第 49 卷 第 13 期/2022 年 7 月/中国激光 研究论文

中国激光

基于 G-like 态的两方半量子密钥协商协议

何业锋，庞一博*，狄曼，岳玉茹，李国庆，刘继祥

西安邮电大学网络空间安全学院，陕西 西安 710121

摘要 量子密钥协商协议虽然可以实现参与者之间建立安全共享密钥的目的，但是目前大多数量子密钥协商协议对参与者能力和设备的要求较高。针对此问题，利用 G-like 态的纠缠特性和测量-重发操作方法提出了一个两方半量子密钥协商协议。该协议允许两个半量子参与方在一个具备全量子能力的可信第三方协助下公平地建立安全共享密钥。由于两个半量子方只需要执行反射操作以及进行简单的量子态制备和测量，因此该协议降低了对参与者能力和设备的要求。最终，安全性分析证明了该协议可以很好地抵抗参与者攻击和外部攻击。并且，该协议在性能方面也有一定优势。

关键词 量子光学；量子密码；半量子密钥协商；G-like 态；量子比特效率

中图分类号 TN918 **文献标志码** A **DOI**：10.3788/CJL202249.1312001

1 引 言

量子密码是密码学和量子力学相结合产生的新研究领域，它的安全性由量子力学基本原理保证。因此，理论上量子密码可以实现无条件安全，它吸引了研究者的广泛关注。目前，量子密码的研究主要包括以下几个方向：量子密钥分发（QKD）[1-7]、量子密钥协商（QKA）[8-10]、量子秘密共享（QSS）[11-12]以及量子安全直接通信（QSDC）[13-14]等。其中，QKA 是量子密码的一个重要分支，它允许两个或多个参与者通过公开量子信道共同协商建立一个共享密钥，并且要求参与者对共享密钥的贡献是相等的，也就是说任意部分参与者不能独自控制共享密钥。

目前，学者们在 QKA 协议方面开展了很多研究。2004 年，Zhou 等[15]基于量子隐形传态提出了第一个 QKA 协议。之后，在 BB84 协议的基础上，Chong 等[16]利用幺正变换和延迟测量技术[17]提出了一个两方 QKA 协议。随后 QKA 协议也被扩展到了多方。2013 年，Shi 等[18]设计了一个多方量子密钥协商协议。然而，Liu 等[19]指出，这个 QKA 协议不能很好地抵御参与者攻击，并且基于单光子提出了一个新的多方 QKA 协议。之后，Sun 等[20]提出了一个环形多方 QKA 协议，解决了多方 QKA 协议的效率问题。2016 年，He 等[21]还提出了一种免疫噪声的 QKA 协议。然而，以上 QKA 协议要求所有参与者必须拥有性能良好的量子设备。但是，在实际应用中，量子设备比较昂贵且不易携带，因此并非所有参与者都可以满足该要求。为了应对这种情况，2017 年，Shukla 等[22]基于 Bell 态提出了一个两方半量子密钥协商协议。此处的半量子密钥协商协议（SQKA）是指协议中的一个参与者具备全量子能力，其他参与者只具备半量子能力。其中，具备全量子能力的实体可以是一些大型机构或公司，而具备半量子能力的实体则是一些普通用户，即他们只能使用 Z 基（$|0\rangle$，$|1\rangle$）进行量子态的制备和测量。同年，Liu 等[23]提出了一种基于 Bell 态和委托量子计算的多方半量子密钥协商协议。2020 年，Zhou 等[24]又基于四粒子 Cluster 态提出了一个三方半量子密钥协商协议。

本文基于三粒子 G-like 态，提出了一个两方半量子密钥协商协议。其中 Alice 和 Bob 是两个半量子方，他们需要在一个具备全量子能力的可信第三方 Charlie 的协助下才能进行密钥协商。并且我们证明了该 SQKA 协议可以很好地抵抗参与者攻击和外部攻击，同时该协议在性能方面也具有一定优势。

2 新的两方半量子密钥协商协议

2.1 基础知识

Bell 态是两粒子最大纠缠态。四个 Bell 态的定义为

$$\begin{cases} |\varphi^+\rangle=(|00\rangle+|11\rangle)/\sqrt{2} \\ |\varphi^-\rangle=(|00\rangle-|11\rangle)/\sqrt{2} \\ |\psi^+\rangle=(|01\rangle+|10\rangle)/\sqrt{2} \\ |\psi^-\rangle=(|01\rangle-|10\rangle)/\sqrt{2} \end{cases}。 \tag{1}$$

