基于 GHZ 态局域测量的量子秘密共享

宋 云
(陕西师范大学计算机科学学院,陕西西安 710062)

摘 要: 提出了一个基于 GHZ 态局域测量的新颖且高效的量子秘密共享方案. 该方案充分利用了 GHZ 态 3 个粒子间的相关性,不需要进行任何酉操作或纠缠交换,只通过局域测量,就可在通信者之间建立共享联合密钥. 除去用于窃听检测的粒子,其余粒子全部用于消息传输,每个 GHZ 态可以共享一个比特经典消息,效率达到 100%. 同时,对于可能存在的攻击方式,文中给出了详细的安全性证明. 最后,建立了效率与安全的关系模型,并用 MATLAB 进行了比较深入的仿真分析.

关键词: 量子秘密共享; Greenberger-Horne-Zeilinger 态; 局域测量; 安全性分析
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2019)07-1443-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.07.007

Quantum Secret Sharing Based on GHZ States Local Measurements

SONG Yun
(*School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*)

Abstract: This paper proposes a novel quantum secret sharing (QSS) scheme based on quantum correlations among three particles in a GHZ state. Without any unitary operation or entanglement swapping, receivers can obtain the joint key by using local measurements of photons. Except a few particles which is used to check the security of quantum channel, every GHZ state can be used to share 1 bit of information. The total efficiency of the scheme approaches 100%. Taking all possible attacks into account, the security proofs are detailed. We finally establish a mathematical model about the efficiency and security of the scheme and perform simulation analyses with different parameters using MATLAB.

Key words: quantum secret sharing; Greenberger-Horne-Zeilinger state; local measurements; security analysis

1 引言

近些年来,量子通信迅速发展,相关理论与应用已成为各界关注的焦点. 目前量子通信的分支主要包括量子密钥分发(QKD)[1,2]、量子秘密共享(QSS)[3~7]、量子安全通信[8,9]以及量子认证[10~12]等. 本文主要涉及的是量子秘密共享(Quantum Secret Sharing, QSS). 假设 Alice 想让她远距离的两个助理 Bob、Charlie 获得一条秘密的消息,但是两个助理其中有一个是不可靠的,可 Alice 并不知是其中的哪一个,于是 Alice 不直接将信息传送给他们,他们可以简单地利用 QKD:①Alice 与 Bob 间分发一个密钥 K_B;②Alice 与 Charlie 间分发一个密钥 K_C;③Alice 计算 $K_A = K_B \oplus K_C$. 然后,Alice 就可以用 K_A 加密她的消息,而只有 Bob 和 Charlie 联合才能获得这个秘密. 但正如文献[3]所说,这种方案不是用量子信道实现秘密共享的好的方式,它将导致较大的资源浪费. 所以,应把所要共享的信息直接拆分成两个部分,并将其分别发送给 Bob 和 Charlie. Bob 和 Charlie 只有联合起来才能够恢复出 Alice 的秘密信息,任何一个助理单独行动都无法获得信息,这样诚实的助理就可以监督不诚实的助理,保证信息的安全. 由此可见,研究消耗更少资源、具有更高效率和安全性的量子秘密共享方案是非常重要的.

QSS 最早是由 Hillery 等人[3]在 1999 年提出的,它是利用 GHZ 纠缠态来实现的,称为 HBB99 协议. 在协议中,每个参与方持有 Greenberger-Horne-Zeilinger (GHZ) 态的一个粒子,三人都随机选用一对共轭基中的一个(X 基或 Y 基)测量自己的粒子,在公布测量基以后,只要三人选用的基相同就能建立共享联合密钥. 这与 1992 年由 Bennett 等[4]提出的量子密钥分发协议类似. 但因为 HBB 协议的非确定性,要想得到 1 bit 的经典消息,就要平均消耗 2 个 GHZ 态,因此理论上效率较低. 文献[5]提出的基于 2 粒子非正交纠缠态的 QSS 方案(KKI 协议). 文献[6]

收稿日期:2017-03-05;修回日期:2018-12-28;责任编辑:孙瑶
基金项目:国家自然科学基金(No. 61602291, No. 11671244, No. 61802241);中国博士后科学基金(No. 2018M633456);国家留学基金(No. 201806875032);陕西省自然科学基础研究计划(No. 2019JQ-472)

虽然提出了一种高效的 QSS 方案,理论上效率很高,但经典通信次数较多,并且需要两步检验窃听. 近年来,各种 QSS 方案相继提出[13~21], 发展十分迅速. 这些协议按量子态性质大致可以分为两类:一类是基于纠缠态的 QSS 方案,如文献[13~18];另一类是基于直积态的 QSS 方案,如文献[19~21]. 上述协议的发送者均是应用酉(幺正)操作将要发送的秘密信息编码到量子态粒子上,共享方须通过纠缠交换或酉(幺正)操作并进行联合测量后才能得到各自信息.

