一种基于纠缠交换的可验证量子秘密共享协议*

方阿芬，谭晓青†
（暨南大学 信息科学技术学院，广州 510632）

摘 要：提出了一种新的基于纠缠交换的可验证量子秘密共享协议，秘密分发者与其他参与者进行一对一的信息交互，对某一参与者等概率进入检测模式或信息模式，直至确定信息发送安全后，再与下一参与者进行信息交互。本协议不仅能够避免外部窃听，又可以防止内部欺骗，从而保证共享信息的正确性和安全性，达到可验证的效果。

关键词：量子秘密共享；纠缠交换；信息交互；可验证秘密共享
中图分类号：TP309 **文献标志码**：A **文章编号**：1001-3695(2012)04-1399-03
doi:10.3969/j.issn.1001-3695.2012.04.055

Verifiable quantum secret sharing protocol based on entanglement swapping

FANG A-fen, TAN Xiao-qing†
(*College of Information Science & Technology, Jinan University, Guangzhou* 510632, *China*)

Abstract: This paper proposed a verifiable quantum secret sharing protocol based on entanglement swapping. The dealer communicated with the participants one by one. He chose the detection pattern or information pattern by uniform distribution, until he could make sure the information to the participant was safe, and then communicated with the next participant. It could prevent not only the external eavesdropping but also the internal cheating, and guaranteed the correction and security of information shared for verifying.

Key words: quantum secret sharing (QSS); entanglement swapping; communication; verifiable secret sharing

0 引言

量子通信近年来发展迅速，其理论与应用已成为各界关注的焦点，研究重点主要在于量子密钥分发[1]、量子秘密共享(quantum secret sharing, QSS)[2]、量子安全通信[3]以及量子认证[4]等方面。

QSS 的基本思想如下：若 Alice 要传递一个秘密信息给 Bob 和 Charlie，但是 Alice 需确认以下两点：a)至少有一个代理人是诚实的；b)两个代理人合作可以解出 Alice 的秘密消息，但每一个代理人都不能单独获得关于此秘密的任何信息。需注意的是量子秘密共享是多方(三方以及三方以上)的通信，因此在通信过程中不但要排除外部窃听行为，还要防止内部潜在的欺骗行为。

自从 1999 年 Hillery 等人[2]利用 GHZ 纠缠态提出第一个 QSS 协议(称为 HBB99 协议)以来，出现了多种 QSS 方案。这些方案中，有通过量子力学特征在分享者之间共享经典信息或直接共享任意的量子消息(量子态)。按照实现秘密共享所依赖的量子力学特征，这些方案又可分为基于纠缠态的 QSS 和基于直积态的 QSS。2005 年，Zhang 等人[5]基于纠缠交换和局域幺正操作提出了一种共享经典消息的 ZM05 量子秘密共享协议。2007 年，Wang 等人[6]在 ZM05 协议基础上提出了基于纠缠交换的 QSS 协议(ES-QSS)。ZM05 协议是基于两粒子纠缠和局域幺正操作的，与 HBB99 协议相比实现简单；ES-QSS 协议是 ZM05 协议的改进，无须进行幺正操作，实现起来更容易。

文献[7] 提出了一种基于纠缠交换的 QSS 改进协议。本文分析了该协议的不安全性，并在此基础上提出了一种新的基于纠缠交换的改进 QSS 协议。本协议克服了文献[7]所提协议的不安全性，不仅能够阻止外部窃听，还能够防止内部不诚实参与者的欺骗，在多方(大于三方)秘密共享的情况下，还可以防止典型的不诚实两方合作欺骗。本协议能保证共享信息的正确性与安全性，并具有可验证的功能。

1 基于纠缠交换的 QSS 协议

文献[7]中的 QSS 协议，其原理如图 1 所示，该协议用到的纠缠态为四个 Bell 基态：

$$|\varphi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)=\frac{1}{\sqrt{2}}(|++\rangle+|--\rangle)$$
$$|\varphi^-\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)=\frac{1}{\sqrt{2}}(|+-\rangle+|-+\rangle)$$
$$|\psi^+\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)=\frac{1}{\sqrt{2}}(|++\rangle-|--\rangle)$$
$$|\psi^-\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)=\frac{1}{\sqrt{2}}(|+-\rangle-|-+\rangle)$$

