第 43 卷 第 20 期/2023 年 10 月/光学学报 研究论文

光学学报

基于四粒子cluster态的四方半量子密钥协商协议

何业锋，庞一博*，狄曼，岳玉茹，刘继祥，李国庆

西安邮电大学网络空间安全学院，陕西 西安 710121

摘要 为了满足多用户安全通信的需求，利用四粒子cluster态的纠缠特性和测量-重发操作提出一个四方半量子密钥协商协议。该协议能够使一个全量子方和三个半量子方在无可信第三方协助的情况下进行密钥协商，并公平地建立共享密钥。由于该协议的半量子方仅需执行简单量子态制备、测量和反射操作，因此该协议降低了对参与者能力和设备的要求。研究结果表明，该协议在有效地抵御参与者攻击和所有外部攻击的同时具备良好的性能。

关键词 量子光学；量子密码；半量子密钥协商；四粒子cluster态；量子比特效率

中图分类号 TN918 **文献标志码** A **DOI**：10.3788/AOS230828

1 引 言

量子密钥协商（QKA）协议[1-5]是一种基于量子信道的安全协议，它要求参与者之间可以通过协商建立一个安全的共享密钥，并且不允许任意部分参与者控制整个密钥的生成。与依靠数学困难问题来保证安全的经典密钥协商协议不同，QKA协议的安全性由量子力学的基本原理保证，可以达到无条件安全性，因此更符合实际需求。目前，在研究者的不懈努力下，QKA协议的研究迎来了蓬勃的发展并取得了许多优秀的研究成果[6-16]。

2004年，Zhou等[1]首次给出一个采用量子隐形传态设计的QKA协议。之后，Tsai和Hwang提出一个针对参与者攻击模型的QKA协议。2010年，Chong等[2]设计出一个安全的两方QKA协议。之后，学者们在此基础上设计出更多符合实际需要的QKA协议，如多方QKA协议[6-8]、免疫噪声的QKA协议[9-11]、可控QKA协议[12-13]以及互认证QKA协议[14-16]等。然而，上述协议只能用于参与者均具备全量子能力的情况，且某些量子设备是昂贵或不易携带的。为此，学者们提出了半量子密钥协商（SQKA）协议[17-23]，它是指其中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的协议。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，他们只需使用Z基$\{|0\rangle,|1\rangle\}$进行量子态的制备或测量。2017年，Shukla等[17]首次基于Bell态提出了一个两方半量子密钥协商协议。同年，Liu等[18]基于Bell态和委托量子计算提出一个多方半量子密钥协商协议。2022年，Xu等[21]基于多粒子GHZ态提出一个多方半量子密钥协商协议。然而，目前对多方SQKA协议的研究还较少，且存在依赖可信第三方或量子比特效率较低的情况。因此，对多方SQKA协议的研究是非常有必要的。

本文基于四粒子cluster态提出了一个四方半量子密钥协商协议。该协议中的全量子方Dave以及三个半量子方Alice、Bob和Charlie能够在无可信第三方协助的情况下进行密钥协商。并且，该协议可以在有效抵御参与者攻击和所有外部攻击的情况下具有较好的性能。

2 新的四方半量子密钥协商协议

2.1 基础知识

团簇态是由Briegel和Raussendorf[24]两位科学家提出的一种N粒子纠缠态，其具有很强的退相干能力，并且很容易被单向量子计算机处理。四粒子cluster态可以表示为

$$\begin{aligned}|\phi\rangle_{abcd}&=\frac{1}{2}\left(|0000\rangle+|0110\rangle+|1001\rangle-|1111\rangle\right)=\\&\frac{1}{\sqrt{2}}\left(|0\rangle_a|\varphi^+\rangle_{bc}|0\rangle_d+|1\rangle_a|\varphi^-\rangle_{bc}|1\rangle_d\right)=\\&\frac{1}{\sqrt{2}}\left(|0\rangle_b|\varphi^+\rangle_{ad}|0\rangle_c+|1\rangle_b|\varphi^-\rangle_{ad}|1\rangle_c\right)。\end{aligned}\tag{1}$$

2.2 新的四方半量子密钥协商协议

假设3个只能使用Z基对量子态进行制备和测量的半量子方Alice、Bob和Charlie以及一个全量子方

收稿日期：2023-04-17；**修回日期**：2023-04-28；**录用日期**：2023-05-19；**网络首发日期**：2023-06-28

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

Dave希望在公开量子信道上共同协商建立一个安全的共享密钥。为了实现这一目的，采用四粒子cluster态作为初始量子资源，设计了一个四方SQKA协议。该协议的工作流程如图1所示，具体步骤如下：