本文提出了一种基于 GHZ 三重态的局部操作的量子秘密共享方案. 文中提出的协议无需进行任何酉操作或纠缠交换,发送方与接收方之间只需进行一次量子通信,并使用局域操作和局域测量即可完成信道安全检测和秘密共享,而这些相对于联合测量更容易实现. 同时,除去用于窃听检测的粒子, 平均消耗一个 GHZ 态即可建立 1 bit 联合密钥,效率达到了 100%. 安全性分析表明,方案不仅可以抵抗外部窃听者的截获—重发攻击、内部参与者的截获—重发攻击,还能抵抗纠缠附加粒子攻击.

2 基于 GHZ 态的量子秘密共享方案

GHZ 态为

$$|\mathrm{GHZ}_{xyz}\rangle_{ABC}=\frac{1}{\sqrt{2}}[\,|0,y,z\rangle_{ABC}+(-1)^{x}|1,y\oplus 1,z\oplus 1\rangle_{ABC}].$$

其中 A,B,C 分别代表三个粒子;$x,y,z\in\{0,1\}$;$\oplus$代表模 2 加.

测量基$|+x\rangle,|-x\rangle,|+y\rangle,|-y\rangle$用基失$|0\rangle,|1\rangle$表示为

$$|+x\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),$$

$$|-x\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle),$$

$$|+y\rangle=\frac{1}{\sqrt{2}}(|0\rangle+i|1\rangle),$$

$$|-y\rangle=\frac{1}{\sqrt{2}}(|0\rangle-i|1\rangle),$$

则基$|0\rangle,|1\rangle$用基$|+x\rangle,|-x\rangle,|+y\rangle,|-y\rangle$可表示为

$$|0\rangle=\frac{1}{\sqrt{2}}(|+x\rangle+|-x\rangle),$$

$$|1\rangle=\frac{1}{\sqrt{2}}(|+x\rangle-|-x\rangle),$$

$$|0\rangle=\frac{1}{\sqrt{2}}(|+y\rangle+|-y\rangle),$$

$$|0\rangle=\frac{1}{\sqrt{2}i}(|+y\rangle-|-y\rangle).$$

下面将详细描述本协议的过程.

(1)Alice 制备一列 GHZ 态,每个 GHZ 态随机地处于$|\mathrm{GHZ}_{000}\rangle_{123}$和$|\mathrm{GHZ}_{100}\rangle_{123}$,其中:

$$|\mathrm{GHZ}_{000}\rangle_{123}=\frac{1}{\sqrt{2}}(|000\rangle_{123}+|111\rangle_{123}),$$

$$|\mathrm{GHZ}_{100}\rangle_{123}=\frac{1}{\sqrt{2}}(|000\rangle_{123}-|111\rangle_{123}).$$

对于每个纠缠态,Alice 自己保留第一个粒子,将第二个粒子和第三个粒子分别发送给 Bob 和 Charlie. 分别用 L_A,L_B,L_C 表示三人所拥有的粒子组. 假设总共有 n 个纠缠态,P 代表粒子,则 $L_A=(P_{1A},P_{2A},\cdots,P_{nA})$,$L_B=(P_{1B},P_{2B},\cdots,P_{nB})$,$L_C=(P_{1C},P_{2C},\cdots,P_{nC})$.

(2)Bob 和 Charlie 分别收到粒子序列 L_B,L_C 后,三方共同检测窃听. Alice 从自己的粒子序列 L_A 中随机抽取一些粒子,并使用基 $B_x=\{|+x\rangle,|-x\rangle\}$ 进行测量. 然后 Alice 告诉 Bob 和 Charlie 检测粒子的位置,并指定用测量基 $B_x=\{|+x\rangle,|-x\rangle\}$ 或 $B_y=\{|+y\rangle,|-y\rangle\}$ 进行测量.