其中：$|0\rangle$ 和 $|1\rangle$ 是 σ_z 的本征态，$|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$，$|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ 为 σ_x 的本征态。

收稿日期：2011-09-02；**修回日期**：2011-10-17 **基金项目**：国家自然科学青年基金资助项目(61003258)；广东省安全生产监督管理局 2010 年专项基金资助项目(34110004)

作者简介：方阿芬(1986-)，女，福建福州人，硕士研究生，主要研究方向为密码学；谭晓青(1976-)，女(通信作者)，湖南衡阳人，副教授，博士，主要研究方向为密码编码学(ttanxq@jnu.edu.cn).

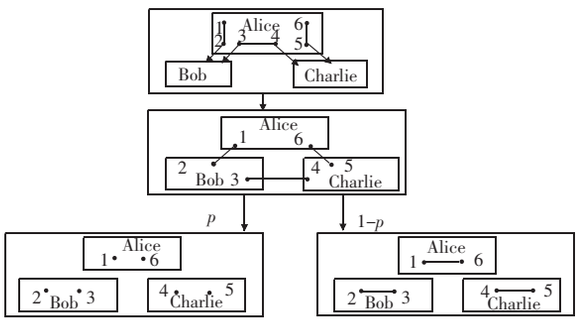

图 1 基于纠缠交换的 QSS 协议

具体步骤为(如图 1 所示):

a) Alice、Bob 和 Charlie 共同约定将四个 Bell 态 $|\varphi^+\rangle$、$|\varphi^-\rangle$、$|\psi^+\rangle$ 和 $|\psi^-\rangle$ 分别编码为经典信息比特 00、01、10 和 11。首先 Alice 产生三个纠缠态,均处于 $|\varphi^+\rangle$,并将每个纠缠态的两个粒子分别称为 1 和 2、3 和 4、5 和 6 粒子,然后 Alice 保存粒子 1 和 6,将粒子 2 和 3 按随机相对顺序发送给 Bob,同样将粒子 4 和 5 也按随机相对顺序发送给 Charlie。

b) 直到 Alice 发送粒子完毕后,接着以概率 p 选择进行检测模式,以概率 $1-p$ 选择进行信息模式。如果 Alice 选择检测模式,那么通信各方进入步骤 c);否则跳转至步骤 d)。

c) Alice 将粒子 2、3 和粒子 4、5 的相对顺序分别告之 Bob 和 Charlie,由于他们知道了粒子的相对顺序,这样 Bob 和 Charlie 就可以将粒子 2 和 5 区分出来。

接下来实施信道安全性检测。为了检测 Alice 和 Bob 之间的信道安全性,Bob 随机选择 σ_z 或者 σ_x 基对粒子 2 进行相应的测量,并将所选的基及最后测量结果告诉给 Alice,Alice 就用该测量基对粒子 1 进行测量,测量的结果应该跟 Bob 所测量的结果是相同的,从而判断出粒子 2 在给 Bob 的传输过程中的安全性。对于外部窃听者而言,由于粒子 2、3 发送顺序是随机的,那么外部窃听者就不能确切分辨出粒子 2 和 3,所以粒子 2 的安全性完全能够代表 Alice 到 Bob 之间量子信道的安全性。

同理,通过对粒子 5 实施安全性检测,可知 Alice 和 Charlie 之间信道的安全性。

若这两个量子信道都是安全的,则返回步骤 a),否则终止通信。

d) Alice、Bob 和 Charlie 分别对粒子 1、6,粒子 2、3 和粒子 4、5 进行联合 Bell 态测量,由以下等式的展开关系可得到表 1。因此,Alice 就与 Bob 和 Charlie 根据各自 Bell 态测量结果共享 2 bit 经典信息。