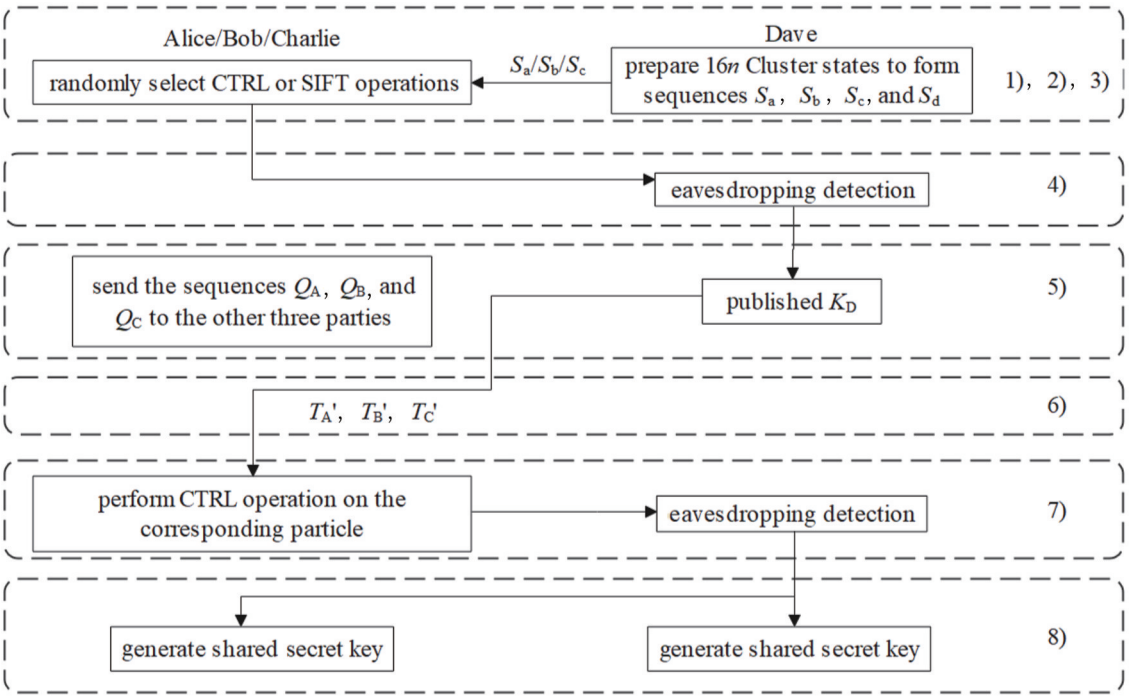

图1　SQKA协议工作流程

Fig. 1　Workflow of the proposed SQKA protocol

1）Alice、Bob、Charlie和Dave分别随机生成自己的初始密钥 $K_A=\{K_A^1,K_A^2,\cdots,K_A^n\}$、$K_B=\{K_B^1,K_B^2,\cdots,K_B^n\}$、$K_C=\{K_C^1,K_C^2,\cdots,K_C^n\}$ 和 $K_D=\{K_D^1,K_D^2,\cdots,K_D^n\}$，其中 K_A^i、K_B^i、K_C^i、$K_D^i\in\{0,1\}$，且 $i=1,2,\cdots,n$。

2）Dave制备16n个四粒子cluster态 $|\phi\rangle_{abcd}$，并将16n个四粒子cluster态 $|\phi\rangle_{abcd}$ 分成4个序列 S_a、S_b、S_c 和 S_d，其中序列 $S_t(t=a、b、c、d)$ 由cluster态中的所有 t 粒子组成。最后，Dave将序列 S_a、S_b 和 S_c 中的粒子一一发送给Alice、Bob和Charlie，以便能够进行后续通信。

3）Alice、Bob和Charlie收到序列 S_a、S_b 和 S_c 中的第 $j(j=1,2,\cdots,16n)$ 个粒子后，随机对接收到的粒子执行以下两种操作中的一种：

a）CTRL操作——反射该粒子；

b）SIFT操作——对接收到的第 j 个粒子进行Z基测量，并分别得到测量结果 M_A^j、M_B^j 和 M_C^j。之后根据测量结果制备相应的粒子并发送给Dave（新粒子的状态与原粒子相同）。注意，Alice、Bob和Charlie选择CTRL操作和SIFT操作的概率相等，并且Alice、Bob和Charlie最终分别得到经典比特序列 $M_A=\{M_A^1,M_A^2,\cdots,M_A^{8n}\}$、$M_B=\{M_B^1,M_B^2,\cdots,M_B^{8n}\}$ 和 $M_C=\{M_C^1,M_C^2,\cdots,M_C^{8n}\}$。

4）Alice、Bob和Charlie分别通知Dave执行了SITF操作的粒子的位置。之后，Dave根据Alice、Bob和Charlie的选择对接收的粒子执行不同的操作。

在Case Ⅰ中，Alice、Bob和Charlie均对粒子执行了CTRL操作。因此，Dave使用cluster基对来自Alice、Bob和Charlie的粒子进行测量，并根据式(1)计算错误率。如果错误率低于门限值，则继续执行协议；反之，则终止协议。

在Case Ⅱ中，Alice和Bob对粒子执行了CTRL操作，而Charlie对粒子执行了SIFT操作；在Case Ⅲ中，Alice和Charlie对粒子执行了CTRL操作，而Bob对粒子执行了SIFT操作；在Case Ⅳ中，Bob和Charlie对粒子执行了SIFT操作，而Alice对粒子执行了CTRL操作。对于以上3种情况，Dave利用Bell基对来自Alice的粒子以及自己手中的粒子进行测量，并根据式(1)计算错误率。如果错误率低于门限值，则协议继续进行；反之，协议将被终止。