对于$|\mathrm{GHZ}_{000}\rangle_{123}$和$|\mathrm{GHZ}_{100}\rangle_{123}$,在 Alice 用基 $B_x=\{|+x\rangle,|-x\rangle\}$ 测量 L_A 的情况下,我们只考虑有关联属性的测量基的组合,四种情况如下所示:

如果三方用 B_x,B_x,B_x 基来测量$|\mathrm{GHZ}_{000}\rangle_{123}$, 则

$$\begin{aligned}|\mathrm{GHZ}_{000}\rangle_{123}=\frac{1}{2}(&|+x\rangle|+x\rangle|+x\rangle\\&+|-x\rangle|-x\rangle|+x\rangle+|+x\rangle|-x\rangle|-x\rangle\\&+|-x\rangle|+x\rangle|-x\rangle)\end{aligned}\tag{1}$$

如果三方用 B_x,B_y,B_y,基来测量$|\mathrm{GHZ}_{000}\rangle_{123}$,则

$$\begin{aligned}|\mathrm{GHZ}_{000}\rangle_{123}=\frac{1}{2}(&|+x\rangle|+y\rangle|-y\rangle\\&+|-x\rangle|-y\rangle|+y\rangle+|-x\rangle|+y\rangle|+y\rangle\\&+|-x\rangle|-y\rangle|-y\rangle)\end{aligned}\tag{2}$$

如果三方用 B_x,B_x,B_x 基来测量$|\mathrm{GHZ}_{100}\rangle_{123}$,则

$$\begin{aligned}|\mathrm{GHZ}_{100}\rangle_{123}=\frac{1}{2}(&|+x\rangle|+x\rangle|-x\rangle\\&+|+x\rangle|-x\rangle|+x\rangle+|-x\rangle|-x\rangle|-x\rangle\\&+|-x\rangle|+x\rangle|+x\rangle)\end{aligned}\tag{3}$$

如果三方用 B_x,B_y,B_y 基来测量$|\mathrm{GHZ}_{100}\rangle_{123}$,则

$$\begin{aligned}|\mathrm{GHZ}_{100}\rangle_{123}=\frac{1}{2}(&|+x\rangle|+y\rangle|+y\rangle\\&+|+x\rangle|-y\rangle|-y\rangle+|-x\rangle|+y\rangle|-y\rangle\\&+|-x\rangle|-y\rangle|+y\rangle)\end{aligned}\tag{4}$$

简单分析可知,在 Alice 只用基 $B_x=\{|+x\rangle,|-x\rangle\}$ 测量 L_A 的情况下,如果另两方都采用 B_x 或 B_y 基测量,那么他们的测量结果是有关联的,见表 1.

对每个用来检测窃听的实例,Alice 要求 Bob 和 Charlie 公开他们所选择的测量结果. 这里的测量结果指测得四个态$\{|\pm x\rangle,|\pm y\rangle\}$中的那个态. 为了加强安

全性,对每个实例,Alice 随机地要求 Bob 或 Charlie 先做出声明,而 Alice 不会公开自己在这些实例中测量的基和值,她只需根据 Bob 和 Charlie 的声明以及自己的测量结果来判断它们是否满足表 1 中的关联性. 基于此,Alice 通过三方的测量结果计算错误率,如果错误率高于某个阈值,则放弃这次通信. 否则,协议继续.

表1　$|GHZ_{000}\rangle_{123}$和$|GHZ_{100}\rangle_{123}$的三方测量结果的关联性

Bob的测量结果	Charlie测量结果	Alice的测量结果 $\|+x\rangle$	Alice的测量结果 $\|-x\rangle$
$\|+x\rangle$	$\|+x\rangle$	$\|0\rangle+\|1\rangle$	$\|0\rangle-\|1\rangle$
$\|+x\rangle$	$\|-x\rangle$	$\|0\rangle-\|1\rangle$	$\|0\rangle+\|1\rangle$
$\|+y\rangle$	$\|+y\rangle$	$\|0\rangle-i\|1\rangle$	$\|0\rangle+i\|1\rangle$
$\|-y\rangle$	$\|-y\rangle$	$\|0\rangle+i\|1\rangle$	$\|0\rangle-i\|1\rangle$

Bob的测量结果	Charlie测量结果	Alice的测量结果 $\|+x\rangle$	Alice的测量结果 $\|-x\rangle$
$\|+x\rangle$	$\|+x\rangle$	$\|0\rangle-\|1\rangle$	$\|0\rangle+\|1\rangle$
$\|+x\rangle$	$\|-x\rangle$	$\|0\rangle+\|1\rangle$	$\|0\rangle-\|1\rangle$
$\|+y\rangle$	$\|+y\rangle$	$\|0\rangle+i\|1\rangle$	$\|0\rangle-i\|1\rangle$
$\|-y\rangle$	$\|-y\rangle$	$\|0\rangle-i\|1\rangle$	$\|0\rangle+i\|1\rangle$

(3) Alice, Bob 和 Charlie 在确定信道安全的情况下,对自己的每个粒子进行测量. 其中,Bob 随机用 B_x 或 B_y 基测量手中剩余的粒子并告诉 Charlie 测量基的信息,然后 Charlie 用相同基测量手中剩余的粒子并记录结果. 这些测量结果转化为二进制数,即设测量结果 $|+x\rangle$ 和 $|+y\rangle$ 对应于 1 而 $|-x\rangle$ 和 $|-y\rangle$ 对应于 0,进而构成 Bob 和 Charlie 的密钥,即 K_B 和 K_C. 同时测量基的信息也可以转化为比特串 K_a,编码方法为:当 Bob 和 Charlie 用 B_x(B_y)基来测量各自的粒子 P_{iB} 和 P_{iC} 时,K_a 的第 i 个比特为 0(1).