$$|\varphi_{12}^+\rangle\otimes|\varphi_{34}^+\rangle\otimes|\varphi_{56}^+\rangle=\frac{1}{4}\times(|\varphi_{16}^+\rangle|\varphi_{23}^+\rangle|\varphi_{45}^+\rangle+|\varphi_{16}^+\rangle|\varphi_{23}^-\rangle|\varphi_{45}^-\rangle+$$
$$(|\varphi_{16}^+\rangle|\psi_{23}^+\rangle|\psi_{45}^+\rangle+|\varphi_{16}^+\rangle|\psi_{23}^-\rangle|\psi_{45}^-\rangle+(|\varphi_{16}^-\rangle|\varphi_{23}^+\rangle|\varphi_{45}^-\rangle+|\varphi_{16}^-\rangle|\varphi_{23}^-\rangle|\varphi_{45}^+\rangle+$$
$$(|\varphi_{16}^-\rangle|\psi_{23}^-\rangle|\psi_{45}^+\rangle+|\varphi_{16}^-\rangle|\psi_{23}^+\rangle|\psi_{45}^-\rangle+(|\psi_{16}^-\rangle|\varphi_{23}^+\rangle|\psi_{45}^-\rangle-|\psi_{16}^+\rangle|\varphi_{23}^+\rangle|\psi_{45}^-\rangle+$$
$$(|\psi_{16}^-\rangle|\varphi_{23}^-\rangle|\psi_{45}^-\rangle-|\psi_{16}^-\rangle|\varphi_{23}^+\rangle|\psi_{45}^-\rangle+(|\psi_{16}^-\rangle|\psi_{23}^-\rangle|\varphi_{45}^+\rangle+|\psi_{16}^-\rangle|\psi_{23}^-\rangle|\varphi_{45}^-\rangle)$$

表 1 Alice、Bob、Charlie 测量结果对应关系

分享的秘密	Alice 测量的结果	Bob 和 Charlie 测量的结果
00	$\|\varphi_{16}^+\rangle$	$\{\|\varphi_{23}^+\rangle,\|\varphi_{45}^-\rangle\},\{\|\varphi_{23}^-\rangle,\|\varphi_{45}^+\rangle\},\{\|\psi_{23}^-\rangle,\|\psi_{45}^+\rangle\},\{\|\psi_{23}^+\rangle,\|\psi_{45}^-\rangle\}$
01	$\|\varphi_{16}^-\rangle$	$\{\|\varphi_{23}^+\rangle,\|\varphi_{45}^+\rangle\},\{\|\varphi_{23}^-\rangle,\|\varphi_{45}^-\rangle\},\{\|\psi_{23}^-\rangle,\|\psi_{45}^+\rangle\},\{\|\psi_{23}^+\rangle,\|\psi_{45}^-\rangle\}$
10	$\|\psi_{16}^+\rangle$	$\{\|\varphi_{23}^+\rangle,\|\varphi_{45}^+\rangle\},\{\|\varphi_{23}^-\rangle,\|\psi_{45}^-\rangle\},\{\|\psi_{23}^+\rangle,\|\varphi_{45}^+\rangle\},\{\|\psi_{23}^-\rangle,\|\varphi_{45}^-\rangle\}$
11	$\|\psi_{16}^-\rangle$	$\{\|\varphi_{23}^-\rangle,\|\psi_{45}^-\rangle\},\{\|\varphi_{23}^+\rangle,\|\psi_{45}^-\rangle\},\{\|\psi_{23}^-\rangle,\|\varphi_{45}^+\rangle\},\{\|\psi_{23}^+\rangle,\|\varphi_{45}^-\rangle\}$

2 不安全性分析

2.1 ZM05 协议的不安全分析

ZM05 协议强调的是所有的纠缠态都先由 Alice 来制备,待制备完成后,发送给 Bob 和 Charlie。这里假设 Bob 是不诚实的一方,Bob 截取粒子 4 并丢弃粒子 3 和粒子 4,然后制备不合要求的纠缠态:

$$|\varphi_{3^*4^*}^-\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)=\frac{1}{\sqrt{2}}(|+-\rangle+|-+\rangle)$$