在Case Ⅴ中，Bob和Charlie对粒子执行了CTRL操作，而Alice对粒子执行了SIFT操作。因此，Dave利用Bell基对来自Bob和Charlie的粒子进行检测，并根据式(1)计算错误率。如果错误率低于门限值，则协议继续执行；反之，协议将被终止。

在Case Ⅵ中，Alice和Charlie对粒子执行了SIFT操作，而Bob对粒子执行了CTRL操作。因此，Dave利用Z基对来自Bob的粒子进行测量，并记录测量所

得到的结果。同时，Alice 和 Charlie 告诉 Dave 自己得到的测量结果。最后，Dave 利用自己的测量结果以及 Alice 和 Charlie 的测量结果与式(1)进行对比来判断协议是否继续执行。如果错误率低于门限值，则协议继续执行；反之，协议将被终止。

在 Case Ⅶ 中，Alice 和 Bob 对粒子执行了 SIFT 操作，而 Charlie 对粒子执行了 CTRL 操作。因此，Dave 利用 Z 基对来自 Charlie 的粒子进行测量，并将测量得到的结果记录下来。同时，Alice 和 Bob 通知 Dave 自己对相应位置的粒子的测量结果。最后，Dave 利用自己的测量结果以及 Alice 和 Bob 的测量结果与式(1)进行对比来判断协议是否继续执行。如果错误率低于门限值，则协议继续执行；反之，协议将被终止。

5)在 Case Ⅷ 中，Alice、Bob 和 Charlie 均对粒子执行了 SIFT 操作。之后，Dave 分别选择其中一半的粒子利用 Z 基进行测量，并将所选粒子的位置信息通知 Alice、Bob 和 Charlie。然后他们将所选粒子的测量结果发送给 Dave。最后，Dave 将测量结果与式(1)进行对比。如果错误率低于门限值，则协议继续执行，否则，协议将被终止。窃听检测完成后，Alice、Bob、Charlie 和 Dave 利用剩下的 n 个粒子进行密钥协商。用于密钥协商的粒子被作为 INFO 粒子，并将 Alice、Bob 和 Charlie 的 INFO 粒子序列分别表示为 $M_{\mathrm{A_F}}=\left\{M_{\mathrm{A_F}}^1, M_{\mathrm{A_F}}^2, \cdots, M_{\mathrm{A_F}}^n\right\}$、$M_{\mathrm{B_F}}=\left\{M_{\mathrm{B_F}}^1, M_{\mathrm{B_F}}^2, \cdots, M_{\mathrm{B_F}}^n\right\}$ 和 $M_{\mathrm{C_F}}=\left\{M_{\mathrm{C_F}}^1, M_{\mathrm{C_F}}^2, \cdots, M_{\mathrm{C_F}}^n\right\}$。其中，序列 $M_{\mathrm{A_F}}$、$M_{\mathrm{B_F}}$、$M_{\mathrm{C_F}}$ 之间的关系满足式(1)。之后，Alice、Bob、和 Charlie 分别计算序列 $Q_{\mathrm{A}}=M_{\mathrm{A_F}}\oplus K_{\mathrm{A}}$、$Q_{\mathrm{B}}=M_{\mathrm{B_F}}\oplus K_{\mathrm{B}}$ 和 $Q_{\mathrm{C}}=M_{\mathrm{C_F}}\oplus K_{\mathrm{C}}$，其中序列 $Q_t=\left\{Q_t^1, Q_t^2, \cdots, Q_t^n\right\}$，$t=\mathrm{A}, \mathrm{B}, \mathrm{C}$。最后，Alice、Bob、Charlie 将计算得到的序列 Q_{A}、Q_{B}、Q_{C} 经过置换操作后发送给其他三方，而 Dave 公布 K_{D}。

6) Dave 首先利用 Z 基分别对 Alice、Bob 和 Charlie 的 INFO 粒子进行测量后得到序列 $M_{\mathrm{A_F}}$、$M_{\mathrm{B_F}}$、$M_{\mathrm{C_F}}$。之后，Dave 根据序列 $M_{\mathrm{A_F}}$、$M_{\mathrm{B_F}}$、$M_{\mathrm{C_F}}$ 的情况并按照表 1 的构造规则分别构造量子态序列 T_{A}、T_{B} 和 T_{C}，其中 $T_t=\left\{T_t^1, T_t^2, \cdots, T_t^n\right\}$，$t=\mathrm{A}, \mathrm{B}, \mathrm{C}$，$j=1, 2, \cdots, n$。然后，Dave 将第 4)步中 Case Ⅰ 中的粒子分成 3 份，并作为诱骗态随机插入序列 T_{A}、T_{B} 和 T_{C}，以此构建序列 T_{A}'、T_{B}' 和 T_{C}'。Dave 最终将序列 T_{A}'、T_{B}' 和 T_{C}' 分别发送给 Alice、Bob 和 Charlie，用于进一步执行协议。