收稿日期：2021-10-18；**修回日期**：2021-11-18；**录用日期**：2021-12-13

基金项目：国家自然科学基金（61802302）、陕西省自然科学基础研究计划项目（2021JM-462）

通信作者：*122979357@qq.com

它们形成了 4 维 Hilbert 空间的一组完全正交基。

GHZ 态是三粒子最大纠缠态，它们形成了 8 维 Hilbert 空间的一组完全正交基。G-like 态也是三粒子纠缠态的一种。它是通过对单光子和 Bell 态进行纠缠和量子受控非门(C-NOT)操作来实现的。G-like 具有特殊的纠缠特性，且在现有的实验条件下更容易制备[25]。G-like 态的定义为

$$
\begin{aligned}
|G\rangle_{abc}=&\frac{1}{2}(|001\rangle+|010\rangle+|100\rangle+|111\rangle)_{abc}=\\
&\frac{1}{\sqrt{2}}(|0\rangle_c|\psi^+\rangle_{ab}+|1\rangle_c|\varphi^+\rangle_{ab})=\\
&\frac{1}{\sqrt{2}}(|0\rangle_b|\psi^+\rangle_{ac}+|1\rangle_b|\varphi^+\rangle_{ac})=\\
&\frac{1}{\sqrt{2}}(|0\rangle_a|\psi^+\rangle_{bc}+|1\rangle_a|\varphi^+\rangle_{bc}),
\end{aligned}\tag{2}
$$

式中：a，b，c 为 Alice，Bob，Charlie 手中的粒子。

2.2 新的两方半量子密钥协商协议

假设 Alice 和 Bob 想要协商一个共享密钥用于后续的通信。然而，Alice 和 Bob 是两个半量子方，即双方只能使用 Z 基($|0\rangle$、$|1\rangle$)进行量子态的制备和测量。因此，Alice 和 Bob 需要在一个具备全量子能力的可信第三方 Charlie 的协助下进行密钥协商。

首先 Alice 和 Bob 随机生成自己的私钥 $K_a=\{K_a^1,K_a^2,\cdots,K_a^{2n}\}$，$K_b=\{K_b^1,K_b^2,\cdots,K_b^{2n}\}$，其中 $K_a^{i'},K_b^{i'}\in\{0,1\}$，且 $i'=1,2,\cdots,2n$，n 为共享密钥的长度。协议步骤(图 1)如下。

1) Charlie 首先制备 $4n$ 个 G-like 态。然后，Charlie 将 $4n$ 个 G-like 态分为 3 个序列 S_a、S_b 和 S_c，其中序列 S_t (t=a，b，c)由 G-like 态中的所有 t 粒子组成。最后，Charlie 将序列 S_a 和 S_b 分别发送给 Alice 和 Bob，自己保留序列 S_c。

2) Alice 和 Bob 收到序列 S_a 和 S_b 之后，随机对序列中的粒子执行以下两种操作。

a)反射该粒子(CTRL)。

b)对该粒子进行 Z 基测量，并制备一个新的粒子(SIFT)。制备新粒子的规则如下。Alice 记录自己的测量结果，并将测量结果编码为序列 $R_a=\{R_a^1,R_a^2,\cdots,R_a^{2n}\}$，其中编码规则为 $|0\rangle\rightarrow0$，$|1\rangle\rightarrow1$。之后，Alice 利用公式 $D_a=R_a\oplus K_a$ 对 K_a 进行编码，得到序列 $D_a=\{D_a^1,D_a^2,\cdots,D_a^{2n}\}$。然后，Alice 根据序列 D_a 制备新的粒子序列 $Q_a=\{|q_a^1\rangle,|q_a^2\rangle,\cdots,|q_a^{2n}\rangle\}$，其中 $q_a^i=D_a^i$ ($i=0,1,2,\cdots,2n$)。Bob 采用相同的方法得到序列 $D_b=R_b\oplus K_b$，并用同样的方法得到粒子序列 Q_b。