这个纠缠态的两个粒子称为 3^* 和 4^*,他保留粒子 3^*,将粒子 4^* 发送给 Charlie,然后按协议步骤继续进行。由于他没有破坏粒子 2 和 5,因此通过窃听检测过程不能发现 Bob 的存在。如果 Alice 为了增加安全性,也检测粒子 3 和 4。但是 Bob 完全可以根据自己的测量结果推出 Charlie 的测量结果,公布自己应该得到的测量结果,这样 Bob 就逃过了窃听检测。在信息模式下,Bob 可以根据 Charlie 的测量结果推出粒子 2、5 的纠缠态,进而推出 Alice 的密钥,而 Charlie 只能根据 Bob 公布的信息得到错误的密钥。此时在不诚实 Bob 存在情况下,粒子 1、2、3、4、5、6 的态可表示为 $|\varphi_{12}^+\rangle\otimes|\varphi_{3^*4^*}^-\rangle\otimes|\varphi_{56}^+\rangle$,从而得到表 2。

表 2 不诚实 Bob 存在时 Alice、Bob、Charlie 测量结果对应关系

分享的秘密	Alice 测量的结果	Bob 和 Charlie 测量的结果
00	$\|\varphi_{16}^+\rangle$	$\{\|\varphi_{23}^-\rangle,\|\varphi_{45}^+\rangle\},\{\|\varphi_{23}^+\rangle,\|\varphi_{45}^-\rangle\},\{\|\psi_{23}^+\rangle,\|\psi_{45}^+\rangle\},\{\|\psi_{23}^-\rangle,\|\psi_{45}^-\rangle\}$
01	$\|\varphi_{16}^-\rangle$	$\{\|\varphi_{23}^-\rangle,\|\varphi_{45}^-\rangle\},\{\|\varphi_{23}^+\rangle,\|\varphi_{45}^+\rangle\},\{\|\psi_{23}^+\rangle,\|\psi_{45}^+\rangle\},\{\|\psi_{23}^-\rangle,\|\psi_{45}^-\rangle\}$
10	$\|\psi_{16}^+\rangle$	$\{\|\varphi_{23}^-\rangle,\|\psi_{45}^-\rangle\},\{\|\varphi_{23}^+\rangle,\|\psi_{45}^-\rangle\},\{\|\psi_{23}^+\rangle,\|\varphi_{45}^-\rangle\},\{\|\psi_{23}^-\rangle,\|\varphi_{45}^+\rangle\}$
11	$\|\psi_{16}^-\rangle$	$\{\|\varphi_{23}^-\rangle,\|\psi_{45}^-\rangle\},\{\|\varphi_{23}^+\rangle,\|\psi_{45}^+\rangle\},\{\|\psi_{23}^+\rangle,\|\varphi_{45}^+\rangle\},\{\|\psi_{23}^-\rangle,\|\varphi_{45}^-\rangle\}$

2.2 文献[7]中 QSS 协议的不安全性

对于该协议,虽然由 Alice 发送粒子 2、3 给 Bob,发送粒子 4、5 给 Charlie 是按随机的相对顺序进行的,但笔者注意到,这样虽然可以使得外部窃听者无法获取真正的发送顺序,也无法根据已知的发送粒子获得密钥,但对于内部欺骗者来说,Bob 试图截取粒子 4,丢弃粒子 3、4,并制备新的纠缠态 3^*、4^*,将 4^* 发送给 Charlie。现在由于 Alice 发送给 Charlie 的粒子 4、5 的顺序是随机的,使得 Bob 有 50% 的概率截取到的是粒子 5,这将导致 Bob 无法顺利丢弃原始的纠缠态而替换为新的欺骗性纠缠态。但 Bob 仍有 50% 的概率可以截取成功,那么它仍然可以利用自己欺骗性纠缠态 3^*、4^* 推测出 Charlie 的测量结果,故 Bob 仍有机会可以逃过窃听检测,所以该协议仍然不是完全安全的。

3 基于纠缠交换的可验证 QSS 协议

基于以上的分析,协议不安全的主要原因在于内部欺骗者总可以采取截取置换的方法来制造欺骗性纠缠态粒子。为解决这一问题,本文提出一种新的基于纠缠交换的量子秘密共享协议——基于纠缠交换一对一的可验证 QSS 协议,原理如图 2 所示。

