(4,4)的量子秘密共享协议及其模型化检测

江英华, 张仕斌, 杨帆, 昌燕, 张航

成都信息工程大学网络空间安全学院, 四川 成都 610225

摘要 根据GHZ(Greenberger-Horne-Zeilinger)态的纠缠特性,设计了一种基于五粒子GHZ态的量子秘密共享协议。协议中由发起者制备五粒子GHZ态的量子序列,秘密共享方总人数为4,只有当4个人都参与解密时才能解出秘密信息。分析了协议的正确性和安全性,结果表明协议能抵抗截获重发攻击、中间人攻击和纠缠攻击。当诱惑粒子存在时,使用模型化工具Prism得到了窃听者在不同噪声环境下被发现的概率。

关键词 量子光学; 秘密共享; 纠缠; 模型化检测

中图分类号 TN918.1 **文献标识码** A

doi: 10.3788/LOP54.122704

(4,4) Quantum Secret Sharing Protocol and Its Modeling Checking

Jiang Yinghua, Zhang Shibin, Yang Fan, Chang Yan, Zhang Hang

School of Cybersecurity, Chengdu University of Information Technology, Chengdu, Sichuan 610225, *China*

Abstract According to the entanglement features of GHZ (Greenberger-Horne-Zeilinger) states, a quantum secret sharing protocol based on the five-particle GHZ state is designed. In the protocol, the quantum sequence of the five-particle GHZ state is prepared by the initiator, and the total number of the secret sharing parties is 4. Only when all the four people are involved in decryption can the secret information be solved. The correctness and security of the protocol are analyzed, and the results show that the protocol can be used to resist the interception retransmission attack, the man-in-the-middle attack and the entanglement attack. When the temptation particles exist, the probabilities of being found for the eavesdroppers under different noise environments are obtained by using the modeling tool Prism.

Key words quantum optics; secret sharing; entanglement; modeling checking

OCIS codes 270.5568; 270.5565

1 引 言

在导弹发射、遗嘱生效、银行联名账户使用资金等场合,为了加强信息的安全性,会让多个人共同持有保密信息。基于这种场景,学者们设计了秘密共享这种秘密保护方式。在秘密共享协议中,秘密信息按照一定规则被拆分成若干部分,并被分别分配给不同的参与者保管;而当需要使用秘密信息时,必须由保密信息持有者共同参与解密才能够得到秘密信息。1998年,Hillery等[1]将量子的特性融入到经典秘密共享理论之中,利用三粒子GHZ(Greenberger-Horne-Zeilinger)态的关联特性,提出了第一个量子秘密共享方案。2007年,Yan等[2]提出了一种多方与多方的量子秘密共享方案。2008年,Lin等[3]提出了一种基于纠缠交换的量子秘密共享方案。2011年,Yang等[4]提出了一种抗集体振幅阻尼噪声的容错量子秘密共享方案。2012年,Mouzali等[5]提出了一种具有纠错功能的量子秘密共享协议方案。而近年来,量子秘密共享得到快速发展,一系列的研究成果被报道[6-12]。

收稿日期: 2017-06-16; **收到修改稿日期**: 2017-07-21

基金项目: 国家自然科学基金(61572086, 61402058)

作者简介: 江英华(1989—),男,硕士研究生,主要从事量子通信方面的研究。E-mail: 250364629@qq.com

导师简介: 张仕斌(1971—),男,博士,教授,硕士生导师,主要从事量子安全通信和网络空间安全方面的研究。E-mail: cuitzsb@cuit.edu.cn(通信联系人)

上述研究大多使用额外的粒子,存在安全性有漏洞。本文提出了一种基于五粒子 GHZ 态的(4,4)秘密共享协议,即 1 名发起者将秘密信息分配给 4 名不同的参与者,当需要得到秘密信息时,需要 4 名参与者共同合作,在共享者人数上有了进一步增加。并且不需要使用额外粒子,而是将其中 1 个纠缠粒子的信息共享给了所有参与者,解决了文献[1]秘密共享协议中信息泄漏的问题。当诱惑粒子存在时,使用模型化工具得到了不同噪声环境下窃听者被发现的概率,证明了协议的安全性,所提协议能够抵御截获重发攻击、中间人攻击和纠缠攻击。