最后，Alice 和 Bob 分别将 a)中反射的 $2n$ 个粒子和 b)中新制备的粒子随机组合得到新序列 S'_a 和 S'_b。最终，Alice 和 Bob 分别将序列 S'_a 和 S'_b 发送给 Charlie。

3)确定 Charlie 收到序列 S'_a 和 S'_b 之后，Alice 和 Bob 公布执行了 SIFT 操作的粒子位置。

4)根据 Alice 和 Bob 的操作，会出现以下四种情况。Charlie 根据不同的情况进行相应的操作。

i)如果 Alice 和 Bob 均对粒子执行了 CTRL 操作，那么 Charlie 对 Alice 和 Bob 以及自己的粒子执行三粒子联合测量，并根据式(2)计算错误率。如果错误率低于门限值则协议继续进行，否则，协议终止。

ii)如果 Alice 对粒子执行了 SIFT 操作，Bob 对相应的粒子执行了 CTRL 操作，那么 Charlie 对自己和 Bob 的粒子执行 Bell 测量，并根据式(2)计算错误率。如果错误率低于门限值则协议继续进行，否则，协议终止。

iii)如果 Alice 对粒子执行了 CTRL 操作，Bob 对相应的粒子执行了 SIFT 操作，那么 Charlie 对自己和 Alice 的粒子执行 Bell 测量，并根据式(2)计算错误率。如果错误率低于门限值则协议继续进行，否则，协议终止。

iv)如果 Alice 和 Bob 均对粒子执行了 SIFT 操作，那么 Charlie 保留 Alice 和 Bob 的粒子分别得到序列 Q'_a 和 Q'_b。

5)步骤 4)中所有窃听检测通过之后，Charlie 将步骤 a)中 Alice 和 Bob 反射的粒子分别随机插入序列 Q'_a 和 Q'_b，得到序列 S_a^* 和 S_b^*。然后 Charlie 将序列 S_b^* 发送给 Alice，将 S_a^* 发送给 Bob。

6)确认 Alice 和 Bob 分别收到序列 S_b^* 和 S_a^* 之后，Charlie 分别通知 Alice 和 Bob 插入粒子的位置。Alice 和 Bob 再将 Charlie 插入的粒子反射给 Charlie。

7)Charlie 结合 Alice 和 Bob 反射的粒子以及自己手中相应位置的粒子，进行三粒子联合测量，并根据式(2)计算错误率。如果错误率低于门限值则协议继续进行，否则，协议终止。

8)窃听检测通过之后，Charlie 对序列 S_c 进行 Z 基测量，得到序列 R_c 并公布。Alice 对序列 Q'_b 进行 Z 基测量，得到序列 D'_b。之后，Alice 基于式 2)，利用序列 R_a 和 R_c 得到序列 R_b，再结合序列 D'_b 得到 $K'_b=\{K_b^{1'},K_b^{2'},\cdots,K_b^{n'}\}$，Bob 利用同样的方法得到 $K'_a=\{K_a^{1'},K_a^{2'},\cdots,K_a^{n'}\}$。最终，Alice 和 Bob 可以得到共享密钥 $K=K'_a\oplus K'_b$。K'_a 和 K'_b 只有 n 比特，这是因为在步骤 4)中，步骤 i)、ii)、iii)中被执行 CTRL 操作的粒子用于窃听检测，只有步骤 iv)中的粒子可以用于密钥协商。同样，D'_a，Q'_a，D'_b 和 Q'_b 也都只有 n 比特。