(4) Alice 得到密钥. 在与第(3)步中的 Bob 和 Charlie 同时测量粒子时,Alice 用测量基 B_x 测量并将测量结果编码为比特串 k,即测量结果 $|+x\rangle$ 对应于 1 而 $|-x\rangle$ 对应于 0. 同时,假设 $|GHZ_{000}\rangle_{123}$ 代表 1 而 $|GHZ_{100}\rangle_{123}$ 代表 0,Alice 可以从第(2)步后的剩余的纠缠对中得到一个比特串 $K_{A'}$. Alice 最终的密钥为 $K_A = K_{A'} \oplus K_a \oplus k$.

最后,Alice, Bob 和 Charlie 各自得到一串密钥 K_A, K_B 和 K_C. 容易验证,$K_A = K_B \oplus K_C$. 至此量子秘密共享顺利完成.

从上述方案看,Alice 和 Bob 不需要进行任何酉操作和纠缠交换,只需通过量子信道进行一次传输,并用 B_x 或 B_y 基进行测量即可完成信道安全检测和秘密共享. 除去少量用于检测量子信道安全的粒子,其余每个 GHZ 态粒子共享一个比特的经典信息.

3　安全性与效率分析

方案的安全性是基于量子信道传输的安全性,如果粒子在传输中能够有效防范各种攻击,相关信息无法被攻击者窃听,那么该秘密共享方案的安全性也就得到了保证. 事实上,就窃听而言,相对外部攻击者,内部攻击者本身就合法地拥有部分信息,并且在检测窃听过程中可以通过说谎掩盖自己,使其具有更强的窃听能力;同时,外部攻击者也可以看作是有一定限制性的内部攻击者. 因此,如果可以通过检测窃听发现参与方的窃听,那么任何窃听者(无论内部还是外部)的窃听行为均会被检测到,故本文安全性的分析重点在讨论内部攻击者所采取的攻击. 同时,方案的安全性证明是针对理想信道,即假设量子信道几乎是无噪声的.

假设内部参与者 Bob 或 Charlie 是不诚实的,想要获得诚实参与者的信息,进而得到最终的秘密信息. 想要达到此目的,唯一的机会是在 Alice 分发粒子串(第(1)步)时进行攻击. 由于方案只有这一次量子信道通信,所以对于不可见光攻击和木马攻击是免疫的. 下面就内部攻击者采用的截获—重发攻击和纠缠攻击来进行分析.

3.1　截获—重发攻击

(1)截获—测量—重发攻击

假设 Bob 是不诚实的(记为 Bob*),Bob* 在接收自己粒子序列 L_B 的同时还截获了 Alice 发给 Charlie 的粒子序列 L_C. 如果 Bob* 对截获的两个粒子进行测量(见图 1),然后将其中一个粒子发送给 Charlie,并希望由此获得 Alice 的密钥. 但是 Bob* 是随机用 B_x 或 B_y 基对所截获的粒子进行测量的,而当 Charlie 收到粒子序列 $L_{C'}$ 后,Alice 才随机挑选一些粒子让他们测量来检测窃听. 这就意味着不管 Bob* 发送什么样的假粒子给 Charlie,在第(2)步他都会以 50% 的概率被检测到.

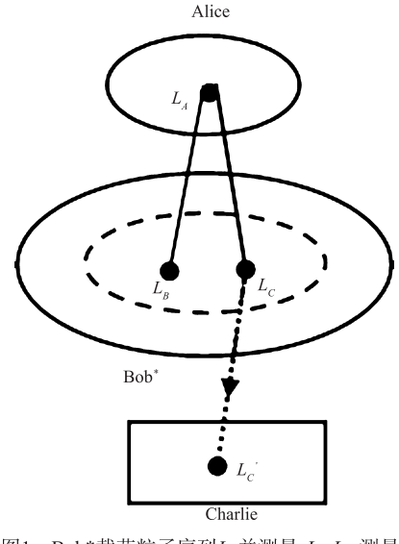

图1　Bob*截获粒子序列Lc并测量 L_B,L_C,测量后 的L_C 用 L_C,表示, 虚线表示Bob*对粒子序列 L_B, L_C 进行测量

(2)截获—重发攻击

Bob* 截获了 Alice 发给 Charlie 的粒子序列 L_C(见图 2),企图想不通过与 Charlie 的合作也能获得 Alice 的秘密消息.