2 理论基础

2.1 三粒子 GHZ 态的纠缠关联

处于 Z 基下的三粒子 GHZ 态的波函数为 $\varphi=1/\sqrt{2}(|000\rangle+|111\rangle)_{123}$,其在 X 基下的表示方式为

$$\varphi=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{123}=\frac{1}{\sqrt{2}}(|0\rangle|0\rangle|0\rangle+|1\rangle|1\rangle|1\rangle)_{123}=\frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|+\rangle+|-\rangle)\otimes\frac{1}{\sqrt{2}}(|+\rangle+|-\rangle)\otimes\frac{1}{\sqrt{2}}(|+\rangle+|-\rangle)+\frac{1}{\sqrt{2}}(|+\rangle-|-\rangle)\otimes\frac{1}{\sqrt{2}}(|+\rangle+|-\rangle)\otimes\frac{1}{\sqrt{2}}(|+\rangle+|-\rangle)\right]=\frac{1}{2}(|+++\rangle+|+--\rangle+|-+-\rangle+|--+\rangle)_{123},\tag{1}$$

式中$|+\rangle$表示粒子的偏振角度为 45°,$|-\rangle$表示粒子的偏振角度为 135°。

由(1)式可知,粒子 1、2、3 具有等效性。当其中 1 个粒子的状态为$|+\rangle$时,另外 2 个粒子的状态为$|+\rangle|+\rangle$或$|-\rangle|-\rangle$;当其中 1 个粒子的状态为$|-\rangle$时,另外 2 个粒子的状态为$|+\rangle|-\rangle$或$|-\rangle|+\rangle$。

2.2 五粒子 GHZ 态的纠缠关联

处于 Z 基下的五粒子 GHZ 态的波函数为 $\varphi=(|00000\rangle+|11111\rangle)_{12345}/\sqrt{2}$,其在 X 基下的表示方式为

$$\varphi=\frac{1}{\sqrt{2}}(|00000\rangle+|11111\rangle)_{12345}=\frac{1}{4}(|+++++\rangle+|+++--\rangle+|++-+-\rangle+|++--+\rangle+|+-+-+\rangle+|+-++-\rangle+|+--+-\rangle+|+----\rangle+|-++++\rangle+|-+-++\rangle+|-++-+\rangle+|-+---\rangle+|--++-\rangle+|--+--\rangle+|---+-\rangle+|----+\rangle)_{12345}。\tag{2}$$

由(2)式可知,五粒子 GHZ 态也存在上述三粒子 GHZ 态表现出的特性。整理(2)式,得到第 1、2 粒子状态与 3、4、5 粒子状态的对应表,见表 1。

表 1 第 1、2 粒子状态与 3、4、5 粒子状态的对应

Table 1 Correspondence between state of particles 1,2 and state of particles 3,4,5

Particle 1,2 status	$\|++\rangle$	$\|--\rangle$	$\|+-\rangle$	$\|-+\rangle$
Particle 3,4,5 status	$\|+++\rangle$	$\|+++\rangle$	$\|++-\rangle$	$\|++-\rangle$
	$\|+--\rangle$	$\|+--\rangle$	$\|+-+\rangle$	$\|+-+\rangle$
	$\|-+-\rangle$	$\|-+-\rangle$	$\|-++\rangle$	$\|-++\rangle$
	$\|--+\rangle$	$\|--+\rangle$	$\|---\rangle$	$\|---\rangle$

由表 1 可知,当粒子 3,4,5 粒子处于$|+++\rangle$,$|+--\rangle$,$|-+-\rangle$,$|--+\rangle$中的任意状态时,粒子 1,2 的状态相同,为$|++\rangle$或$|--\rangle$。当粒子 3,4,5 粒子处于$|++-\rangle$,$|+-+\rangle$,$|-++\rangle$,$|---\rangle$中的任意状态时,粒子 1,2 的状态相反,为$|+-\rangle$或$|-+\rangle$。分析(2)式可得,五个粒子中的任意两个粒子都存在类似的关系。总之,当知道五个粒子中某三个粒子的状态时,就能判断出剩下两个粒子的状态是相同($|++\rangle$或$|--\rangle$)还是相反($|+-\rangle$或$|-+\rangle$)。

根据以上性质,假设一种场景,即 Alice、Bob、Charlie、David 在第三方(TP)存放了一个物品,TP 制备 n 对处于五粒子纠缠态 $\varphi=1/\sqrt{2}(|00000\rangle+|11111\rangle)_{12345}$ 的粒子序列。TP 将 φ 中下标为 1(2,3,4,5)的粒子

