然未获取到任何有用的信息。

2.4.2 内部攻击

假设 Candy 是不诚实的一方,Candy 通过拦截 Alex 发送给 Bess 的信道粒子,将自己准备的纠缠粒子发送给 Bess。如果 Bess 为秘密重构者,最后将测量结

果一比对,存在窃听的行为。由于 Bess 无法知道 Candy 的信息,他每次猜中的概率为 50% 。次数越多,概率越小。过程中因增加误码率而被中断通信。相反 Candy 为秘密重构者,由于 Bess 的粒子发生了替换,他和其他参与者的粒子发生 Bell 测量,最后重构的秘密与秘密发送者的秘密一比对,也会存在窃听的行为。此外,对参与者和秘密发送方进行认证,并安全地检测通信之间的量子信道,也能识别出是假冒的。所以一方不诚实者获取不了未知粒子信息。

假设 Candy 和 Bess 合作,Candy 截获发送给 Del 的粒子。将自己准备好的粒子发送给 Del,如果 Del 为秘密重构者,重构的秘密会与发送者的不同,或者通过信道安全性的检测也可以发现有盗听者的存在。这些不诚实方想通过欺骗、合作的方式来获取秘密,然而不管怎样他们都不会知道合法秘密重构者手里的粒子的量子态,他们对所拥有的粒子信息的窃取也只能相应猜测,存在概率误差。实际上,方案的粒子数越多,内部窃听成功的概率越低。所以两个不诚实者获取不了未知粒子信息。

事实上,选取数目较多的参与者有助于提高方案的安全性,但是由于数目增多,方案的操作也会增多,效率会因此下降,它们之间有个均衡的关系,这里不做讨论。

事实上,只要秘密重构者坚守自己的操作,不让自己的粒子参与 Bell 测量,那么其他欺骗者们也就无法重构出秘密。

另外,该方案完全采用量子隐形传输的方式,秘密量子态不会直接被传输,在整个重构秘密和秘密共享过程中,任意一个参与者都无从获知秘密量子真正的量子态。而在某些非量子隐形传输方案中,在秘密分发者都允许的情况下,最后秘密重构者可以将自己所重构的秘密公布出来进行相应的对比验证即可。

3　结束语

考虑了秘密重构者持有两个粒子的情况,这样一来,其中一个粒子参与 Bell 测量,而另一个粒子则根据最后的测量结果进行相应的幺正变换即可恢复秘密。不需要依靠其他参与者幺正变换,只需要单纯的 Bell 测量、X 基测量即可恢复秘密,在其他代理相互合作的情况下,秘密量子态也不会转移到其他粒子上去,在一定程度上减小了欺骗的概率。接下来将研究秘密量子态从单到多的转换,最终在量子秘密共享中更好地运用。

参考文献:

[1] SHAMIR A. How to share a secret[J]. Communication of the ACM,1979,22(11):612-613.

[2] BLAILLEY G R. Safeguarding cryptographic keys[C]// Proceedings of the national computer conference. New York: AFIPS Press,1979:313-317.

[3] HE J,DAWSON E. Multistage secret sharing based on one-way function[J]. Electronics Letters,1994,30(19):1591-1592.

[4] 秦素娟,温巧燕,朱甫臣. 利用 Bell 态纠缠交换的环式量子秘密共享协议[J]. 北京邮电大学学报,2006,29(2):34-37.

[5] 刘丽丹,郑海兰,符力平. 基于重复使用纠缠 W 态的量子秘密分享[J]. 长沙理工大学学报:自然科学版,2010,7(2):72-75.

[6] 钱晓捷,王海江. 基于非纠缠量子秘密共享的盲签名方案[J]. 计算机应用与软件,2013,30(8):307-310.

[7] 吴君钦,林慧英. 一种新的未知三粒子量子态秘密共享方案[J]. 量子电子学报,2015,32(3):315-320.

[8] 张建中,张文昊. 两个基于四粒子纠缠态的量子秘密共享方案[J]. 计算机应用研究,2016,33(1):225-228.

[9] 高　明,汪学明. 基于量子理论的多方秘密共享方案的构建[J]. 计算机应用研究,2018,35(7):2135-2138.

[10] 麻　敏,李志慧,徐廷廷. 可验证的(n,n)门限量子秘密共享方案[J]. 计算机工程,2017,43(8):169-172.

[11] 李志慧,白海艳,白晨明. 基于量子电路的门限量子秘密共享方案[J]. 武汉大学学报:理学版,2019,65(2):200-206.

[12] 梁建武,刘晓书,程　资. 基于图态和中国剩余定理的量子秘密共享方案[J]. 通信学报,2018,39(10):72-78.

[13] 于　浩,贾　玮,眷继业,等. 基于诱骗态的 BB84 协议量子秘密共享方案[J]. 量子电子学报,2019,36(3):348-353.

[14] QIN H,TSO R. Efficient quantum secret sharing based on polarization and orbital angular momentum[J]. Journal of the Chinese Institute of Engineers,2019,42(2):1047-1052.

[15] 李培培,谭晓青. 基于可重用的不对称三粒子纠缠态的量子秘密共享[J]. 计算机应用研究,2016,33(4):1120-1123.

[16] 刘成基,李志慧,司萌萌,等. 基于局域区分的六粒子正交纠缠态的量子秘密共享方案[J]. 信息网络安全,2018(4):56-64.