表 1 构造规则

Table 1 Construct rules

$M_{\mathrm{A_F}}^j$	$M_{\mathrm{B_F}}^j$	$M_{\mathrm{C_F}}^j$	T_{A}^j	T_{B}^j	T_{C}^j
0	0	0	0	0	0
0	1	1	0	1	1
1	0	0	0	1	1
1	1	1	0	0	0

7) Alice、Bob 和 Charlie 分别收到序列 T_{A}'、T_{B}' 和 T_{C}' 后公布各自的置换操作。之后，Dave 公布诱骗态的位置。然后，Alice、Bob 和 Charlie 对所有的诱骗态执行 CTRL 操作。最后，Dave 对执行了 CTRL 操作的粒子利用 cluster 基进行测量，如果测量结果为 $\left|\phi\right\rangle_{\mathrm{abcd}}$，则协议继续，否则协议终止。

8)对于 Dave，在 Alice、Bob 和 Charlie 公布各自的置换操作之后，Dave 可以利用序列 $M_{\mathrm{A_F}}$、$M_{\mathrm{B_F}}$、$M_{\mathrm{C_F}}$ 以及序列 Q_{A}、Q_{B}、Q_{C} 分别得到 K_{A}、K_{B}、K_{C}；Alice 利用 Z 基对序列 T_{A} 进行测量，并结合序列 Q_{B}、Q_{C} 得到 $K_{\mathrm{B}}\oplus K_{\mathrm{C}}$；Bob 利用 Z 基对序列 T_{B} 进行测量，并结合序列 Q_{A}、Q_{C} 得到 $K_{\mathrm{A}}\oplus K_{\mathrm{C}}$；Charlie 利用 Z 基对序列 T_{C} 进行测量，并结合序列 Q_{A}、Q_{B} 得到 $K_{\mathrm{A}}\oplus K_{\mathrm{B}}$。最后，4 个参与者得到最终的共享密钥 $K_{\mathrm{F}}=K_{\mathrm{A}}\oplus K_{\mathrm{B}}\oplus K_{\mathrm{C}}\oplus K_{\mathrm{D}}$。

3 分析与讨论

3.1 安全性分析

经过分析，新的 SQKA 协议可以有效地抵御参与者攻击，以及特洛伊木马攻击、截获-重发攻击、测量-重发攻击、纠缠-测量攻击等外部攻击。因此，新协议是一个安全的 SQKA 协议。

3.1.1 参与者攻击

在新协议中，4 位参与者可以共同决定最终的共享密钥，并且任意一个或多个参与者都无法独自决定最终的共享密钥。

假设 Dave 是一个不诚实的参与者，他企图独自决定共享密钥，因此 Dave 必须在公布 K_{D} 之前获得 K_{A}、K_{B}、K_{C} 的信息。然而，在协议中 Dave 只有先公布 K_{D}，Alice、Bob 和 Charlie 才会公布自己的置换操作。所以，Dave 无法独自决定最终的共享密钥。

如果 Alice 是一名不诚信的参与者，她企图独自决定共享密钥，因此 Alice 必须先获得序列 K_{B}、K_{C}、K_{D}。然而，在协议中 Alice 发送序列 Q_{A} 之后 Dave 才会公布 K_{D}，并且 Alice 发送序列 Q_{A} 之后 Bob 和 Charlie 才公布相应的置换操作。因此，Alice 无法独自决定最终的共享密钥。同样，Bob 和 Charlie 也无法通过这种方法独自决定最终贡献密钥的生成。

如果 Alice 和 Dave 是两个不诚实的参与者，他们知道彼此的密钥信息，并且企图独自决定共享密钥。那么他们必须先获取序列 K_{B}、K_{C}。但是，Bob 和 Charlie 只有先获得序列 K_{D} 才会发送序列 Q_{B}、Q_{C}，并且 Alice 不知道 Bob 和 Charlie 执行的置换操作，也无法得到 K_{B}、K_{C}。因此，Alice 和 Dave 无法控制最终共享密钥的生成。同样，Bob 和 Dave 以及 Charlie 和 Dave 也无法独自控制最终共享密钥的生成。

如果 Alice 和 Bob 是两个不诚实的参与者，他们知道彼此的密钥信息，并且企图独自决定共享密钥。那么 Alice 和 Bob 需要在发送自己的密钥信息之前得到

K_C、K_D。然而，Dave只有在接收到携带K_A、K_B信息的序列Q_A、Q_B之后才会公布K_D，并且Alice和Bob不知道Charlie执行的置换操作，也无法得到K_C。因此，Alice和Bob无法控制最终共享密钥的生成。同样，Alice和Charlie以及Bob和Charlie也无法独自控制最终共享密钥的生成。

综上，所提SQKA协议可以抵御参与者攻击。

3.1.2 外部攻击

假设有一名恶意攻击者Eve，他企图利用自己的恶意手段来窃取共享密钥。通过分析得知，攻击者Eve可以得知Dave的初始密钥。如果攻击者Eve想要窃取共享密钥，他还需得知K_A、K_B和K_C的相关信息。因此，Eve可以利用特洛伊木马、截获-重发、测量-重发和纠缠-测量等技术来实现自己的目的。下面对这4种攻击进行分析。