提出来，按原有顺序编成量子序列 $S_1(S_2,S_3,S_4,S_5)$。TP 自己保留 S_1，并将 S_2,S_3,S_4,S_5 通过量子传输信道一一对应分别发送给 Alice，Bob，Charlie，David。经过一系列操作之后，Alice，Bob，Charlie，David 分别获得一串量子序列，但是他们手中的信息并不携带任何有效信息。当他们想取出存放在 TP 的物品时，需要每个人的参与才能获得最终的秘密信息，进而提取出物品。

3 协议描述

由于 4 个参与者的操作类似，以 TP 与 Alice 秘密共享为重点介绍协议。具体步骤如下。

1) TP 制备 n 对处于 GHZ 态 $\varphi=1/\sqrt{2}\,(|00000\rangle+|11111\rangle)_{12345}$ 的五粒子，在 S_2、S_3、S_4、S_5 相同位置处插入具有相同状态的诱惑粒子(包含$|0\rangle$，$|1\rangle$，$|+\rangle$和$|-\rangle$)。TP 通过量子传输信道将 S_2,S_3,S_4,S_5 分别发送给 Alice，Bob，Charlie，David。

2) 所有参与者都收到量子序列之后，通知 TP。TP 接到通知之后，公布诱惑粒子的位置和使用的基(X 基或 Z 基)。4 名参与者都抽出相应位置的诱惑粒子，选择 TP 公布的基来检测其状态。4 名参与者通过经典信道与 TP 比对测量结果，若每一个参与者出现的错误测量结果都低于错误阈值，进行下一步；若任意一个用户出现的错误测量结果高于错误阈值，放弃此次通信。

3) TP 和 4 名参与者都使用 X 基测量手中的量子序列。

4) TP 将 S_1 的测量结果按照$|+\rangle$编码为 1、$|-\rangle$编码为 0 的规则生成一个二进制密钥序列 k。

5) Alice 按照图 1 所示规则公布量子序列 S_2 的第 2、3、4 段的状态，并保留第 1 段的状态。Bob，Charlie 和 David 根据图 1 也进行类似的操作(黑色部分为需要保密的量子序列状态，蓝色部分为需要公开的量子序列状态)。

6) Alice 将 S_2 中保留的测量结果按照$|+\rangle$编码为 1、$|-\rangle$编码为 0 的规则生成一个二进制密钥序列 k_1：若 Bob，Charlie 和 David 公布的第 1 段(图 1 中第 1 段蓝色的部分)第 i 位测量结果为$|+++\rangle$，$|+--\rangle$，$|-+-\rangle$，$|--+\rangle$中的一种，则 k_1 对应的第 i 位的二进制数不变；若 Bob，Charlie 和 David 公布的第 1 段第 i 位测量结果为$|++-\rangle$，$|+-+\rangle$，$|-++\rangle$，$|---\rangle$中的一种，则 k_1 对应的第 i 位的二进制数取反(1 变为 0，0 变为 1)。经过如上的操作，Alice 得到一个新的二进制字符串 k_1'。

7) 完成以上操作之后，k_1'与 k 的前 1/4 段的值是相同的。Bob，Charlie 和 David 经过类似的操作，分别获得 k_2'，k_3'和 k_4'。k_1'，k_2'，k_3'和 k_4'的值分别为 k 的一部分，当它们组合在一起就是 k，即参与者获得了 TP 手中的密钥 k。

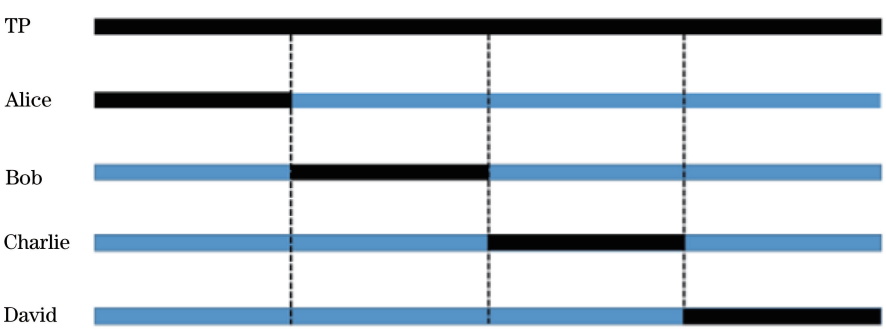

图 1 TP 与参与者公布的量子测量状态图

Fig. 1 Diagram of quantum measurement state published by TP and participants

4 协议分析

4.1 协议的正确性分析

TP 用 X 基对自己手中的 S_1 进行测量之后，根据五粒子 GHZ 态 $\varphi=(|00000\rangle+|11111\rangle)_{12345}/\sqrt{2}$ 的纠缠特性，S_2、S_3、S_4、S_5 会发生相应的变化。具体而言，当 TP 对 S_1 进行 X 基的测量之后，五个粒子的状态