协议步骤如下:

a) Alice 制备三个 EPR 对,分别为 $|\varphi_{12}^+\rangle$、$|\varphi_{34}^+\rangle$、$|\varphi_{56}^+\rangle$。

b) Alice 将粒子 2、3 发送给 Bob,Bob 确认收到两个粒子。

Alice 等概率地先后执行以下两个操作(即操作Ⅰ和Ⅱ的顺序等概率选择):

操作Ⅰ。Alice 按文献[7] QSS 协议中的方法进行安全性检测,以检测 Alice 与 Bob 量子信道的安全性:若信道不安全,则无须进行后面的步骤,对所传递信息予以丢弃;若信道安全,且先进行的是操作Ⅰ时则执行操作Ⅱ,或者,若先进行的是操作Ⅱ时则保留所传递的信息。

操作Ⅱ。Alice 对粒子 1、4 进行 Bell 测量,根据纠缠交换原理,测量后粒子 1、4 处于纠缠态,这时粒子 1、2、3、4 就发生了纠缠交换;与此同时,Bob 对粒子 2、3 进行相应 Bell 测量,粒子 2、3 也处于纠缠态,测量后的结果就是 Bob 所分享的部分秘密信息。相应的测量结果由以下等式确定:

$$|\varphi_{12}^{+}\rangle\otimes|\varphi_{34}^{+}\rangle=$$

$$\frac{1}{2}(|\varphi_{23}^{+}\rangle|\varphi_{14}^{+}\rangle+|\varphi_{23}^{-}\rangle|\varphi_{14}^{-}\rangle+$$

$$|\psi_{23}^{+}\rangle|\psi_{14}^{+}\rangle+|\psi_{23}^{-}\rangle|\psi_{14}^{-}\rangle)$$

这样 Alice 与 Bob 之间就单独完成了部分信息的传递,不涉及到第三方的参与。

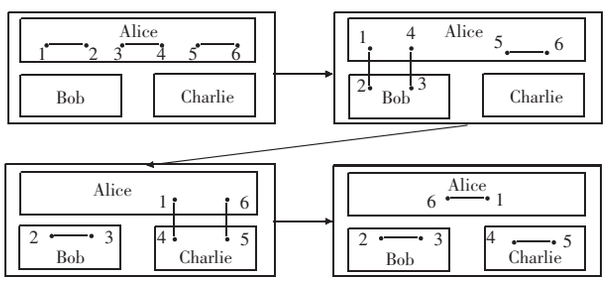

图 2　基于纠缠交换一对一的可验证 QSS 协议

c) Alice 将粒子 4、5 发送给 Charlie,Charlie 确认收到两个粒子。Alice 先后执行以下两个操作:

操作Ⅲ。Alice 按文献[7]协议中的方法进行安全性检测,以检测 Alice 与 Charlie 量子信道的安全性。由于 Alice 知道粒子 1、4 所处的 Bell 态,因此在安全性检测后,若发现信道不安全,Alice 可以再制备一个新的与原 EPR 对处于相同 Bell 态的 EPR 对来继续后面的协议操作;若信道安全,则无须再制备 EPR 对就可继续之后的操作。

操作Ⅳ。Alice 对粒子 1、6 进行相应 Bell 测量,此时粒子 1、6 也处于纠缠态。相应的测量结果由以下等式确定:

$$|\varphi_{14}^{+}\rangle\otimes|\varphi_{56}^{+}\rangle=$$

$$\frac{1}{2}(|\varphi_{45}^{+}\rangle|\varphi_{16}^{+}\rangle+|\varphi_{45}^{-}\rangle|\varphi_{16}^{-}\rangle+$$

$$|\psi_{45}^{+}\rangle|\psi_{16}^{+}\rangle+|\psi_{45}^{-}\rangle|\psi_{16}^{-}\rangle)$$

d) Alice 公布对 1、6 进行 Bell 测量的结果。依照表 1,Bob 和 Charlie 根据 Alice 公布的测量结果,可以互相合作获得Alice 所分享的原始秘密信息。