1）特洛伊木马攻击。在新协议中，量子态序列被传输了两次。因此，攻击者Eve可以通过两种木马攻击[25-26]来窃取K_A、K_B和K_C的相关信息。但是，参与者可以利用波长量子滤波器（WQF）和光子数分离器（PNS）这两种光学设备来抵御特洛伊木马攻击。因此，所提SQKA协议可以有效地抵御特洛伊木马攻击。

2）截获-重发攻击。Eve通过截获传输中的序列，再伪造一段序列发送给接收者，以实现截获-重发攻击。以Case Ⅰ为例，攻击者Eve可以截取Alice、Bob和Charlie发送给Dave的量子态序列并替换成自己伪造的序列，然后将其发送给Dave，以此来实现其目的。然而，攻击者Eve并不知道哪些粒子被Alice、Bob和Charlie执行了CTRL操作，所以攻击者Eve的恶意操作会被Dave在安全检查中发现。因此，所提SQKA协议可以抵御截获-重发攻击。

3）测量-重发攻击。测量-重发攻击是指攻击者Eve截取传输中的粒子，在对被截取的粒子利用Z基进行测量之后重新发送给相应的接收者。以Case Ⅰ为例，假设攻击者Eve截获Alice、Bob和Charlie发送给Dave的量子态序列，并对截获的量子态序列利用Z基进行测量。然而，攻击者Eve不知道哪些粒子被他们执行了CTRL操作，所以攻击者Eve的恶意操作一定会被Dave发现。因此，所提SQKA协议可以抵御测量-重发攻击。

4）纠缠-测量攻击。攻击者Eve对四粒子cluster态以及自己的辅助粒子$|E\rangle$执行纠缠操作U，其结果为

$$\begin{aligned}U|\phi\rangle_{abcd}|E\rangle=&\frac{1}{2}\Big[|0000\rangle_{abcd}\big(|e_{0,0}\rangle+|e_{1,0}\rangle+|e_{2,0}\rangle+|e_{3,0}\rangle\big)+\\&|0110\rangle_{abcd}\big(|e_{0,1}\rangle+|e_{1,1}\rangle+|e_{2,1}\rangle+|e_{3,1}\rangle\big)+\\&|1001\rangle_{abcd}\big(|e_{0,2}\rangle+|e_{1,2}\rangle+|e_{2,2}\rangle+|e_{3,2}\rangle\big)+\\&|1111\rangle_{abcd}\big(|e_{0,3}\rangle+|e_{1,3}\rangle+|e_{2,3}\rangle+|e_{3,3}\rangle\big)\Big]。\end{aligned}\tag{2}$$

因为在新协议中，只有Case Ⅷ中的粒子携带有用的信息，所以接下来只对Case Ⅷ中的粒子进行分析。在Case Ⅷ中，Alice、Bob和Charlie均对手中的粒子利用Z基进行测量，并且他们得到的测量结果为$|0\rangle$或$|1\rangle$。因此，可以得到Alice-Bob-Charlie-Dave-Eve的混合系统为

$$\begin{aligned}\rho_{ABCDE}=&\frac{1}{4}\Big[|0\rangle_A\langle 0|\otimes|0\rangle_B\langle 0|\otimes|0\rangle_C\langle 0|\otimes|0\rangle_D\langle 0|\big(|e_{0,0}\rangle\langle e_{0,0}|+|e_{1,0}\rangle\langle e_{1,0}|+|e_{2,0}\rangle\langle e_{2,0}|+|e_{3,0}\rangle\langle e_{3,0}|\big)+\\&|0\rangle_A\langle 0|\otimes|1\rangle_B\langle 1|\otimes|1\rangle_C\langle 1|\otimes|0\rangle_D\langle 0|\big(|e_{0,1}\rangle\langle e_{0,1}|+|e_{1,1}\rangle\langle e_{1,1}|+|e_{2,1}\rangle\langle e_{2,1}|+|e_{3,1}\rangle\langle e_{3,1}|\big)+\\&|1\rangle_A\langle 1|\otimes|0\rangle_B\langle 0|\otimes|0\rangle_C\langle 0|\otimes|1\rangle_D\langle 1|\big(|e_{0,2}\rangle\langle e_{0,2}|+|e_{1,2}\rangle\langle e_{1,2}|+|e_{2,2}\rangle\langle e_{2,2}|+|e_{3,2}\rangle\langle e_{3,2}|\big)+\\&|1\rangle_A\langle 1|\otimes|1\rangle_B\langle 1|\otimes|1\rangle_C\langle 1|\otimes|1\rangle_D\langle 1|\big(|e_{0,3}\rangle\langle e_{0,3}|+|e_{1,3}\rangle\langle e_{1,3}|+|e_{2,3}\rangle\langle e_{2,3}|+|e_{3,3}\rangle\langle e_{3,3}|\big)\Big]。\end{aligned}\tag{3}$$