Bob* 准备假粒子态 $|GHZ_{000}\rangle_{1'2'3'}$,记粒子 3′组成的粒子序列为 $L_{C'}$. Bob* 在截获了 L_C 后,将自己的假冒粒

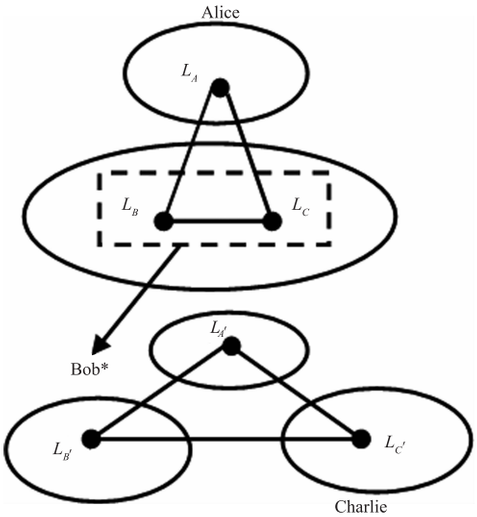

图2 Bob*截获粒子序列L_C,发送假冒粒子序列$L_{C'}$给Charlie,虚线表示Bob*窃取粒子序列L_B,L_C

子序列$L_{C'}$发送给 Charlie. 但是,因为 Charlie 的粒子与 Alice 的粒子间无任何相关性,Charlie 的测量结果是随机的. 在三方检测窃听的时候,Alice 随机地先让 Bob 和 Charlie 公布测量结果,这样 Bob 就无法欺骗 Alice,因此会被检测到.

3.2 纠缠附加粒子攻击

Stinespring Dilation 定理[22]表明,通过作用在更大希尔伯特(Hilbert)空间上的酉操作,不忠实的参与者的窃听可以实现,即将酉算子$\hat{F}$作用于诚实参与者的粒子和 s 位(s 取决于具体的攻击策略)的辅助粒子 F 上,窃听者通过测量辅助粒子获取诚实参与者的信息. 因此,以$|\mathrm{GHZ}_{000}\rangle_{123}$为例,当酉算子$\hat{F}$作用后,Alice,Bob 和 Charlie 的系统状态可以表示为

$$\hat{F}|\mathrm{GHZ}_{000}\rangle_{123}|F\rangle=|\varphi'\rangle=\sum_{ijk}|ijk\rangle_{abc}\otimes\eta_{ijk} \tag{5}$$

其中,$i,j,k=0,1$,η_{ijk}是不忠实参与者引入的 s 位辅助粒子的状态.

则 Alice,Bob 和 Charlie 用 B_x 基表示$|\varphi'\rangle$状态为

$$\begin{aligned}|\varphi'\rangle=&\frac{1}{2\sqrt{2}}(|+x\rangle+|-x\rangle)^{\otimes3}\eta_{000}+\frac{1}{2\sqrt{2}}(|+x\rangle-|-x\rangle)^{\otimes3}\eta_{111}\\=&\frac{1}{2\sqrt{2}}(|+x\rangle|+x\rangle|+x\rangle+|-x\rangle|-x\rangle|+x\rangle\\&+|+x\rangle|-x\rangle|-x\rangle+|-x\rangle|+x\rangle|-x\rangle)(\eta_{000}+\eta_{111})\\&+\frac{1}{2\sqrt{2}}(|-x\rangle|+x\rangle|+x\rangle+|+x\rangle|-x\rangle|+x\rangle\\&+|+x\rangle|+x\rangle|-x\rangle+|-x\rangle|-x\rangle|-x\rangle)(\eta_{000}-\eta_{111})\end{aligned} \tag{6}$$

另一方面,用 B_x,B_y,B_y 基表示$|\varphi'\rangle$状态为

$$\begin{aligned}|\varphi'\rangle=&\frac{1}{2\sqrt{2}}(|+x\rangle+|-x\rangle)(|+y\rangle+|-y\rangle)^{\otimes2}\eta_{000}\\&-\frac{1}{2\sqrt{2}}(|+x\rangle-|-x\rangle)(|+y\rangle-|-y\rangle)^{\otimes2}\eta_{111}\\=&\frac{1}{2\sqrt{2}}(|+x\rangle|+y\rangle|+y\rangle+|-x\rangle|-y\rangle|+y\rangle\\&+|-x\rangle|+y\rangle|-y\rangle+|+x\rangle|-y\rangle|-y\rangle)(\eta_{000}-\eta_{111})\\&+\frac{1}{2\sqrt{2}}(|-x\rangle|+y\rangle|+y\rangle+|+x\rangle|-y\rangle|+y\rangle\\&+|+x\rangle|+y\rangle|-y\rangle+|-x\rangle|-y\rangle|-y\rangle)(\eta_{000}+\eta_{111})\end{aligned} \tag{7}$$

