基于五粒子不对称纠缠态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　针对量子在不对称纠缠态下的秘密共享问题，基于不对称的五粒子纠缠态，提出一个量子秘密共享方案，其中共享的秘密是未知双粒子态和未知双粒子态。发送者与参与者的粒子进行 bell 基测量消去，协助者经过单粒子测量，秘密重构者经过幺正操作或施加受控非门操作后，引入辅助粒子进行 CNOT 操作，重构原始秘密。计算发现不是所有的非对称纠缠态都可以通过隐形传态来实现秘密共享。分析外部攻击和内部攻击可知，该方案安全性高。

关键词　量子秘密共享　受控非门　CNOT 操作　幺正操作

中图分类号　TP309　　**文献标志码**　A　　DOI:10.3969/j.issn.1000-386x.2020.09.045

QUANTUM SECRET SHARING SCHEME BASED ON FIVE-PARTICLE ASYMMETRIC ENTANGLED STATES

Xia Honghong　Wang Xueming*　Yang Wanxin
(*College of Computer Science and Technology*, *Guizhou University*, *Guiyang 550025*, *Guizhou*, *China*)

Abstract　In order to solve the problem of quantum secret sharing in asymmetric entangled states, we propose a quantum secret sharing scheme based on asymmetric five-particle entangled states, in which the shared secret is the unknown single particle state and the unknown two particle state. The particles of the sender and participant were eliminated by bell basis measurement, the helper was tested by single particle measurement, and the secret reformer was tested by unitary operation or controlled non-gate operation. The auxiliary particles were introduced, and CNOT operation was performed to reconstruct the original secret. It is found that not all the asymmetric entangled states can achieve secret sharing through teleportation. The external attack and internal attack are analyzed, and it is concluded that the security of the scheme is high.

Keywords　Quantum secret sharing　Controlled not gate　CNOT operation　Unitary operations

0　引　言

秘密共享是一种密码技术，在过去的密码技术中，秘密过于集中，利用秘密共享技术可以分散风险，是信息安全和数据保密中的重要手段。其思想是：发送者想要发送秘密给其他人，必须所有人一起合作才能恢复秘密，至少有一方可信，这样可以很好地避免一方或双方不诚实导致秘密也无法重构的问题。

秘密共享是一种由多方参与共同管理秘密的方法[1]，最初的动机是解决密钥管理问题。高明等[6]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。邵婷婷等[7]提出一种基于 Bell 态的(3,3)量子秘密共享方案，进行局域操作对比三者的测量结果可以推算出发送者发送的信息，实现(3,3)量子秘密共享。

无论在理论还是实验方面，各种各样基于 bell 态或 GHZ 态等纠缠态的量子秘密共享方案陆续被提出[8-14]，大多数都是基于对称纠缠态。Bae 等[15]提出了一个三方量子隐形传态基于非对称态，该方案表明

收稿日期：2019-06-14。贵州省自然科学基金项目(黔科合 J 字[2014]7641)。**夏红红**，硕士生，主研领域：密码学，信息安全。**汪学明**，教授。**杨万鑫**，硕士生。

非对称量子信道的量子隐形传态可以比对称信道的量子隐形传态传递更多的量子信息,即非对称纠缠态作为量子信道可能更有用。本文提出了基于五粒子不对称纠缠态的量子秘密共享方案。一个重构秘密是未知单粒子态,另一个是未知双粒子态。当重构秘密是未知单粒子态时,发送者需要将所持有的粒子和别的粒子进行 bell 测量消去,协助者进行单粒子态测量,最后重构者进行相应的幺正变换就可以恢复原始秘密。当重构秘密是未知双粒子态时,发送者与参与者的粒子进行 bell 基测量消去,重构者进行受控非门操作后,引入辅助粒子进行 CNOT 操作,恢复未知双粒子态。本文通过计算发现,不是所有的非对称纠缠态都可以通过隐形传态来实现量子秘密共享。

1 未知单粒子态的量子秘密共享

存在三个合法的参与者 Alex、Bess、Candy 来参与量子秘密的共享,其中 Alex 发送秘密消息,Bess 和 Candy 是消息的代理者,需要他们一起合作才能重构 Alex 的消息。现在 Alex 所要传送的未知单粒子态为:

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

式中:α 和 β 满足 $|\alpha|^2 + |\beta|^2 = 1$,且 α 和 β 是复数。Alex、Bess、Candy 共享一个不对称的五粒子纠缠态:

$$|\varphi\rangle_{12345} = \frac{1}{2}(|00000\rangle + |01101\rangle + |10011\rangle + |11110\rangle)_{12345} \tag{2}$$

Alex 拥有量子信道中的 3 个粒子 1、3、4,Bess 和 Candy 拥有粒子 2 和 5,则秘密消息和共享的五粒子不对称纠缠态组成的复合系统为:

$$|\tau\rangle_{n12345} = \frac{1}{2}(\alpha|0\rangle_n + \beta|1\rangle_n) \otimes (|00000\rangle + |01101\rangle + |10011\rangle + |11110\rangle)_{12345} \tag{3}$$

要想重构出秘密,首先 Alex 对所持有的 3 个粒子以及未知粒子对 $(1,n)$ 和 $(3,4)$ 分别进行 bell 测量。

由于纠缠变换的作用,所持有的粒子态将会塌缩到以下情况之一:

$$_{n134}\langle\phi^+|\tau\rangle_{n12345} = \frac{1}{4}[(\alpha|00\rangle + |11\rangle)_{25} + (\beta|01\rangle + |10\rangle)_{25}] \tag{4}$$

$$_{n134}\langle\phi^-|\tau\rangle_{n12345} = \frac{1}{4}[(\alpha|00\rangle + |11\rangle)_{25} - (\beta|01\rangle + |10\rangle)_{25}] \tag{5}$$

$$_{n134}\langle\psi^+|\tau\rangle_{n12345} = \frac{1}{4}[(\alpha|01\rangle + |10\rangle)_{25} + (\beta|00\rangle + |11\rangle)]_{25} \tag{6}$$

$$_{n134}\langle\psi^-|\tau\rangle_{n12345} = \frac{1}{4}[(\alpha|01\rangle + |10\rangle)_{25} - (\beta|00\rangle + |11\rangle)]_{25} \tag{7}$$

不失一般性,假设 bell 测量结果为 $|\psi^+\rangle_{n134}$,根据测量结果,Bess 和 Candy 可知道各自的粒子处于何种状态,根据式(6),将 Bess 和 Candy 塌缩的态写为:

$$|\phi\rangle_{25} = \frac{1}{4}[(\alpha|01\rangle + |10\rangle)_{25} + (\beta|00\rangle + |11\rangle)_{25}] \tag{8}$$

$$|\phi\rangle_{25} = \frac{1}{4\sqrt{2}}[|0\rangle_2(\alpha|1 + \beta|0\rangle)_5 + |1\rangle_2(\alpha|0\rangle + \beta|1\rangle)_5] \tag{9}$$

1.1 Candy 为秘密重构者

想要恢复出未知量子态信息,需要 Bess 的协助,Bess 对自己所持有的粒子 2 作单粒子测量。如果 Bess 的测量结果是 $|0\rangle_2$,那么 Candy 将会塌缩到态 $\alpha|1\rangle_5 + \beta|0\rangle_5$,此时 Candy 对粒子 5 实施幺正操作 σ_x,将粒子 5 转化为态 $\alpha|0\rangle_5 + \beta|1\rangle_5$,这个态就是 Alex 发送的原始量子态;如果 Bess 的测量结果是 $|1\rangle_2$,那么 Candy 将会塌缩到态 $\alpha|0\rangle_5 + \beta|1\rangle_5$,无须任何幺正操作,这个态就是所需要的未知态。方案具体结果见表 1。其中:M 为 Alex 对粒子 1、m、3、4 的 bell 态测量结果;M_2 为 Bess 对粒子 2 进行的单粒子测量结果;$|\varphi\rangle_5$ 是 Bess 发布测量结果之后塌缩的态;U_b 为 Candy 要恢复 Alex 发送的未知单粒子态所需要做的幺正操作。