根据文献[27-28]可以推得Alice、Bob、Charlie和Dave的测量结果为$|0\rangle$或$|1\rangle$的概率：

$$P_{A_0}=P_{D_0}=\frac{1}{4}\big(\langle e_{0,0}|e_{0,0}\rangle+\langle e_{1,0}|e_{1,0}\rangle+\langle e_{2,0}|e_{2,0}\rangle+\langle e_{3,0}|e_{3,0}\rangle+\langle e_{0,1}|e_{0,1}\rangle+\langle e_{1,1}|e_{1,1}\rangle+\langle e_{2,1}|e_{2,1}\rangle+\langle e_{3,1}|e_{3,1}\rangle\big),\tag{4}$$

$$P_{A_1}=P_{D_1}=\frac{1}{4}\big(\langle e_{0,2}|e_{0,2}\rangle+\langle e_{1,2}|e_{1,2}\rangle+\langle e_{2,2}|e_{2,2}\rangle+\langle e_{3,2}|e_{3,2}\rangle+\langle e_{0,3}|e_{0,3}\rangle+\langle e_{1,3}|e_{1,3}\rangle+\langle e_{2,3}|e_{2,3}\rangle+\langle e_{3,3}|e_{3,3}\rangle\big),\tag{5}$$

$$P_{B_0}=P_{C_0}=\frac{1}{4}\big(\langle e_{0,0}|e_{0,0}\rangle+\langle e_{1,0}|e_{1,0}\rangle+\langle e_{2,0}|e_{2,0}\rangle+\langle e_{3,0}|e_{3,0}\rangle+\langle e_{0,2}|e_{0,2}\rangle+\langle e_{1,2}|e_{1,2}\rangle+\langle e_{2,2}|e_{2,2}\rangle+\langle e_{3,2}|e_{3,2}\rangle\big),\tag{6}$$

$$P_{B_1}=P_{C_1}=\frac{1}{4}\big(\langle e_{0,1}|e_{0,1}\rangle+\langle e_{1,1}|e_{1,1}\rangle+\langle e_{2,1}|e_{2,1}\rangle+\langle e_{3,1}|e_{3,1}\rangle+\langle e_{0,3}|e_{0,3}\rangle+\langle e_{1,3}|e_{1,3}\rangle+\langle e_{2,3}|e_{2,3}\rangle+\langle e_{3,3}|e_{3,3}\rangle\big)。\tag{7}$$

在不存在窃听且粒子数较多的情况下，Alice系统的香农熵$H(A)$为：$H(A)=h(P_{A_0},P_{A_1})=1$。由于Dave可以通过测量自己的粒子来推得Alice粒子的状态，因此条件熵$H(A|D)=0$，且Alice和Dave之间的互信息为：$I(D:A)=H(A)-H(A|D)=1$。

此外，攻击者Eve和Dave之间的互信息为$I(D:$

E)。当Alice、Bob和Charlie均对相应粒子执行CTRL操作时，Dave的测量结果应为$|\phi\rangle_{abcd}$，即Dave必须使

$$\left(|e_{0,0}\rangle\langle e_{0,0}|+|e_{1,0}\rangle\langle e_{1,0}|+|e_{2,0}\rangle\langle e_{2,0}|+|e_{3,0}\rangle\langle e_{3,0}|\right)=\left(|e_{0,1}\rangle\langle e_{0,1}|+|e_{1,1}\rangle\langle e_{1,1}|+|e_{2,1}\rangle\langle e_{2,1}|+|e_{3,1}\rangle\langle e_{3,1}|\right)=$$
$$\left(|e_{0,2}\rangle\langle e_{0,2}|+|e_{1,2}\rangle\langle e_{1,2}|+|e_{2,2}\rangle\langle e_{2,2}|+|e_{3,2}\rangle\langle e_{3,2}|\right)=\left(|e_{0,3}\rangle\langle e_{0,3}|+|e_{1,3}\rangle\langle e_{1,3}|+|e_{2,3}\rangle\langle e_{2,3}|+|e_{3,3}\rangle\langle e_{3,3}|\right),\quad(8)$$

否则他将发现Eve的操作，但是这样会导致Dave与Eve之间的互信息$I(\mathrm{D}:\mathrm{E})=0$。因此，$I(\mathrm{D}:\mathrm{A})>I(\mathrm{D}:\mathrm{E})$。可见，Eve不能利用纠缠-测量攻击获得任何有价值的信息。

根据文献[29-30]，噪声引起的量子误码率在2%～8.9%范围内。因此，可以通过选择合适的门限值(一般为0.1～0.2)，使所提出的SQKA协议在量子噪声信道中也是安全的。

3.2　性能分析

Cabello[31]指出，QKA协议的量子比特效率为$\eta=c/q$，其中c表示协商的共享密钥的比特长度，q表示协议中使用的量子比特数量。在所提协议中$c=n$，并且$q=4\times16n=64n$。因此，新协议的量子比特效率为$\eta=1.6\%$。表2给出了所提SQKA协议与已有安全的多方SQKA协议的比较，可以看到：与Liu等[18]提出的SQKA协议相比，所提SQKA协议的密钥协商过程无需可信第三方的参与；与Xu等[21]提出的SQKA协议相比，所提SQKA协议在量子比特效率方面有所改善。根据协议的具体步骤，所提SQKA协议在窃听检测过程中充分使用了协议中具有纠缠特性的量子态，因此该协议节省了所使用的量子资源。例如，在3.2节的步骤6)中使用了Case Ⅰ中的量子态。