会以相同的概率(概率为 1/16)处于(2)式中的 16 种状态之中。Alice 与 TP 之间的量子序列编码见表 2。

表 2 Alice 与 TP 的秘密共享情况

Table 2 Secret sharing case of Alice and TP

Status	S_3, S_4, and S_5	$\|+++\rangle$, $\|+--\rangle$, $\|-+-\rangle$, $\|--+\rangle$		$\|++-\rangle$, $\|+-+\rangle$, $\|-++\rangle$, $\|---\rangle$	
	S_1	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$
First segment value of k		1	0	1	0
Status of S_2		$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$
k_1		1	0	0	1
k_1'		1	0	1	0

由表 2 可知,当 S_3、S_4、S_5 测量结果为$|+++\rangle$、$|+--\rangle$、$|-+-\rangle$、$|--+\rangle$中的一种时,S_1 与 S_2 的测量结果相同,根据编码规则,得出的 k 值与 k_1 值相同。当 S_3、S_4、S_5 测量结果为$|++-\rangle$、$|+-+\rangle$、$|-++\rangle$、$|---\rangle$中的一种时,S_1 与 S_2 的测量结果相反,根据编码规则,得出的 k 值与 k_1 值相反,这时需要对 k_1 的值进行修正,完成修正之后 $k=k_1'$。在获得秘密信息时,这个过程相当于让 Alice 获得了 k 的一部分信息,完成了对 Alice 的秘密信息传递。Bob,Charlie 和 David 经过类似的操作也能获得 k 的一部分信息,当所有人都完成以上步骤,就完成了秘密信息的共享。

4.2 协议的安全性分析

4.2.1 截获重发攻击和中间人攻击

当信道不安全、存在截获重发攻击和中间人攻击时,由于 TP 在量子序列 S_2、S_3、S_4、S_5 相同位置处插入了相同状态的诱惑粒子,窃听者不知道诱惑粒子插入的位置和状态,只能随机选择基(选 X 基和 Z 基的概率都为 50%)进行测量。根据量子不可克隆定理,窃听者选错基对诱惑粒子进行测量之后,诱惑粒子的状态会发生变化。当 TP 公布诱惑粒子的位置和选择的基之后,由于 TP 插入的 S_2、S_3、S_4、S_5 中的诱惑粒子的位置和状态相同,则 Alice、Bob、Charlie 和 David 都可以根据 TP 公布的诱惑粒子的位置把诱惑粒子抽取出来,用 TP 公布的基检测其状态,4 名参与者可通过经典信道与 TP 比对测量结果。TP 根据诱惑粒子状态出现错误的阈值判断信道是否安全。如果出现错误的测量结果概率低于阈值,则不存在截获重发攻击和中间人攻击;若测量出现错误的测量结果概率高于阈值,则存在截获重发攻击和中间人攻击,放弃此次通信。

由于量子现象具有随机性,而随机事件都是用概率来描述的,因此基于概率的模型检测是分析量子现象最恰当的方法。模型化工具 Prism 软件就是为了对具有随机或者概率行为的系统进行建模和验证而设计的。具体而言,模型存在四个模块,分别是发送端模块、信道模块、接收端模块和窃听模块。在模型中模拟粒子在各个模块中的状态,再统计出窃听行为被发现的概率,过程如图 2 所示。

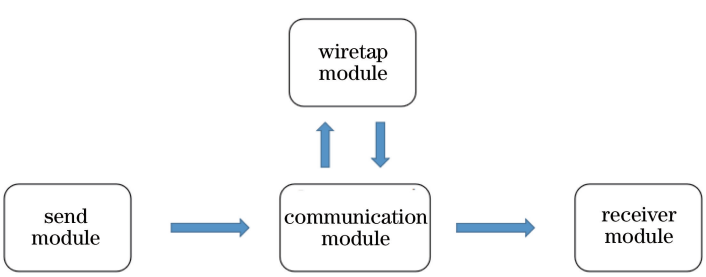

图 2 粒子在模型中的传递过程

Fig. 2 Transmission process of particles in model

对于将单光子的偏振态作为诱惑粒子的情况,当诱惑粒子被窃听者截取然后重发之后,使用模型化工具 Prism 检测参与者发现窃听者的概率。其中 n 为诱惑粒子数量,P_1 为窃听者在无噪声情况下被发现的概率,P_2 为窃听者在低噪声情况(诱惑粒子有 70%的概率保持其初始状态)下被发现的概率,P_3 为窃听者在高噪声情况(诱惑粒子有 50%的概率保持其初始状态)下被发现的概率,结果如图 3 所示。