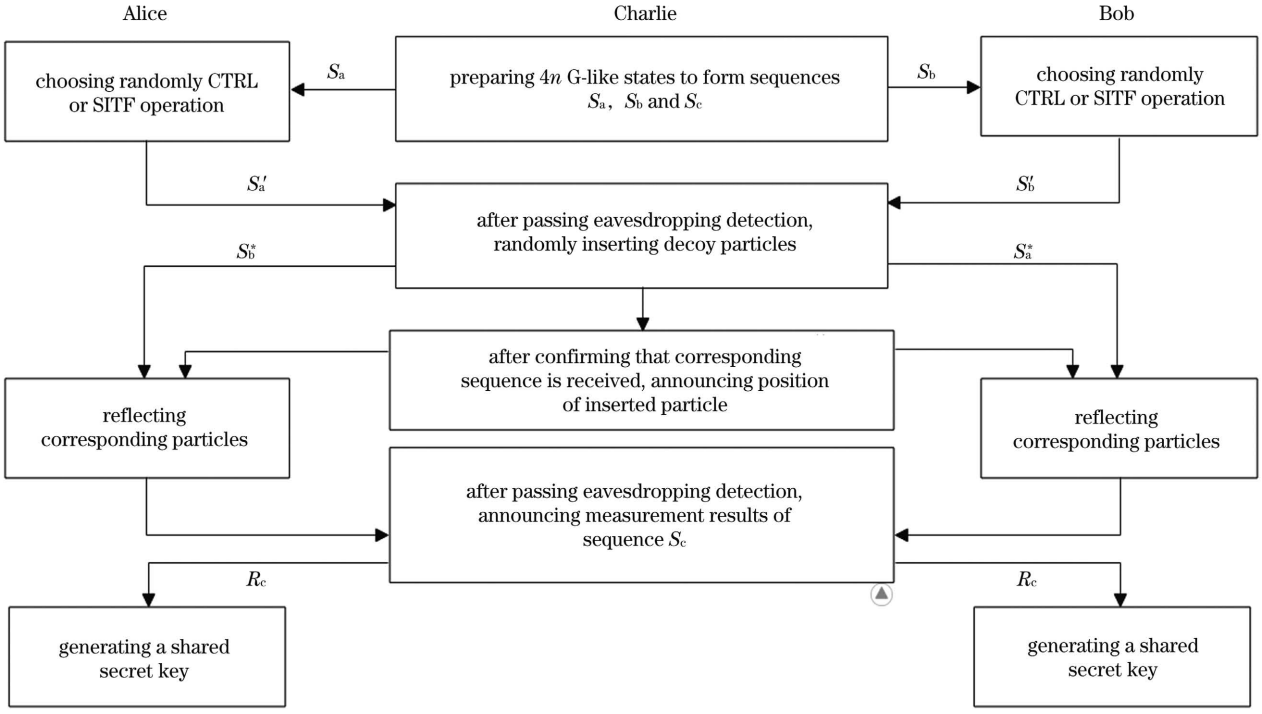

图 1 协议工作流程

Fig. 1 Working flow of proposed protocol

3 分析与讨论

3.1 安全性分析

一个安全的密钥协商协议必须能抵抗参与者攻击和外部攻击。下面从这两个方面分析该协议的安全性。

3.1.1 参与者攻击

在我们设计的 SQKA 协议中，共享密钥是由 Alice 和 Bob 在可信第三方 Charlie 的协助下生成的，其中每一个参与者对共享密钥做出的贡献是相等的。并且 Alice 和 Bob 任意一方都无法独自决定共享密钥。

假设 Alice 是一个不诚实的参与者，她试图独自决定该共享密钥。那么，Alice 需要在发送序列 S'_a 之前得到 K_b 才能实现该目的。然而，该协议中 Charlie 是一个可信第三方，在 Alice 将自己编码后的量子比特发送给 Charlie 之前，Alice 不会收到有关 K_b 的信息，即序列 S^*_b。同样，Bob 也无法通过这种手段独自决定该共享密钥。所以，双方都无法成功执行参与者攻击。

3.1.2 外部攻击

假设有一个攻击者 Eve，他试图窃取最终的共享密钥。Eve 只能通过对传输的量子序列 S'_a、S'_b、S^*_a 和 S^*_b 进行以下攻击来达到其目的。

特洛伊木马攻击。在本文协议中，信息粒子在信道中被传输了三次。为了抵御两种木马攻击[26-27]，可以引入波长量子滤波器（WQF）和光子数分离器（PNS）这两种光学设备。因此，该协议也可以抵御木马攻击。

截获-重发攻击。以 Eve 截获 Alice 发送给 Charlie 的序列为例。由于 Eve 并不知道被执行了 CTRL 操作的粒子的位置信息，他的操作会使 G-like 态粒子间的纠缠特性被破坏，因此 Eve 的攻击行为会在安全检测时被发现。

测量-重发攻击。以 Eve 对 Alice 发送给 Charlie 的粒子实施测量-重发攻击为例。同样，Eve 并不知道哪些粒子被执行了 CTRL 操作，他的操作会使粒子之间的纠缠特性被破坏。因此，Eve 伪造的序列无法通过安全检测。