协议分析如下:

此协议由 Alice 与其他参与者单独进行一对一的粒子传递,并在传递后第一时间内完成检测或是测量,可以使得外部窃听者无法获取真正的发送顺序,也无法根据已知的发送粒子获得密钥;且对于内部欺骗者来说,由于 Alice 与 Bob 或 Charlie 都是单独两方进行秘密传递,双方在进行信道安全性检测或信息测量时,就可防止欺骗方的存在,有可验证的功能。假如 Bob 试图截取粒子 4 可以成功,那么它利用自己欺骗性纠缠态 3^{*}、4^{*}想推测出 Charlie 的测量结果,但此时粒子 4 已经不与粒子 3 处于纠缠态,而是与粒子 5 处于纠缠态,且 Bob 自身的粒子 3 却与粒子 2 处于纠缠态,故 Bob 得不到任何关于 Charlie 的秘密信息,这样又很好地避免了内部欺骗者截取置换的危险性。与文献[7]协议的比较如表 3 所示。

表 3　本文协议与文献[7]协议的比较

比较项	本文协议	文献[7]的协议
粒子传递途径	间断式	一站式
安全性	较安全	不安全
效率	较高	一般
可验证性	可验证	条件验证

不失一般性地,推广到多方的情况下(本文以经典的四方为例),假设参与者中有两者是不诚实的,分别是 Bob 和 David。在 ZM05 协议中 Bob、David 联合即可以顺利窃密[5],而应用本协议可避免这种窃密的发生。由于 Alice 对粒子 1、4 进行测量,可以强制使得粒子 2、3 产生纠缠,这样即使 Bob 将粒子 2 发送给 David 也无法获得 Alice 的任何秘密信息。所以本文改进后的协议既可以封闭性地防止外部窃听,又可以在内部欺骗存在的状况下,一方面阻止内部参与者截取置换粒子,另一方面又能防止典型的不诚实两方合作欺骗。此外该协议对文献[8]提出的假粒子欺骗攻击也是安全的。

4　结束语

本文分析了文献[7]中基于纠缠交换的 QSS 协议的不安全性,虽然由 Alice 产生所有的纠缠态,且在发送过程中随机选择给同一参与者两个粒子的相对顺序,但在内部欺骗者的存在下,仍有一定概率会受到截取置换的攻击。在此基础上,本文提出了一种基于纠缠交换的一对一的可验证 QSS 协议,此协议利用一对一的服务思想,一站式地进行消息传递,确保安全后再进行下一方信息传递,不仅可避免外部窃听,且防止了内部欺骗者存在的威胁。

参考文献:

[1] BEMETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing[C]//Proc of IEEE International Conference on Computrs. Systems and Signal Processing. New York: IEEE, 1984:175-179.

[2] HILLERY M, BUZEK V, BERTHIAUME A. Quantum secret sharing [J]. Physical Review A, 1999, 59:1829-1834.

[3] BOSTROM K, FELBINGER T. Deterministic secure direct communication using entanglement[J]. Physical Review Letters, 2002, 89(18):187902-1-187902-4.

[4] ZENG Gui-hua, ZHANG Wei-ping. Identity verification in quantum key distribution[J]. Physical Review A, 2000, 61(2):022301-022303.

[5] ZHANG Zhan-jun. Multiparty quantum secret sharing of classical messages based on entanglement swapping[J]. Physical Review A, 2005, 72(2):022303-1-022303-4.

[6] WANG Jian, CHEN Huang-qing. Quantum secure communication protocols on the basis of entanglement swapping[J]. Journal of National University of Defense Technology, 2007, 29(2):56-60.

[7] 权东晓,赵楠. 一种新的基于纠缠交换的量子秘密共享协议[J]. 电子·激光, 2011, 22(1):71-74.

[8] QIN Su-juan, WEN Qiao-yan. Improving the security of multiparty quantum secret sharing against an attack with a fake signal[J]. Physical Letters A, 2006, 357(2):101-103.