激光与光电子学进展

基于四粒子团簇态的量子密钥协商协议

何业锋，李智*，杨梦玫
西安邮电大学网络空间安全学院，陕西 西安 710121

摘要 由于量子力学独特的性质，量子密钥协商理论上具有无条件安全性。设计了一个以四粒子团簇态为量子信源，通信双方分别进行联合Bell测量，并通过受控非门与Hadamard门进行编码操作，从而共享密钥的量子密钥协商协议。为应对传输过程中的退相干性，还使用了弱测量和量子测量翻转的方法。本文提出的密钥协商协议不仅具有应对各种参与者攻击与外部攻击的能力，还具有更高的通信效率。

关键词 量子密码；量子密钥协商；四粒子团簇态；Bell测量；量子比特效率
中图分类号 TN918 **文献标志码** A **DOI**：10.3788/LOP222701

Quantum Key Agreement Protocol Based on Four-Particle Cluster States

He Yefeng, Li Zhi*, Yang Mengmei
School of Cyberspace Security, Xi'an University of Posts & Telecommunications, Xi'an 710121, *Shaanxi, China*

Abstract Owing to the unique properties of quantum mechanics, the quantum key agreement has unconditional security in theory. In this paper, a quantum key agreement protocol is designed. The four-particle cluster states are used as quantum sources. Two communication parties conduct joint Bell measurements respectively, and code through the controlled NOT gate and Hadamard gate to achieve shared secret. Here, weak measurement and quantum measurement reversal methods are used to deal with decoherence during transmission. The proposed key agreement protocol not only has the ability to respond to various participant and external attacks but also has higher communication efficiency.

Key words quantum cryptography; quantum key agreement; four-particle cluster states; Bell measurement; quantum bit efficiency

1 引 言

随着社会的发展，各种各样的信息攻击手段也接踵而至，人们越发重视通信过程中的安全性。密码学是信息安全的基础理论，作为密码学一个重要分支的密钥协商(KA)也受到了人们的关注与研究。1976年，Diffie和Hellman[1]提出了第一个密钥协商协议。随后，人们陆续提出了许多密钥协商协议，它们的安全性主要基于计算复杂度假设。然而，随着计算能力的快速发展，尤其是量子计算机的问世和量子搜索算法[2-3]的提出，传统密码学的安全性受到了严峻的挑战。与经典的密钥协商协议相比，基于量子力学基本原理的量子密钥协商(QKA)协议在安全性上有着明显的优势，这是因为它在理论上能实现无条件安全性。近年来，随着量子技术[4]的逐渐发展和成熟，量子密钥协商[5]也不断吸引着人们的研究热情。2004年，Zhou等[6]利用量子隐形传态技术提出了一个两方QKA协议。2010年，Chong和Hwang[7]在BB84协议的基础上，利用延迟测量技术提出了一个成功的QKA协议，该协议被证明是一个公平的QKA协议，面对外部攻击和内部攻击时都是安全的。2013年，Shi和Zhong[8]提出了一个基于Bell态和Bell测量的多方密钥协商协议。在这之后，研究者们在设计量子密钥协商协议时使用了更多不同的量子态。2014年，Xu等[9]提出了一个基于GHZ态的量子密钥协商协议。2019年Yang等[10]提出了一个基于团簇态的量子密钥协商协议。后来，为了确保那些不具备强量子计算能力的参与者能进行量子密钥协商，研究者提出了半量子密钥协商协议[11-13]。然而，大部分QKA协议都是在理想的环境下设计的。实际上，量子比特在通过量子信道传输的过

收稿日期：2022-10-08；**修回日期**：2022-11-09；**录用日期**：2022-11-16；**网络首发日期**：2022-11-26
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：*2213886909@qq.com

程中，不可避免地受到了信道噪声的影响。为了解决噪声的影响，人们在设计量子直接通信[14-15]（QSDC）协议时，主要采用了构造无消相干子空间[16-18]（DFS）的方法。因为无消相干子空间中的逻辑量子态几乎不受集体噪声的影响。2014 年，Huang 等[19]基于 EPR 对和单粒子测量提出了一个两方 QKA 协议，并利用逻辑量子态使其在噪声信道上实现。随后，He 等[20-21]也利用逻辑量子态，设计了几个免疫集体噪声的 QKA 协议。然而，在使用无消相干子空间时，需要庞大的希尔伯特空间[22]。在不增加希尔伯特空间的情况下可以使用弱测量和量子翻转测量的方法抑制退相干。

不同于比特翻转信道和相位翻转信道等全局噪声信道，振幅阻尼信道仅会使部分$|1\rangle$态转变为$|0\rangle$态。为应对振幅阻尼信道对量子态的退相干性，本文设计了一个基于四粒子团簇态的两方量子密钥协商协议。通信双方分别进行联合 Bell 测量，并利用受控非门与 Hadamard 门进行编码。通过弱测量和量子测量翻转的方法使新协议可以在振幅阻尼信道中抵抗退相干性。而且协议可以抵抗各种内部攻击与外部攻击。最后，还计算了新协议的量子比特效率。