纠缠-测量攻击。当 Eve 用准备的辅助粒子去纠缠传输粒子时，他执行 U 操作后可以得到以下状态：

$$U|G\rangle_{abc}|E\rangle=\frac{1}{2}\{|001\rangle_{abc}(|e_{0,0}\rangle+|e_{1,0}\rangle+|e_{2,0}\rangle+|e_{3,0}\rangle)+|010\rangle_{abc}(|e_{0,1}\rangle+|e_{1,1}\rangle+|e_{2,1}\rangle+|e_{3,1}\rangle)+$$
$$|100\rangle_{abc}(|e_{0,2}\rangle+|e_{1,2}\rangle+|e_{2,2}\rangle+|e_{3,2}\rangle)+|111\rangle_{abc}(|e_{0,3}\rangle+|e_{1,3}\rangle+|e_{2,3}\rangle+|e_{3,3}\rangle)\},\tag{3}$$

式中：$|e_{0,0}\rangle,\cdots,|e_{3,3}\rangle$ 为幺正变换 U 唯一确定的纯态。

Alice 和 Bob 用 Z 基测量他们的粒子只能得到两种结果 $|0\rangle$ 或者 $|1\rangle$。由于 G-like 态的测量相关性，Charlie 的测量结果会受到 Alice 和 Bob 测量结果的影响。根据文献[24,28]，我们可以推得 Alice 的测量结果为 $|0\rangle(|1\rangle)$ 时的概率为 $P_{A_0}(P_{A_1})$，以及 Charlie 的测量结果为 $|0\rangle(|1\rangle)$ 时的概率为 $P_{C_0}(P_{C_1})$。

$$P_{A_0}=\frac{1}{4}(\langle e_{0,0}\mid e_{0,0}\rangle+\langle e_{1,0}\mid e_{1,0}\rangle+\langle e_{2,0}\mid e_{2,0}\rangle+\langle e_{3,0}\mid e_{3,0}\rangle+\langle e_{0,1}\mid e_{0,1}\rangle+\langle e_{1,1}\mid e_{1,1}\rangle+\langle e_{2,1}\mid e_{2,1}\rangle+\langle e_{3,1}\mid e_{3,1}\rangle),\tag{4}$$

$$P_{A_1}=\frac{1}{4}(\langle e_{0,2}\mid e_{0,2}\rangle+\langle e_{1,2}\mid e_{1,2}\rangle+\langle e_{2,2}\mid e_{2,2}\rangle+\langle e_{3,2}\mid e_{3,2}\rangle+\langle e_{0,3}\mid e_{0,3}\rangle+\langle e_{1,3}\mid e_{1,3}\rangle+\langle e_{2,3}\mid e_{2,3}\rangle+\langle e_{3,3}\mid e_{3,3}\rangle),\tag{5}$$

$$P_{C_0}=\frac{1}{4}(\langle e_{0,1}\mid e_{0,1}\rangle+\langle e_{1,1}\mid e_{1,1}\rangle+\langle e_{2,1}\mid e_{2,1}\rangle+\langle e_{3,1}\mid e_{3,1}\rangle+\langle e_{0,2}\mid e_{0,2}\rangle+\langle e_{1,2}\mid e_{1,2}\rangle+\langle e_{2,2}\mid e_{2,2}\rangle+\langle e_{3,2}\mid e_{3,2}\rangle),\tag{6}$$

$$P_{C_1}=\frac{1}{4}(\langle e_{0,0}\mid e_{0,0}\rangle+\langle e_{1,0}\mid e_{1,0}\rangle+\langle e_{2,0}\mid e_{2,0}\rangle+\langle e_{3,0}\mid e_{3,0}\rangle+\langle e_{0,3}\mid e_{0,3}\rangle+\langle e_{1,3}\mid e_{1,3}\rangle+\langle e_{2,3}\mid e_{2,3}\rangle+\langle e_{3,3}\mid e_{3,3}\rangle)。\tag{7}$$

在错误率不超过门限值的情况下，P_{A_0} 和 P_{A_1} 近似相等，P_{C_0} 和 P_{C_1} 也近似相等。因此，Alice 系统(A)的 Shannon 熵为 $H(A)=h[(P_{A_0}+P_{A_1}),(P_{C_0}+P_{C_1})]=1$。由于 Charlie(C)可以通过测量自己手中的粒子得到 Alice 手中粒子的状态，因此条件熵 $H(A|C)=0$。现在，可以得到 Charlie 与 Alice 之间的互信息为 $I(C:A)=H(A)-H(A|C)=1$。