表 1 Candy 重构秘密结果汇总 1

M	M_2	$\|\varphi\rangle_5$	U_b
$\|\varphi^+\rangle$	$\|0\rangle_2$	$\alpha\|0\rangle_5 + \beta\|1\rangle_5$	I
	$\|1\rangle_2$	$\alpha\|1\rangle_5 + \beta\|0\rangle_5$	σ_x
$\|\varphi^-\rangle$	$\|0\rangle_2$	$\alpha\|0\rangle_5 - \beta\|1\rangle_5$	σ_z
	$\|1\rangle_2$	$\alpha\|1\rangle_2 - \beta\|0\rangle_5$	$-i\sigma_y$
$\|\psi^+\rangle$	$\|0\rangle_2$	$\alpha\|1\rangle_5 + \beta\|0\rangle_5$	σ_x
	$\|1\rangle_2$	$\alpha\|0\rangle_5 + \beta\|1\rangle_5$	I
$\|\psi^-\rangle$	$\|0\rangle_2$	$\alpha\|1\rangle_5 + \beta\|0\rangle_5$	$-i\sigma_y$
	$\|1\rangle_2$	$\alpha\|0\rangle_2 - \beta\|1\rangle_5$	σ_z

1.2 Bess 为秘密重构者

和上述方法相同,Candy 重构秘密具体结果见表 2。发送者 Alex 对自己所持有的 3 个粒子与 1 个未知单粒子进行 bell 测量,每次 bell 测量可消去 2 个粒子,4 个粒子进行 2 次 bell 测量即可消去,剩余 Bess 和 Candy 的 2 个粒子。一方想要恢复秘密,需要另一方

的协助,协助方对自己粒子做单粒子测量,重构方可以根据辅助方的测量结果,通过幺正变换恢复未知量子态信息。M_5 是 Candy 对粒子 5 进行的单粒子测量结果,$|\phi\rangle_2$ 是 Candy 发布测量结果之后塌缩的态,U_c 是 Bess 要恢复 Alex 发送的未知单粒子态所需要做的幺正操作。

表 2　Bess 重构秘密结果汇总 1

M	M_5	$\|\phi\rangle_2$	U_c
$\|\phi^+\rangle$	$\|0\rangle_5$	$\alpha\|1\rangle_2+\beta\|0\rangle_2$	σ_x
	$\|1\rangle_5$	$\alpha\|0\rangle_2+\beta\|1\rangle_2$	I
$\|\phi^-\rangle$	$\|0\rangle_5$	$\alpha\|1\rangle_2-\beta\|0\rangle_2$	$-i\sigma_y$
	$\|1\rangle_5$	$\alpha\|0\rangle_2-\beta\|1\rangle_2$	σ_z
$\|\psi^+\rangle$	$\|0\rangle_5$	$\alpha\|0\rangle_2+\beta\|1\rangle_2$	I
	$\|1\rangle_5$	$\alpha\|1\rangle_2+\beta\|0\rangle_2$	σ_x
$\|\psi^-\rangle$	$\|0\rangle_5$	$\alpha\|0\rangle_2-\beta\|1\rangle_2$	σ_z
	$\|1\rangle_5$	$\alpha\|1\rangle_2+\beta\|0\rangle_2$	$-i\sigma_y$

2　未知双粒子态的量子秘密共享

假设三个合法的参与者 Alex、Bess、Candy,Alex 发送了一个未知的双粒子态:

$$|\varphi\rangle_{12}=\alpha|00\rangle_{12}+\beta|11\rangle_{12} \tag{10}$$

式中:α 和 β 满足 $|\alpha|^2+|\beta|^2=1$,并且 α 和 β 都是复数。Alex 已知 α 和 β 的值,3 个合法参与者仍然利用一个不对称的五粒子纠缠态作为量子信道:

$$|\delta\rangle_{34567}=\frac{1}{2}(|00101\rangle+|01110\rangle+|10101\rangle+|11110\rangle)_{34567} \tag{11}$$

Alex 拥有量子信道中的 2 个粒子 3 和 4,粒子 5 和 6 给 Bess,粒子 7 给 Candy,则秘密消息和共享的五粒子不对称态组成的复合系统为:

$$|\delta\rangle_{1234567}=\frac{1}{2}(\alpha|00\rangle_{12}+\beta|11\rangle_{12})\otimes(|00101\rangle+|01110\rangle+|10101\rangle+|11110\rangle)_{34567} \tag{12}$$