为了在第(3)步的检测中不引入错误,根据表 1,上述两方面均可以推出 $\eta_{000}=\eta_{111}$. 这也就意味着$|\varphi'\rangle=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)\eta_{000}$.

也就是说,如果想在第(3)步不被检测到,那么不忠实的参与者的辅助粒子与 GHZ 态组成的状态空间一定是张量积的关系. 此时辅助粒子 F 的密度算子是

$$\begin{aligned}\rho_f=&\mathrm{tr}_{\mathrm{GHZ}}(|\mathrm{GHZ}_{000}\rangle|\eta'_{000}\rangle\langle\eta'_{000}|\langle\mathrm{GHZ}_{000}|)\\=&|\eta'_{000}\rangle\langle\eta'_{000}|\mathrm{tr}(|\mathrm{GHZ}_{000}\rangle\langle\mathrm{GHZ}_{000}|)\\=&|\eta'_{000}\rangle\langle\eta'_{000}|\end{aligned} \tag{8}$$

所以,von Neumann 熵 $S(\rho_f)=0$,其中 η'_{000}是 η_{000}归一化后的态.

以上分析表明不忠实的参与者通过观察自己的辅助粒子得不到任何有关 GHZ 态中三粒子的测量结果的信息. 换句话说,如果不忠实的参与者想要得到关于通信三方的测量结果的信息,就不可避免地会引入错误,从而会被检测到.

3.3 效率分析

本文的方案还具有很高的量子比特效率. 根据文献[23]量子比特效率 η_1 的定义为 $\eta_1=\frac{b_s}{q_t}$,其中 q_t 表示通过量子信道传输的总比特数,b_s 表示得到的经典比特数. 除了窃听检测所消耗的量子比特外,当 Alice 通过量子信道传送给 Bob 和 Charlie 共两个量子比特时,Bob 和 Charlie 每人都将得到一个经典比特,即 $\eta_1=\frac{2}{2}\times100\%=100\%$,其效率是文献[3,5]的两倍. 根据文献[24],量子比特效率 η_2 还可定义为 $\eta_2=\frac{q_u}{q_t}$,其中 q_u 为最终有效的量子比特数,q_t 为通过量子信道传输的总比特数. 除去用于窃听检测的量子比特外,其他均用于有效传输密钥,所以该方案量子比特的效率 η_2 的理论值(除去窃听消耗)也达到 100%. 因此,本方案的效率理论上达到最大.

3.4 效率与安全的模型

设 w 为 Eve 引入错误的概率,$\mathrm{I}_{\mathrm{Eve}}$表示 Eve 能获取

的信息量,由文献[17,24,25],w 和 I_{Eve} 满足不等式

$$I_{Eve} \leq -(1-w)\log_2(1-w) - d\log_2(\frac{3}{w}) \quad (9)$$

同时,在协议中,假设用于窃听检测的粒子占比为 p,根据量子比特效率 η_2 的定义,可得效率方程 $\eta = \frac{6n-p\cdot 6n}{6n}$,其中 n 为 Alice 发送的 GHZ 态的个数. 由于 w 为 Eve 引入错误的概率,那么 Eve 在 Alice 窃听检测阶段被发现的概率 f 为 $f=1-(1-w)^{6pn}$.

因此,由上述分析可得一个效率与安全的关系模型方程组,

$$\begin{cases} I_{Eve} \leq -(1-w)\log_2(1-w) - d\log_2(\frac{3}{w}) \\ \eta = \frac{6n-p\cdot 6n}{6n} \\ f = 1-(1-w)^{6pn} \end{cases} \quad (10)$$

不妨假设 $n=2$. 通过 MATLAB 对上述模型进行仿真分析,可以得到图 3 和图 4.