另外，Charlie 与 Eve(E)之间的互信息为 $I(C:E)$。当 Alice 和 Bob 均对相应粒子执行 CTRL 操作时，Charlie 的测量结果应该为 $|G\rangle_{abc}$，否则她将发现 Eve 的操作。如果 Eve 希望自己的操作不被发现，但是这样会导致 Charlie 与 Eve 之间的互信息 $I(C:E)=0$。因此 $I(C:A)>I(C:E)$，Eve 不能提取到任何与共享密钥有关的信息。

3.2 性能分析

QKA 协议用 Cabello 量子比特效率[29]来衡量它的性能。Cabello 量子比特效率定义为 $\eta=c/q$，其中，c 表示协商的共享密钥的比特长度，q 表示协议中用到的量子比特的数量。在该协议中，有 $c=n$，并且 $q=3\times4n+2\times4n+2n=22n$。因此，本协议的量子比特效率为 $\eta=4.5\%$。表 1 给出了我们的 SQKA 协议与已有安全的 SQKA 协议的比较。与 Shukla 的 SQKA 协议[22]相比，本文协议允许更多的半量子方进行密钥协商；与 Zhou 的 SQKA 协议[24]相比，本文协议在量子比特效率上有了一定程度的提高。

表 1 本文 SQKA 协议与其他 SQKA 协议的比较

Table 1 Comparison between SQKA protocol in this paper and other SQKA protocols

Protocol	Ratio of number of participants to number of classical participants	Quantum resource	Qubit efficiency /%
Shukla's SQKA protocol[22]	2/1	Bell states	9.09
Zhou's SQKA protocol[24]	3/2	Cluster states	2.08
Proposed SQKA protocol	2/2	G-like states	4.50

4 结 论

基于 G-like 态提出了一个两方半量子密钥协商协议。两个半量子方 Alice 和 Bob 在具备全量子能力的可信第三方 Charlie 的协助下协商了一个共享密钥。并且，双方的贡献是相等的，任意一方不能独自决定共享密钥的生成。安全性分析证明了新的 SQKA 协议可以抵抗内部攻击和所有外部攻击。最后，与已有安全的 SQKA 协议进行了比较，发现所提 SQKA 协议在性能方面也有一定优势。

参 考 文 献

[1] Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing[J]. Theoretical Computer Science, 2014, 560: 7-11.

[2] Kovalenko O, Ra Y S, Cai Y, et al. Frequency-multiplexed entanglement for continuous-variable quantum key distribution [J]. Photonics Research, 2021, 9(12): 12002351.

[3] Xue Y, Chen W, Wang S, et al. Airborne quantum key distribution: a review[J]. Chinese Optics Letters, 2021, 19(12): 122702.

[4] Zheng X D, Zhang P Y, Ge R Y, et al. Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution[J]. Advanced Photonics, 2021, 3(5): 055002.

[5] 何业锋, 赵艳坤, 李春雨, 等. 标记配对相干态下有限探测器死时间的测量设备无关量子密钥分配[J]. 光学学报, 2020, 40(24): 2427001.
He Y F, Zhao Y K, Li C Y, et al. Measurement-device-independent quantum key distribution of finite detector's dead time in heralded pair coherent state[J]. Acta Optica Sinica, 2020, 40(24): 2427001.

[6] 何业锋, 白倩, 李丽娜, 等. 基于多晶体指示源的测量设备无关量子密钥分配协议[J]. 光学学报, 2021, 41(16): 1627001.
He Y F, Bai Q, Li L N, et al. Measurement-device-independent quantum key distribution protocols based on multiple crystal heralded source[J]. Acta Optica Sinica, 2021, 41(16): 1627001.