要想重构出秘密,首先 Alex 对所持有的 2 个粒子以及未知粒子对(1,3)和(2,4)分别进行 bell 态测量。

由于纠缠变换的作用,所持有的粒子态将会塌缩到以下情况之一:

$${}_{24}\langle\phi^\pm|{}_{13}\langle\phi^+|\delta\rangle_{1\sim6}={}_{24}\langle\phi^\mp|{}_{13}\langle\phi^-|\delta\rangle_{1\sim6}=\frac{1}{4}(\alpha|101\rangle_{56}\pm\beta|110\rangle_{567}) \tag{13}$$

$${}_{24}\langle\psi^\pm|{}_{13}\langle\varphi^+|\delta\rangle_{1\sim6}={}_{24}\langle\psi^\mp|{}_{13}\langle\phi^-|\delta\rangle_{1\sim6}=\frac{1}{4}(\alpha|110\rangle_{56}\pm\beta|101\rangle_{567}) \tag{14}$$

$${}_{24}\langle\phi^\pm|{}_{13}\langle\psi^+|\delta\rangle_{1\sim6}={}_{24}\langle\phi^\mp|{}_{13}\langle\phi^-|\delta\rangle_{1\sim6}=\frac{1}{4}(\alpha|101\rangle_{56}\pm\beta|110\rangle_{567}) \tag{15}$$

$${}_{24}\langle\psi^\pm|{}_{13}\langle\psi^+|\delta\rangle_{1\sim6}={}_{24}\langle\psi^\mp|{}_{13}\langle\phi^-|\delta\rangle_{1\sim6}=\frac{1}{4}(\alpha|110\rangle_{567}\pm\beta|101\rangle_{567}) \tag{16}$$

发送方拥有的粒子纠缠态信息已经传递到粒子 5、6、7 上。由粒子塌缩的结果可知,式(13)和式(15)重复,式(14)和式(16)重复,他们重构未知量子信息的方案是一样的。所以只对式(13)和式(14)做方案说明,将式(13)和式(14)的状态化为:

$$\frac{1}{4}(\alpha|01\rangle+\beta|10\rangle)_{67}\otimes|1\rangle_5 \tag{17}$$

$$\frac{1}{4}(\alpha|01\rangle-\beta|10\rangle)_{67}\otimes|1\rangle_5 \tag{18}$$

$$\frac{1}{4}(\alpha|10\rangle+\beta|01\rangle)_{67}\otimes|1\rangle_5 \tag{19}$$

$$\frac{1}{4}(\alpha|10\rangle-\beta|01\rangle)_{67}\otimes|1\rangle_5 \tag{20}$$

2.1　Bess 为秘密重构者

Bess 以粒子 6 为控制比特,粒子 7 为目标比特[17],对式(17)－式(20)做受控非门运算,得到:

$$\frac{1}{4}(\alpha|0\rangle+\beta|1\rangle)_6\otimes|1\rangle_{57} \tag{21}$$

$$\frac{1}{4}(\alpha|0\rangle-\beta|1\rangle)_6\otimes|1\rangle_{57} \tag{22}$$

$$\frac{1}{4}(\alpha|1\rangle+\beta|0\rangle)_6\otimes|1\rangle_{57} \tag{23}$$

$$\frac{1}{4}(\alpha|1\rangle-\beta|0\rangle)_6\otimes|1\rangle_{57} \tag{24}$$

以式(21)为例,如果 Bess 想要恢复量子信息,需要引入一个初始态为 $|0\rangle_8$ 的辅助粒子 8,则由粒子 6 和粒子 8 构成的双粒子的态可表示为 $(\alpha|0\rangle+\beta|1\rangle)_6\otimes|0\rangle_8$,Bess 对双粒子实施一个 C-NOT 操作,把粒子 6 作为控制比特,粒子 8 作为靶比特,将会得到 $|\psi\rangle_{68}=\alpha|00\rangle_{68}+\beta|11\rangle_{68}$,这个态就是 Alex 所要发送的初始未知态。当受控非门运算为式(22)时,Bess 需要对粒子 6 实施一个幺正操作 σ_x,引入辅助粒子恢复出未知量子信息。具体结果见表 3。