表2　所提SQKA协议与其他SQKA协议的比较

Table 2　Comparison between proposed SQKA protocol and other SQKA protocols

Ref.	Number of participants/classical participants	Whether a trusted third party is required	Qubit efficiency
[18]	N/N	Yes	$\eta=1/(10N-8)$
[21]	$N/N-1$	No	$\eta=\eta/\left[n2^{N-1}(3N-1)+mN+nN\right]$
Proposed protocol	4/3	No	1.6%

4　结　　论

提出一个基于四粒子cluster态的四方SQKA协议。该协议无需可信第三方协助，就可以确保一个全量子方与三个半量子方之间通过协商建立一个安全共享密钥，并且各方对共享密钥的贡献是相等的。经过分析可知，所提SQKA协议能够有效地抵御内部攻击和所有外部攻击，不但在性能方面有所改善，而且还能节约量子资源。

参　考　文　献

[1] Zhou N, Zeng G, Xiong J. Quantum key agreement protocol[J]. Electronics Letters, 2004, 40(18): 1149-1150.

[2] Chong S K, Hwang T. Quantum key agreement protocol based on BB84[J]. Optics Communications, 2010, 283(6): 1192-1195.

[3] He Y F, Ma W P. Quantum key agreement protocols with four-qubit cluster states[J]. Quantum Information Processing, 2015, 14(9): 3483-3498.

[4] 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.

[5] 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.

[6] Gu J, Hwang T. Improvement of "novel multiparty quantum key agreement protocol with GHZ states"[J]. International Journal of Theoretical Physics, 2017, 56(10): 3108-3116.

[7] Sun Z W, Zhang C, Wang P, et al. Multi-party quantum key agreement by an entangled six-qubit state[J]. International Journal of Theoretical Physics, 2016, 55(3): 1920-1929.

[8] Sun Z W, Huang J W, Wang P. Efficient multiparty quantum key agreement protocol based on commutative encryption[J]. Quantum Information Processing, 2016, 15(5): 2101-2111.

[9] He Y F, Ma W P. Two-party quantum key agreement against collective noise[J]. Quantum Information Processing, 2016, 15(12): 5023-5035.

[10] 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.

[11] Zhou Y H, Xu Y, Yang Y G, et al. Measurement-device-independent quantum key agreement against collective noisy channel[J]. International Journal of Theoretical Physics, 2022, 61(7): 201.

[12] Tang J E, Shi L, Wei J H. Controlled quantum key agreement based on maximally three-qubit entangled states[J]. Modern Physics Letters B, 2020, 34(18): 2050201.

[13] He Y F, Yue Y R, Li G Q, et al. New controlled quantum key agreement protocols based on Bell states[J]. Journal of China Universities of Posts and Telecommunications, 2022, 29(4): 42-50.

[14] Xu Y G, Wang C N, Cheng K F, et al. A novel three-party mutual authentication quantum key agreement protocol with GHZ states[J]. International Journal of Theoretical Physics, 2022, 61(10): 245.

[15] He Y F, Yue Y R, Di M, et al. Two-party mutual

authentication quantum key agreement protocol[J]. International Journal of Theoretical Physics, 2022, 61(5): 145.
[16] He Y F, Pang Y B, Di M. Mutual authentication quantum key agreement protocol based on Bell states[J]. Quantum Information Processing, 2022, 21(8): 290.
[17] 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.
[18] 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.
[19] Yan L L, Zhang S B, Chang Y, et al. Semi-quantum key agreement and private comparison protocols using bell states[J]. International Journal of Theoretical Physics, 2019, 58(11): 3852-3862.
[20] 何业锋, 庞一博, 狄曼, 等. 基于G-like态的两方半量子密钥协商协议[J]. 中国激光, 2022, 49(13): 1312001.
He Y F, Pang Y B, Di M, et al. Two-party semi-quantum key agreement protocol based on G-like state[J]. Chinese Journal of Lasers, 2022, 49(13): 1312001.
[21] Xu T J, Chen Y, Geng M J, et al. Single-state multi-party semiquantum key agreement protocol based on multi-particle GHZ entangled states[J]. Quantum Information Processing, 2022, 21(7): 266.
[22] Liu C, Cheng S, Li H H, et al. New semi-quantum key agreement protocol based on the χ-type entanglement states[J]. International Journal of Theoretical Physics, 2022, 61(3): 60.
[23] Zhou N R, Liao Q, Zou X F. Multi-party semi-quantum key agreement protocol based on the four-qubit cluster states[J]. International Journal of Theoretical Physics, 2022, 61(4): 114.
[24] Briegel H J, Raussendorf R. Persistent entanglement in arrays of interacting particles[J]. Physical Review Letters, 2001, 86(5): 910-913.
[25] Cai Q Y. Eavesdropping on the two-way quantum communication protocols with invisible photons[J]. Physics Letters A, 2006, 351(1/2): 23-25.
[26] 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.
[27] 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.
[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] Lin J, Hwang T. New circular quantum secret sharing for remote agents[J]. Quantum Information Processing, 2013, 12(1): 685-697.
[30] He Y F, Ma W P. Two-party quantum key agreement based on four-particle GHZ states[J]. International Journal of Quantum Information, 2016, 14(1): 1650007.
[31] Cabello A. Quantum key distribution in the Holevo limit[J]. Physical Review Letters, 2000, 85(26): 5635-5638.