[7] 何业锋, 李春雨, 郭佳瑞, 等. 基于标记配对相干态的被动测量设备无关量子密钥分配[J]. 中国激光, 2020, 47(9): 0912002.
He Y F, Li C Y, Guo J R, et al. Passive measurement-device-independent quantum key distribution based on heralded pair coherent states[J]. Chinese Journal of Lasers, 2020, 47(9): 0912002.
[8] He Y F, Ma W P. Quantum key agreement protocols with four-qubit cluster states[J]. Quantum Information Processing, 2015, 14(9): 3483-3498.
[9] Shukla C, Alam N, Pathak A. Protocols of quantum key agreement solely using Bell states and Bell measurement[J]. Quantum Information Processing, 2014, 13(11): 2391-2405.
[10] Huang W, Wen Q Y, Liu B, et al. Quantum key agreement with EPR pairs and single-particle measurements[J]. Quantum Information Processing, 2014, 13(3): 649-663.
[11] Liao Q, Liu H J, Zhu L J, et al. Quantum secret sharing using discretely modulated coherent states[J]. Physical Review A, 2021, 103(3): 032410.
[12] Wu X D, Wang Y J, Huang D. Passive continuous-variable quantum secret sharing using a thermal source[J]. Physical Review A, 2020, 101(2): 022301.
[13] Sun Z, Song L Y, Huang Q, et al. Toward practical quantum secure direct communication: a quantum-memory-free protocol and code design[J]. IEEE Transactions on Communications, 2020, 68(9): 5778-5792.
[14] Li T, Long G L. Quantum secure direct communication based on single-photon Bell-state measurement[J]. New Journal of Physics, 2020, 22(6): 063017.
[15] Zhou N, Zeng G, Xiong J. Quantum key agreement protocol [J]. Electronics Letters, 2004, 40(18): 1149-1150.
[16] Chong S K, Hwang T. Quantum key agreement protocol based on BB84[J]. Optics Communications, 2010, 283(6): 1192-1195.
[17] He Y F, Ma W P. Two quantum key agreement protocols immune to collective noise [J]. International Journal of Theoretical Physics, 2017, 56(2): 328-338.
[18] Shi R H, Zhong H. Multi-party quantum key agreement with Bell states and bell measurements[J]. Quantum Information Processing, 2013, 12(2): 921-932.
[19] Liu B, Gao F, Huang W, et al. Multiparty quantum key agreement with single particles [J]. Quantum Information Processing, 2013, 12(4): 1797-1805.
[20] Sun Z W, Zhang C, Wang B H, et al. Improvements on "multiparty quantum key agreement with single particles"[J]. Quantum Information Processing, 2013, 12(11): 3411-3420.
[21] He Y F, Ma W P. Two-party quantum key agreement against collective noise[J]. Quantum Information Processing, 2016, 15(12): 5023-5035.
[22] Shukla C, Thapliyal K, Pathak A. Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue[J]. Quantum Information Processing, 2017, 16(12): 295.
[23] Liu W J, Chen Z Y, Ji S, et al. Multi-party semi-quantum key agreement with delegating quantum computation [J]. International Journal of Theoretical Physics, 2017, 56(10): 3164-3174.
[24] Zhou N R, Zhu K N, Wang Y Q. Three-party semi-quantum key agreement protocol[J]. International Journal of Theoretical Physics, 2020, 59(3): 663-676.
[25] DiCarlo L, Reed M D, Sun L, et al. Preparation and measurement of three-qubit entanglement in a superconducting circuit[J]. Nature, 2010, 467(7315): 574-578.
[26] Cai Q Y. Eavesdropping on the two-way quantum communication protocols with invisible photons[J]. Physics Letters A, 2006, 351(1/2): 23-25.
[27] Deng F G, Li X H, Zhou H Y, et al. Improving the security of multiparty quantum secret sharing against Trojan horse attack [J]. Physical Review A, 2005, 72(4): 044302.
[28] Chen L Y, Gong L H, Zhou N R. Two semi-quantum key distribution protocols with G-like states [J]. International Journal of Theoretical Physics, 2020, 59(6): 1884-1896.
[29] Cabello A. Quantum key distribution in the Holevo limit[J]. Physical Review Letters, 2000, 85(26): 5635-5638.