表 3 Bess 重构秘密结果汇总 2

BSM	CM	NM	U_6
$\|\phi^+\rangle_{13}\|\phi^+\rangle_{24}$ or $\|\phi^-\rangle_{13}\|\phi^-\rangle_{24}$	$\alpha\|0\rangle_6+\beta\|1\rangle_6\otimes 11\rangle_{57}$	$\alpha\|0\rangle_6+\beta\|1\rangle_6\otimes 0_8$	$I+CNOT_{68}$
$\|\phi^+\rangle_{13}\|\phi^-\rangle_{24}$ or $\|\phi^-\rangle_{13}\|\phi^+\rangle_{24}$	$\alpha\|0\rangle_6-\beta\|1\rangle_6\otimes 11\rangle_{57}$	$\alpha\|0\rangle_6-\beta\|1\rangle_6\otimes 0\rangle_8$	σ_z+CNOT_{68}
$\|\phi^+\rangle_{13}\|\psi^+\rangle_{24}$ or $\|\phi^-\rangle_{13}\|\psi^-\rangle_{24}$	$\alpha\|1\rangle_6+\beta\|0\rangle_6\otimes 11\rangle_{57}$	$\alpha\|1\rangle_6+\beta\|0\rangle_6\otimes 0\rangle_8$	σ_x+CNOT_{68}
$\|\phi^+\rangle_{13}\|\psi^-\rangle_{24}$ or $\|\phi^-\rangle_{13}\|\psi^+\rangle_{24}$	$\alpha\|1\rangle_6-\beta\|0\rangle_6\otimes 11\rangle_{57}$	$\alpha\|1\rangle_6-\beta\|0\rangle_6\otimes 0\rangle_8$	$i\sigma_y+CNOT_{68}$

表 3 中：BSM 表示 Alex 对粒子实施 bell 态测量的结果，数字下标表示(1,3)和(2,4)；CM 表示经过受控非门后的状态；NM 表示引入辅助粒子；U_6 表示 Bess 恢复量子信息需要进行的幺正操作和 CNOT 操作。

2.2 Candy 为秘密重构者

Candy 以粒子 7 为控制比特，粒子 6 为目标比特，对式(17)－式(20)做受控非门运算，得到：

$$\frac{1}{4}(\alpha|1\rangle+\beta|0\rangle)_7\otimes 11\rangle_{56} \tag{25}$$

$$\frac{1}{4}(\alpha|1\rangle-\beta|0\rangle)_7\otimes 11\rangle_{56} \tag{26}$$

$$\frac{1}{4}(\alpha|0\rangle+\beta|1\rangle)_7\otimes 11\rangle_{56} \tag{27}$$

$$\frac{1}{4}(\alpha|0\rangle-\beta|1\rangle)_7\otimes 11\rangle_{56} \tag{28}$$

以式(27)为例，如果 Candy 想要恢复量子信息，需要引入一个初始态为$|0\rangle_9$的辅助粒子 9，则由粒子 7 和粒子 9 构成的双粒子的态可表示为$(\alpha|0\rangle+\beta|1\rangle)_7\otimes|0\rangle_9$，Candy 对双粒子实施 C-NOT 操作，把粒子 7 作为控制比特，粒子 9 作为靶比特，将会得到$|\psi\rangle_{79}=\alpha|00\rangle_{79}+\beta|11\rangle_{79}$，这个态就是 Alex 所要发送的初始未知态。当受控非门运算为式(26)时，Bess 需要对粒子 6 实施一个幺正操作$i\sigma_y$，引入辅助粒子恢复出未知量子信息。具体结果见表 4。