2　预备知识

2.1　叠加与测量基

$|0\rangle$和$|1\rangle$是二维 Hilbert 空间的两个基本量子比特，$\alpha|0\rangle+\beta|1\rangle$表示它们的叠加态，并且处于状态$|0\rangle$的概率为$|\alpha|^2$，处于状态$|1\rangle$的概率为$|\beta|^2$，其中$|\alpha|^2+|\beta|^2=1$。对量子态进行测量，可以使用 Z 基$\{|0\rangle,|1\rangle\}$或 X 基$\{|+\rangle,|-\rangle\}$，这两种测量基的关系可以表示为$|+\rangle=1/\sqrt{2}\,(|0\rangle+|1\rangle)$，$|-\rangle=1/\sqrt{2}\,(|0\rangle-|1\rangle)$。

2.2　纠缠态与 Bell 测量

量子纠缠是量子力学中十分重要的一个性质，满足纠缠的情况下，一个粒子的行为将会影响到与其纠缠的其他粒子的状态。双粒子的最大纠缠态为 Bell 态，它们可以表示为$|\phi^{\pm}\rangle_{AB}=1/\sqrt{2}\,(|00\rangle\pm|11\rangle)_{AB}$，$|\varphi^{\pm}\rangle_{AB}=1/\sqrt{2}\,(|01\rangle\pm|10\rangle)_{AB}$。

本文中所使用的四粒子团簇态也是纠缠态的一种，它可以表示为$|\Psi\rangle_{ABCD}=1/2\,(|0000\rangle+|0011\rangle+|1100\rangle-|1111\rangle)_{ABCD}$。相比于 Bell 态，团簇态具有最大连通性、持续纠缠性以及可以抵抗量子比特损失等优良性质。如果对该四粒子团簇态 A、C 与 B、D 位粒子分别进行联合 Bell 态测量，可以得到如下结果：

$$
\begin{aligned}
|\Psi\rangle_{ABCD}=&1/2\,(|0000\rangle+|0011\rangle+|1100\rangle-|1111\rangle)_{ABCD}=\\
&1/2\big(|\phi^+\rangle_{AC}|\phi^-\rangle_{BD}+|\phi^-\rangle_{AC}|\phi^+\rangle_{BD}+\\
&|\varphi^+\rangle_{AC}|\varphi^+\rangle_{BD}+|\varphi^-\rangle_{AC}|\varphi^-\rangle_{BD}\big)。
\end{aligned}\tag{1}
$$

从式(1)可以看出，测量可以得到 4 个可能的结果，分别为$|\phi^+\rangle_{AC}|\phi^-\rangle_{BD}$、$|\phi^-\rangle_{AC}|\phi^+\rangle_{BD}$、$|\varphi^+\rangle_{AC}|\varphi^+\rangle_{BD}$或$|\varphi^-\rangle_{AC}|\varphi^-\rangle_{BD}$，且得到每个结果的概率为 1/4。

2.3　量子逻辑门

量子力学中的粒子可以用逻辑门进行操作。后面我们会用到两个逻辑门，分别是 CNOT 门和 Hadamard 门。

CNOT 门也称为受控非门，它作用于两个量子比特上，其中一个称为控制位（控制量子比特），另一个为目标位（目标量子比特），其矩阵的表达形式为

$$
\boldsymbol{U}_{CNOT}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}。\tag{2}
$$

CNOT 门的操作过程如下：如果控制位为“0”，则不做任何操作；如果控制位为“1”，则目标位执行翻转操作。它的具体操作可以表示为（以 A 为控制位，以 B 为目标位）$|00\rangle_{AB}\rightarrow|00\rangle_{AB}$、$|01\rangle_{AB}\rightarrow|01\rangle_{AB}$、$|10\rangle_{AB}\rightarrow|11\rangle_{AB}$、$|11\rangle_{AB}\rightarrow|10\rangle_{AB}$。

Hadamard 门是作用于单粒子的量子逻辑门，它的矩阵表达形式为$\boldsymbol{H}=\begin{pmatrix}1/\sqrt{2}&1/\sqrt{2}\\1/\sqrt{2}&-1/\sqrt{2}\end{pmatrix}$。Hadamard 门对粒子的操作结果表示为$\boldsymbol{H}|0\rangle\rightarrow|+\rangle$、$\boldsymbol{H}|1\rangle\rightarrow|-\rangle$、$\boldsymbol{H}|+\rangle\rightarrow|0\rangle$、$\boldsymbol{H}|-\rangle\rightarrow|1\rangle$。

以下是利用 CNOT 门与 Hadamard 门对 Bell 态粒子进行的编码操作（编码操作的结果如表 1 所示）。

$$
\begin{aligned}
|\phi^-\rangle_{AB}=&1/\sqrt{2}\,(|00\rangle-|11\rangle)_{AB}\xrightarrow{CNOT_{AB}}\\
&1/\sqrt{2}\,(|00\rangle-|11\rangle)_{AB}=\\
&1/\sqrt{2}\,(|0\rangle-|1\rangle)_A|0\rangle_B\xrightarrow{\boldsymbol{H}_A}|1\rangle_A|0\rangle_B\longrightarrow 10。
\end{aligned}\tag{3}
$$