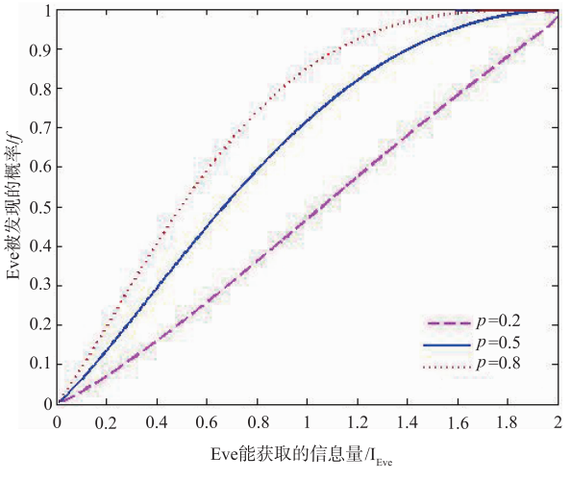

图3　I_{Eve}、p与f的变化关系

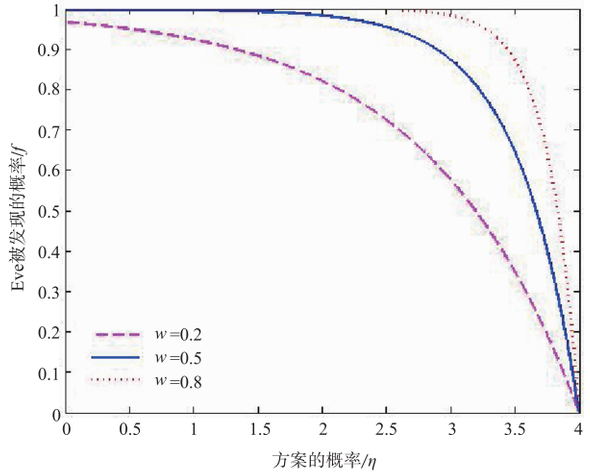

图4　η、w与f的变化关系

从图 3 分析可知,随着 Eve 获取信息量 I_{Eve} 的不断增加,检测窃听中 Eve 被发现的概率也在不断上升;从纵向可以看出,随着用于检测粒子的占比 p 的增加,Eve 被发现的风险也在明显上升. 此外,从图 3 中也可以得出该方案对于附加粒子攻击是绝对安全的,当 $w=0$,即 Eve 不引入错误时,$I_{Eve}=0$,她将得不到任何信息;当 $w>0$ 时,Eve 能得到部分信息,但面临被检测发现的风险. 图 4 是关于方案的效率 η 与 Eve 被发现的概率 f 以及引入错误的概率 w 的关系. 从横向比较不难看出,随着协议效率的不断提高,Eve 被发现的概率是不断下降的;从纵向比较,用于 Eve 引入错误的概率 w 也影响着方案的效率与安全.

从效率与安全的关系分析中不难发现,如果 Eve 能获取信息,那么她必然会引入错误;否则,她将得不到任何信息,这与前面协议的安全性分析的结论是完全相一致的.

4　结论

本文基于多粒子纠缠态 GHZ 的三个粒子所具有的关联性,提出一个在通信者之间建立共享联合密钥的量子秘密共享方案. 方案操作简单,发送方与接收方间只需量子态分发通信以及局域测量即可完成信道安全检测和秘密测量. 文章详细分析了协议的安全性,不仅列举了攻击者可能采用的攻击手段,利用 Stinepring Dilation 定理证明了方案的安全性,还利用 MATLAB 对所建立的效率和安全间的关系模型进行了比较深入的仿真分析. 除去用于窃听检测的粒子,其余粒子全部用于消息传输,平均消耗一个 GHZ 态即可完成 1bit 经典信息的秘密共享,且外部攻击者和不忠实参与方无法在不引入错误的情况下窃取秘密,从而实现了安全高效的量子秘密共享.

参考文献

[1] BROADBENT A, SCHAFFNER C. Quantum cryptography beyond quantum key distribution[J]. Designs, Codes and Cryptography, 2016, 78(1): 351 – 382.

[2] LI Y-H, CAO Y, DAI H, et al. Experimental round-robin differential phase-shift quantum key distribution[J]. Physical Review A, 2016, 93(3): 030302.

[3] HILLERY M, BUZEK V, BERTHIAUME A. Quantum secret sharing[J]. Physical Review A, 1999, 59(3): 1829.

[4] BENNETT C H, BRASSARD G, CREPEAU C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels [J]. Physical Review Letters, 1999, 70(70): 1895 – 1899.

[5] KARLSSON A, KOASHI M, IMOTO N. Quantum entanglement for secret sharing and secret splitting[J]. Physical Review A, 1999, 59: 162 – 168.

[6] GUO F-Z, WEN Q-Y, ZHU F-C. Quantum secret sharing

based on multi-particle entanglement[J]. The Journal of China Universities of Posts and Telecommunications,2005,12(1):15 – 19.