表 4 Candy 重构秘密结果汇总 2

BSM	CM	NM	U_7
$\|\phi^+\rangle_{13}\|\phi^+\rangle_{24}$ or $\|\phi^-\rangle_{13}\|\phi^-\rangle_{24}$	$\alpha\|1\rangle_7+\beta\|0\rangle_7\otimes 11\rangle_{56}$	$\alpha\|1\rangle_7+\beta\|0\rangle_7\otimes 0\rangle_9$	σ_x+CNOT_{79}
$\|\phi^+\rangle_{13}\|\phi^-\rangle_{24}$ or $\|\phi^-\rangle_{13}\|\phi^+\rangle_{24}$	$\alpha\|1\rangle_7-\beta\|0\rangle_7\otimes 11\rangle_{56}$	$\alpha\|1\rangle_7-\beta\|0\rangle_7\otimes 0\rangle_9$	$i\sigma_y+CNOT_{79}$
$\|\phi^+\rangle_{13}\|\psi^+\rangle_{24}$ or $\|\phi^-\rangle_{13}\|\psi^-\rangle_{24}$	$\alpha\|0\rangle_7+\beta\|1\rangle_7\otimes 11\rangle_{56}$	$\alpha\|0\rangle_7+\beta\|1\rangle_7\otimes 0\rangle_9$	$I+CNOT_{79}$
$\|\phi^+\rangle_{13}\|\psi^-\rangle_{24}$ or $\|\phi^-\rangle_{13}\|\psi^+\rangle_{24}$	$\alpha\|0\rangle_7-\beta\|1\rangle_7\otimes 11\rangle_{56}$	$\alpha\|0\rangle_7-\beta\|1\rangle_7\otimes 0\rangle_9$	σ_z+CNOT_{79}

表 4 中：U_7 表示 Candy 需要进行的幺正操作和 CNOT 操作。

3 方案分析

3.1 正确性分析

本文方案严格参照 bell 基测量消去粒子进行 2 次测量，每次测量消去 2 个粒子，在剩余 2 个粒子中，引入一个辅助粒子施加受控非门操作或 1 个粒子进行单粒子态测量，最后秘密重构者进行相应的幺正操作恢复未知量子态信息。整个过程基于量子秘密共享、bell 测量、受控非门操作、幺正变换等操作，使量子态在粒子间相互转换来重构秘密，具备正确性。

3.2 安全性分析

3.2.1 外部攻击

假设 Eve 纠缠的辅助粒子为$|0\rangle_e$，Alex 的测量结果为$|\phi^+\rangle_{24}$，则 Bess、Candy 和 Eve 组合的态变为：

$$(\alpha|101\rangle+\alpha|110\rangle+\beta|101\rangle+\beta|110\rangle)_{567}\otimes|0_e=(\alpha|1010\rangle+\alpha|1100\rangle+\beta|1010\rangle+\beta|1100\rangle)_{567e} \tag{29}$$

经过提取公因式和引入辅助粒子进行受控非门操作，最后塌缩到$(\alpha|00\rangle+\beta|11\rangle)|0\rangle_e$，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$|1\rangle_e$，Alex 的测量结果为$|\psi^-\rangle_{24}$，则 Bess、Candy 和 Eve 组合的态变为：

$$(\alpha|101\rangle+\alpha|110\rangle+\beta|101\rangle-\beta|110\rangle)_{567}\otimes|0_e=(\alpha|1010\rangle+\alpha|1100\rangle+\beta|1010\rangle-\beta|1100\rangle)_{567e} \tag{30}$$

直到塌缩到$(\alpha|00\rangle+\beta|11\rangle)|0\rangle_e$，Eve 仍未获取到任何有用的信息。

3.2.2 内部攻击

假设参与者一方不诚实，若 Bess 一方不诚实，Bess 拦截 Alex 发送给 Candy 的信道粒子，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，过程中会因误码率增加而被中断通信。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。同样 Alex 和 Candy 将部分测量结果公布出来,通过验证也能发现 Bess 是不诚实的。同样参与者两方 Bess 和 Candy 不诚实,通过相关验证也能被发现。

3.3　对比分析

文献[16 - 17]提出了基于三粒子不对称纠缠信道的未知单粒子态和双粒子纠缠态的共享方案,并提出了基于四粒子不对称纠缠信道的未知双粒子纠缠态的共享方案,需要实施 GHZ 态测量和联合幺正操作。而本文利用五粒子不对称纠缠态解决了秘密共方案,操作简单,不需要实施 GHZ 态测量,幺正操作也不需要联合处理,最后一步进行即可。文献[2]利用对称粒子纠缠态作为量子信道完成未知单粒子秘密共享。本文利用非对称五粒子纠缠态除了解决了未知单粒子态的秘密共享,还有未知双粒子态的秘密共享,进一步增加了方案的可选择性。

4　结　语

本文基于五粒子不对称纠缠态,提出一个量子秘密共享的方案。安全分析表明,任何一方不靠其他参与者的协助都无法重构秘密,本文方案是安全的。下一步将深入研究不对称量子信道以及多方量子通信的量子秘密共享方案及其应用。

参　考　文　献

[1] 朱珍超. 基于量子理论的秘密共享协议和对话协议研究[D]. 西安:西安电子科技大学,2011.