由图 3 可知,当存在足够的诱惑粒子时,窃听者被发现的概率接近于 1,证明协议能够抵御截获重发攻击和中间人攻击。

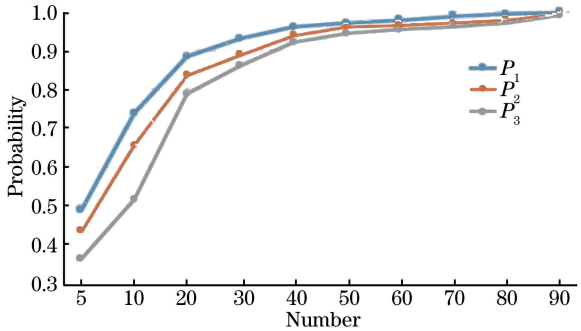

图 3 不同数量的诱惑粒子在不同噪音下窃听者被发现的概率

Fig. 3 Probability of being found for eavesdroppers under different numbers of lure particles under different noises

4.2.2 纠缠攻击

由于用户 Alice,Bob,Charlie 和 David 具有等效性,因此窃听者 Eve 对任意一个用户的窃听过程都是一样的。先假设窃听者 Eve 对用户 Alice 的粒子 S_2 进行截获,并对 S_2 中粒子进行纠缠,选用的附加粒子为 g(初始状态为$|0\rangle$)。Eve 截获 S_2 后,将 S_2 中的粒子经过控制非门与 g 进行纠缠。S_2 中的粒子为控制位,附加粒子 g 为靶位,有

$$|0\rangle_{S_2}|0\rangle_g \rightarrow |0\rangle_{S_2}|0\rangle_g, \tag{3}$$

$$|1\rangle_{S_2}|0\rangle_g \rightarrow |1\rangle_{S_2}|1\rangle_g。 \tag{4}$$

由(3)式可知,当控制位粒子状态为$|0\rangle$时,靶位粒子状态不变。当控制位粒子状态为$|1\rangle$时,靶位粒子状态改变(由$|0\rangle$变为$|1\rangle$)。由于 Eve 并不知道随机插入的诱惑粒子的状态,在对$|+\rangle$和$|-\rangle$进行纠缠时,发生以下变化:

$$|+\rangle_{S_2}|0\rangle_g \rightarrow \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_{S_2}|0\rangle_g \rightarrow \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{S_2g}, \tag{5}$$

$$|-\rangle_{S_2}|0\rangle_g \rightarrow \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)_{S_2}|0\rangle_g \rightarrow \frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)_{S_2g}。 \tag{6}$$

由(5)、(6)式可知,诱惑粒子的状态已经被改变,故当用户 Alice 进行窃听检测时,会发现窃听行为存在而放弃通信。

4.2.3 对用户的安全性分析

在 Hillrey 等[1]的量子秘密共享协议中,用户 A 拥有密文,用户 B 拥有密钥,两名用户都是合法用户。用户 A 对用户 B 的量子窃取行为是不会被发现的(窃听粒子会被合法用户排除掉)。由于秘密信息已经编码在量子序列中,这时候就会造成信息泄露。在本协议中,秘密信息是在各方都收到量子序列之后,利用量子纠缠的特性传输给各个用户的,故合法用户就算躲过了窃听检测,还是无法获得有效信息。

假设用户 Bob 想知道 Alice 手中 k_1 的值,Bob 有两种策略。

1) 利用自己手中的粒子进行推测,由于 Charlie 和 David 的测量结果都会公开,因此 Bob 不需要去窃取 Charlie 和 David 的信息。而对于 Alice 的信息,Bob 可根据自己、Charlie 和 David 的信息进行分析。当 Bob 对量子序列 S_3 进行测量以后,由表 1 可知,S_3、S_4、S_5 测量结果为$|+++\rangle$,$|+--\rangle$,$|-+-\rangle$,$|--+\rangle$中的一种时,S_1 与 S_2 的测量结果相同。但 Bob 并不知道是$|+\rangle|+\rangle$还是$|-\rangle|-\rangle$(因为$|+\rangle|+\rangle$和$|-\rangle|-\rangle$的概率各为 50%)。当 S_3、S_4、S_5 测量结果为$|++-\rangle$,$|+-+\rangle$,$|-++\rangle$,$|---\rangle$中的一种时,S_1 与 S_2 的测量结果相反,Bob 只知道 Alice 和 TP 手中的粒子为$|+\rangle|-\rangle$或者$|-\rangle|+\rangle$,但并不知道是$|+\rangle|-\rangle$还是$|-\rangle|+\rangle$(因为$|+\rangle|-\rangle$或$|-\rangle|+\rangle$的概率各为 50%)。故 Alice 和 TP 手中的粒子状态对于 Bob 来说都是未知的。