[7] 宋云,李志慧,李永明. 含至多四个参与者的量子秘密共享方案的最优信息率[J]. 电子学报,2014,42(10):1951 – 1956.
SONG Yun,LI Zhi-hui,LI Yong-ming. The optimal information rate of quantum-secret-sharing schemes based on at most four participants[J]. Acta Electronica Sinica,2014,42(10):1951 – 1956. (in Chinese)

[8] LUO Y-P,HWANG T. Authenticated semi-quantum direct communication protocols using Bell states[J]. Quantum Information Processing,2016,15(2):947 – 958.

[9] ARRAZOLA J-M,SCARANI V. Covert quantum communication[J]. Physical Review Letters,2016,117(25):250503.

[10] 雷红轩,彭家寅,刘熠. 几类非确定型量子程序的终止验证[J]. 电子学报,2016,44(12):2932 – 2938.
LEI Hong-xuan,PENG Jia-yin,LIU Yi. Termination verification of somekinks nondeterministic quantum programs [J]. Acta Electronica Sinica,2016,44(12):2932 – 2938. (in Chinese)

[11] 林运国,李永明. 基于安全性检测的广义量子 Loop 程序终止验证[J]. 中国科学:信息科学,2015,45(12):1615 – 1631.
LIN YunGuo,LI YongMing. Verification of termination of generalized quantum Loop program based on safety checking[J]. Scientia Sinica(Informationis),2015,45(12):1615 – 1631. (in Chinese)

[12] 朱皖宁,刘志昊. 基于量子计算的用户识别算法[J]. 电子学报,2018,46(1):24 – 30.
ZHU Wan-ning,LIU Zhi-hao. User identifying algorithm based on quantum computing[J]. Acta Electronica Sinica,2018,46(1):24 – 30. (in Chinese)

[13] KOGIAS I,XIANG Y,HE Q,et al. Unconditional security of entanglement-based continuous-variable quantum secret sharing[J]. Physical Review A,2017,95(1):doi 10.1103/PhysRevA.95.012315.

[14] WANG T-Y,LIU Y-Z,WEI C-Y,et al. Security of a kind of quantum secret sharing with entangled states[J]. Scientific Reports,2017,7(1):2485.

[15] ABULKASIM H,HAMAD S,ELHADAD A. Reply to comment on 'authenticated quantum secret sharing with quantum dialogue based on bell states'[J]. Physica Scripta,2018,93(2):027001.

[16] CHEN X-B,DOU Z,XU G,et al. A kind of universal quantum secret sharing protocol[J]. Scientific Reports,2017,7:39845.

[17] SONG Yun,LI Zhihui,LI Yongming. A dynamic multi-party quantum direct secret sharing based on generalized GHZ states[J]. Quantum Information Processing,2018,17(9):244.

[18] LU H,ZHANG Z,CHEN L-K,et al. Secret sharing of a quantum state[J]. Physical Review Letters,2016,117(3):030501.

[19] BAI C-M,LI Z-H,LIU C-J,et al. Quantum secret sharing using orthogonal multiqudit entangled states[J]. Quantum Information Processing,2017,16(12):304.

[20] WANG J,LI L,PENG H,et al. Quantum-secret-sharing scheme based on local distinguishability of orthogonal multiqudit entangled states[J]. Physical Review A,2017,95(2):022320.

[21] XU J,YUAN J-B. Improvement and extension of quantum secret sharing using orthogonal product states[J]. International Journal of Quantum Information,2014,12(1):1450008(1) – 1450008 (10).

[22] BOSTRÖM K,FELBINGER T. Secure direct communication using entanglement[J]. Physical Review Letters,2002,89(18):203 – 209.

[23] CABELLO A. Quantum key distribution in the Holevo limit [J]. Physical Review Letters,2000,85(26):5635 – 5638.

[24] 冯志宏,谭晓青,梁翠. 基于 Bell 态与其纠缠性质的量子密钥分发[J]. 计算机应用研究,2015,32(3):873 – 876.
FENG Zhi-hong,TAN Xiao-qing,LIANG Cui. Quantum key distribution protocol based on Bell states and its entanglement[J]. Application Research of Computers,2015,32(3):873 – 876. (in Chinese)

[25] GAO,F,GUO,F-Z,WEN,Q-Y,et al. Quantum key distribution without alternative measurements and rotations[J]. Physics Letters A,2006,349(1 – 4):53 – 58.

作者简介

宋 云 女,1987 年生于陕西西安. 现为陕西师范大学计算机科学学院讲师、硕士生导师. 研究方向为有限域、密码学.
E-mail:songyun09@snnu.edu.cn