[2] Abulkasim H, Hamad S, Bahnasy K E, et al. Authenticated quantum secret sharing with quantum dialogue based on Bell states[J]. Physica Scripta, 2016, 91(8): 085101.

[3] Grice W P, Evans P G, Lawrie B, et al. Quantum secret sharing with phase-encoded photons[C]//2014 Conference on Lasers and Electro-Optics (CLEO)-Laser Science to Photonic Applications. IEEE, 2014: 1 - 2.

[4] Frikken K B. Secure multiparty computation[C]//Algorithms and theory of computation handbook. Chapman & Hall/CRC, 2010: 927 - 938.

[5] Arrazola J M, Wallden P, Andersson E. Multiparty quantum signature schemes[EB]. arXiv: 1505.07509, 2015.

[6] 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 - 2138,2142.

[7] 邵婷婷,张仕斌,昌燕. 基于 Bell 态的(3,3)量子秘密共享方案[J]. 计算机工程与设计,2019,40(5):1210 - 1213,1224.

[8] 王静涛. 量子秘密共享方案及其应用研究[D]. 北京:北京邮电大学,2018.

[9] 张国帅,许道云. 量子隐形传态的通用线路[J]. 软件学报,2019,30(12):3579 - 3589.

[10] Lu C B, Miao F Y, Hou J P, et al. Verifiable threshold quantum secret sharing with sequential communication[J]. Quantum Information Processing, 2018, 17(11): 310.

[11] Choi M J, Lee Y H, Lee S. Quantum secret sharing and Mermin operator[J]. Quantum Information Processing, 2018, 17(10): 258.

[12] Qin H W, Tang W K S, Tso R. Rational quantum secret sharing[J]. Scientific reports, 2018, 8(1): 11115.

[13] 于浩,贾玮,咎继业,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 W, Tso R. Efficient quantum secret sharing based on polarization and orbital angular momentum[J]. Journal of the Chinese Institute of Engineers, 2019, 42(2): 143 - 148.

[15] Bae J, Jin J W, Kim J, et al. Three-party quantum teleportation with asymmetric states[J]. Chaos, Solitons and Fractals, 2005, 24(4): 1047 - 1052.

[16] 张群永. 基于三粒子纠缠态的未知单粒子态量子秘密共享[J]. 量子电子学报,2012,29(4):421 - 426.

[17] 张群永. 基于四粒子纠缠态的量子秘密共享方案[J]. 量子电子学报,2016,33(6):718 - 723.

[18] 张群永. 基于不对称量子信道的量子态共享协议研究[D]. 苏州:苏州大学,2010.

[19] 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 - 1123,1127.

[20] 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.

[21] 魏敏娜. 多方互动量子秘密共享方案设计与分析[D]. 南京:东南大学,2016.

[22] Song Y, Li Z H, Li Y M. A dynamic multiparty quantum direct secret sharing based on generalized GHZ states[J]. Quantum Information Processing, 2018, 17(9): 244.

[23] 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.

(上接第 276 页)

[13] Shen G, Liu F, Fu Z, et al. Visual cryptograms of random grids via linear algebra[J]. Multimedia Tools and Applications, 2018, 77(10): 12871 - 12899.

[14] Biham E, Itzkovitz A. Visual cryptography with polarization [OL]. https://www.researchgate.net/publication/2872008_Visual_Cryptography_with_Polarization, 2004.

[15] Tuyls P, Hollmann H D, Lint J H, et al. XOR-based visual cryptography schemes[J]. Designs, Codes and Cryptography, 2005, 37(1): 169 - 186.

[16] 郁滨,胡浩,陈武平,等. 一种共享份分块构造的异或区域递增式视觉密码方案[J]. 电子与信息学报,2015,37(8):1978 - 1983.