2) 对 Alice 的序列 S_2 进行窃听,那么在 TP 公布窃听粒子之前,Bob 只是一个普通的窃听者。根据 4.2.1中的分析可知,Bob 的窃听行为会被发现,并不能获得有效的信息。

由以上分析可知,发起者并没有把自己的量子信息发送给任意一名参与者,故就不存在文献[1]中信息

泄露的情况。

5 结 论

提出了一种基于五粒子 GHZ 态的(4,4)秘密共享协议。分析结果表明,所提协议能够抵御截获重发攻击、中间人攻击和纠缠攻击。当存在窃听粒子时,使用模型化工具 Prism 得到了不同噪声环境下窃听者被发现的概率,结果证明了协议的安全性。所提协议简单,且参与者增多,能解决参与者不诚信的问题。

参 考 文 献

[1] Hillery M, Bužek V, Berthiaume A. Quantum secret sharing[J]. Physical Review A, 1998, 59(3): 1829-1834.

[2] Yan F L, Gao T, Li Y C. Quantum secret sharing between multiparty and multiparty with four states[J]. Science in China Series G: Physics, Mechanics & Astronomy, 2007, 50(5): 572-580.

[3] Lin S, Gao F, Qin S J, *et al*. Quantum secret sharing between multiparty and multiparty with entanglement swapping[J]. The Journal of China Universities of Posts and Telecommunications, 2008, 15(4): 63-68.

[4] Yang Y G, Chai H P, Wang Y, *et al*. Fault tolerant quantum secret sharing against collective-amplitude-damping noise[J]. Science in China Series G: Physics, Mechanics & Astronomy, 2011, 54(9): 1619-1624.

[5] Mouzali A, Merazka F, Markham D, *et al*. Quantum secret sharing with error correction[J]. Communications in Theoretical Physics, 2012, 58(11): 661-671.

[6] Gao T, Yan F L, Li Y C. Quantum secret sharing between m-party and n-party with six states[J]. Science in China Series G: Physics, Mechanics & Astronomy, 2009, 52(8): 1191-1202.

[7] Hao L, Li J L, Long G L. Eavesdropping in a quantum secret sharing protocol based on Grover algorithm and its solution[J]. Science in China Series G: Physics, Mechanics & Astronomy, 2010, 53(3): 491-495.

[8] Zhu Z C, Zhang Y Q, Fu A M. Cryptanalysis and improvement of a quantum secret sharing scheme based on χ-type entangled states[J]. Chinese Physics B, 2012, 21(1): 1-5.

[9] Chen P, Deng F, Long G. Multiparty quantum secret sharing of classical and quantum messages[J]. Progress in Natural Science: Materials International, 2007, 17(1): 26-31.

[10] Guo Dabo, Zhang Yanhuang, Wang Yunyan. Performance optimization for reconciliation of Gaussian quantum key distribution[J]. Acta Optica Sinica, 2014, 34(1): 0127001.
郭大波, 张彦煌, 王云艳. 高斯量子密钥分发数据协调的性能优化[J]. 光学学报, 2014, 34(1): 0127001.

[11] Gao Kun, Nie Min, Yang Guang, *et al*. Performance of free-space quantum communication in context of rainfall[J]. Laser & Optoelectronics Progress, 2017, 54(1): 012701.
高锟, 聂敏, 杨光, 等. 降雨背景下自由空间量子通信的性能研究[J]. 激光与光电子学进展, 2017, 54(1): 012701.

[12] Yan Jin, Wang Xiaokai, Guo Dabo, *et al*. Security analysis of post-processing in quantum Gaussian key distribution [J]. Acta Optica Sinica, 2016, 36(3): 0327003.
阎金, 王晓凯, 郭大波, 等. 量子高斯密钥分发中后处理的安全性分析[J]. 光学学报, 2016, 36(3): 0327003.