Four-Party Semi-Quantum Key Agreement Protocol Based on Four-Particle Cluster States

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

Abstract

Objective Quantum cryptography is a new research field emerging from the combination of cryptography and quantum mechanics. Furthermore, the basic principles of quantum mechanics guarantee its security, such as Heisenberg's inaccuracy principle and the unclonability principle which are different from classical ciphers. Therefore, quantum cryptography is theoretically capable of achieving unconditional security. Recently, with the continuous development of quantum cryptography, its related research has received wide attention. Meanwhile, the quantum key agreement is an important branch of quantum cryptography and a quantum channel-based security protocol that calls for a secure shared key able to be negotiated between participants and does not allow any part of the participants to control the generation of this key. Unlike classical key agreement protocols relying on mathematical hard problems to guarantee security, the security of quantum key agreement protocols is guaranteed by the basic principles of quantum mechanics and can achieve unconditional security, thus better meeting practical needs. However, general quantum key agreement protocols can only satisfy the cases where all participants have full quantum capabilities. Thus, semi-quantum key agreements have been proposed by scholars, which means that one participant in the protocol has full quantum capability while the other participants have only semi-quantum capability. In this case, some of the large institutions or companies are treated as entities with full quantum capabilities, while some ordinary users are treated as entities with semi-quantum capabilities who only need to employ the Z-base $\{|0\rangle,|1\rangle\}$ for quantum state preparation or measurement. However, there are still few studies on multi-party semi-quantum key agreement protocols, with cases of reliance on trusted third parties or low efficiency of quantum bits. Therefore, the multi-party semi-quantum key agreement protocol is significant to be studied.

Methods We design a new four-party semi-quantum key protocol based on a four-particle cluster state. Furthermore, the

secure shared key in this protocol is established by one full-quantum party of Dave, and three semi-quantum parties including Alice, Bob, and Charlie through measurement-resend operations and the entanglement properties of the four-particle cluster state, without the assistance of a trusted third party. The four-particle cluster state is a particular sort of four-particle entangled state whose entanglement properties are adopted in the key agreement and eavesdropping detection parts of the protocol. In this protocol, the measurement-resend operation is performed several times. Finally, since CTRL particles that are normally discarded in a previous protocol can be employed again, the quantum resource waste is reduced. In terms of security, the protocol is proven to be effective against internal attacks and all external attacks. Additionally, two optical devices, the wavelength quantum filter (WQF), and the photon number separator (PNS) are introduced in the protocol, which allows both Trojan horse attacks to be effectively defended against. In terms of qubit efficiency, the protocol performance is measured by Cabello qubit efficiency.

Results and Discussions Firstly, general quantum key agreement protocols can achieve the purpose of shared keys securely established between participants. However, in the existing quantum key agreement protocols, participants are required to have excessive capabilities and equipment. Therefore, we put forward a new four-party semi-quantum key negotiation protocol based on a four-particle cluster state. The three semi-quantum participants of Alice, Bob, and Charlie, and one participant Dave with full quantum capability in this protocol can perform key negotiation without any third party. As a consequence, the requirements for participant capacity and equipment in this protocol are reduced. The four-particle cluster state is utilized in the protocol for key agreement and eavesdropping detection. Secondly, the measurement-resend operation is leveraged in the protocol, which means that the particle is randomly executed with a CTRL or SIFT operation. In this case, the CTRL operation means that the particle is subjected to a reflection operation, the SIFT operation means that the particle is subjected to a Z-base measurement with the preparation of a new particle, and finally the newly prepared particle is resent. Furthermore, the measurement-resend operation is performed twice in the protocol to make the CTRL particles normally discarded in the previous protocol can be reused, Therefore, the quantum resource waste is reduced. Thirdly, the protocol is verified to be effective against both external and internal attacks through security analysis. Meanwhile, the protocol shows superior performance through performance analysis.

Conclusions Our paper proposes a four-party semi-quantum key agreement protocol based on a four-particle cluster state. In this protocol, no assistance from trusted third parties is required to ensure that a secure shared key is established by negotiation between a full quantum party and three semi-quantum parties and that the contributions of each party to the shared key are equal. Analysis indicates that internal attacks and all external attacks can be effectively defended by the new semi-quantum key agreement protocol. The final comparison results show that the proposed semi-quantum key agreement protocol can improve performance and save quantum resources simultaneously.

Key words quantum optics; quantum cryptography; semi-quantum key agreement; four-particle cluster states; qubit efficiency