Two-Party Semi-Quantum Key Agreement Protocol Based on G-Like States

He Yefeng, Pang Yibo*, Di Man, Yue Yuru, Li Guoqing, Liu Jixiang
School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, Shaanxi, China

Abstract

Objective With the continuous development of quantum calculations, the classic cryptosystem that relies on mathematical difficulties and computational complexity to ensure security is constantly under threat. Therefore, in recent years, a large number of scholars have attracted attention from the quantum cryptography produced by the combination of cryptography and quantum mechanics. At present, quantum cryptography has many branches, such as quantum key distribution, quantum key agreement, quantum secure sharing, quantum secure direct communication, and deterministic secure quantum communication. Among them, quantum key agreement is an important branch of quantum cryptography. In real life, quantum key agreement is widely used in scenarios such as end-to-end communication and internet of things. Although, in the current quantum key agreement protocol, a secure shared key can be established between legal participants. However, participants in the quantum key agreement protocol are required to have high capabilities and equipment. But, the quantum equipment is still too expensive even in relatively rich future material conditions. In order to cope with this situation, the semi-quantum key agreement protocol is proposed by scholars. It allows one or more participants in the protocol to only have simple quantum capabilities, that is, to use the Z basis ($|0\rangle$, $|1\rangle$) for preparation and measurement. Therefore, the protocol reduces the requirements for participant capabilities and equipment. In addition, research on semi-quantum key agreement is relatively small. Therefore, the semi-quantum key agreement needs to be studied by scholars.

Methods In this paper, a new two-party semi-quantum key agreement protocol is designed based on the G-like state.

The securely shared key in the protocol is established by the two classical parties, Alice and Bob, through the measurement-resending operation and the entanglement characteristics of the G-like state with the assistance of a trusted third party with full quantum capabilities, Charlie, and the contributions of both parties are equal. The shared key cannot be determined by any participants alone. The G-like state is a special three-particle entangled state, and its entanglement properties are used in the key agreement and eavesdropping detection part of the protocol. For example, the measurement result of the counterpart can be inferred by the participant through the entanglement properties of his own initial quantum state and the G-like state. And the measurement-resending operation means that the particles are randomly executed the CTRL and SIFT operations. Among them, the CTRL operation means that the particles are only executed to reflection operations, and the SIFT operation means that the particles are executed to the Z basic measurement and a new particle is prepared. Finally, the newly prepared particles are resent. In this protocol, the measurement-resending operation is performed twice by us. Therefore, the CTRL particles usually discarded in the previous protocol can be reused and the waste of quantum resources is reduced. In terms of security, the security of the protocol is guaranteed by the entanglement characteristics of the G-like state. In addition, two optical devices, wavelength quantum filter (WQF) and photon number separator (PNS), have been introduced, so that the protocol can also resist two Trojan horse attacks. In terms of qubit efficiency, the performance of the protocol is measured by Cabello qubit efficiency.

Results and Discussions Although most of the quantum key agreement protocols have been proposed to enable the secure keys to be established between participants. But all participants in these protocols are required to have full quantum capabilities. However, quantum devices are relatively expensive and difficult to carry. Therefore, the semi-quantum key agreement protocol is proposed to solve this problem. A trusted third party with full quantum capabilities is introduced, and thus the two-party semi-quantum key agreement protocol can be realized. The trusted third party can be used to prepare the G-like state required for this protocol. At the same time, it can also perform eavesdropping detection jointly with all participants. This ensures that the external attacks can be well resisted by the protocol, and in addition, the participant attacks can also be well resisted by the protocol. Since the quantum state in this protocol has been transmitted for many times, the attacker can eavesdrop on the information related to the shared key through a Trojan horse attack. Therefore, two optical devices, the wavelength quantum filter and the photon number separator, are introduced by us. Among them, the invisible photons can be filtered out by the wavelength quantum filter, and the delayed photons can be detected by the photon number separator. This ensures that the protocol can also resist two types of Trojan attacks. In terms of performance, Cabello qubit efficiency is used to measure the performance of the protocol. At present, this method is mainly used to evaluate the performance of the quantum key agreement protocol. The qubit efficiency of the semi-quantum key agreement protocol is generally low. But this kind of agreement has low requirements for participants. Therefore, the semi-quantum key agreement protocol is more suitable for our current situation.

Conclusions In this paper, a two-party semi-quantum key agreement protocol based on G-like state is proposed. A securely shared key can be established by two semi-quantum parties with the assistance of a trusted third party. In terms of security, participant attacks and external attacks can be well resisted. In addition, the protocol also has an advantage in performance.

Key words quantum optics; quantum cryptography; semi-quantum key agreement; G-like states; qubit efficiency