表 1　Bell 态及其编码结果

Table 1　Bell states and their coding results

State	Coding result
$\|\phi^+\rangle_{AB}=1/\sqrt{2}\,(\|00\rangle+\|11\rangle)_{AB}$	00
$\|\phi^-\rangle_{AB}=1/\sqrt{2}\,(\|00\rangle-\|11\rangle)_{AB}$	10
$\|\varphi^+\rangle_{AB}=1/\sqrt{2}\,(\|01\rangle+\|10\rangle)_{AB}$	01
$\|\varphi^-\rangle_{AB}=1/\sqrt{2}\,(\|01\rangle-\|10\rangle)_{AB}$	11

3　抗退相干的两方量子密钥协商协议

振幅阻尼信道是一种常见的量子信道，量子态经过振幅阻尼信道时会发生能量耗散，造成纠缠特性的损失。以$\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$为例，假设环境$E$对传输中粒子$|0\rangle$的影响可以表现为$|0\rangle_E$，退相干强度为$\lambda$，那么纠缠特性的损失可以表现为$|0\rangle|0\rangle_E\rightarrow|0\rangle|0\rangle_E$、$|1\rangle|0\rangle_E\rightarrow\sqrt{1-\lambda}|1\rangle|0\rangle_E+\sqrt{\lambda}|0\rangle|1\rangle_E$、$|+\rangle|0\rangle_E\rightarrow 1/\sqrt{2}\left(|0\rangle|0\rangle_E+\sqrt{1-\lambda}|1\rangle|0\rangle_E+\sqrt{\lambda}|0\rangle|1\rangle_E\right)$、$|-\rangle|0\rangle_E\rightarrow 1/\sqrt{2}\left(|0\rangle|0\rangle_E-\sqrt{1-\lambda}|1\rangle|0\rangle_E-\sqrt{\lambda}|0\rangle|1\rangle_E\right)$。此时，可以很明显地看出，除了$|0\rangle$，其他3个态$|1\rangle$、$|+\rangle$、$|-\rangle$都会受到退相干的影响。

为了消除退相干性，首先将使用四粒子团簇态进行弱测量之后再传输，弱测量可以使部分$|1\rangle$态演化为$|0\rangle$态，假设P为弱测量强度，此过程用非幺正算子表示为$M_W=\begin{pmatrix}0 & 0\\ 0 & \sqrt{1-P}\end{pmatrix}$。在四粒子团簇态中，量子弱测量可表示为

$$M_W(P_1,P_2,P_3,P_4)=\begin{pmatrix}0 & 0\\ 0 & \sqrt{1-P_1}\end{pmatrix}\otimes\begin{pmatrix}0 & 0\\ 0 & \sqrt{1-P_2}\end{pmatrix}\otimes\begin{pmatrix}0 & 0\\ 0 & \sqrt{1-P_3}\end{pmatrix}\otimes\begin{pmatrix}0 & 0\\ 0 & \sqrt{1-P_4}\end{pmatrix}。\tag{4}$$

接收方则可应用量子测量翻转对弱测量之后的量子态进行恢复，量子测量翻转可以使部分$|0\rangle$态演化为$|1\rangle$态。假设P_r为测量翻转强度，此过程用非幺正算子表示为$M_r=\begin{pmatrix}\sqrt{1-P_r} & 0\\ 0 & 0\end{pmatrix}$。在四粒子团簇态中，量子测量翻转可表示为

$$M_r(P_{r1},P_{r2},P_{r3},P_{r4})=\begin{pmatrix}\sqrt{1-P_{r1}} & 0\\ 0 & 0\end{pmatrix}\otimes\begin{pmatrix}\sqrt{1-P_{r2}} & 0\\ 0 & 0\end{pmatrix}\otimes\begin{pmatrix}\sqrt{1-P_{r3}} & 0\\ 0 & 0\end{pmatrix}\otimes\begin{pmatrix}\sqrt{1-P_{r4}} & 0\\ 0 & 0\end{pmatrix}。\tag{5}$$

协议步骤如下：

1）准备阶段

Alice准备了n个四粒子团簇态，并将其中所有粒子按照其所处的粒子位，分为四个有序序列S_A、S_B、S_C、S_D。

2）发送阶段

Alice对序列S_B、S_D执行操作$M_W(P_1,P_2,P_3,P_4)$从而进行弱测量，得到序列S_B^1、S_D^1。在这之后Alice随机从$\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$中选取$2m$个诱骗态粒子（为保证安全性，$m$必须足够大，本文$m=n$），并随机将其中$m$个粒子插入序列$S_B^1$中，剩余的$m$个粒子插入序列$S_D^1$中，形成新的序列$S_B^2$、$S_D^2$。Alice将$S_B^2$、$S_D^2$发送给Bob，自己保留$S_A$和$S_C$。量子态的制备与传输如图1所示。

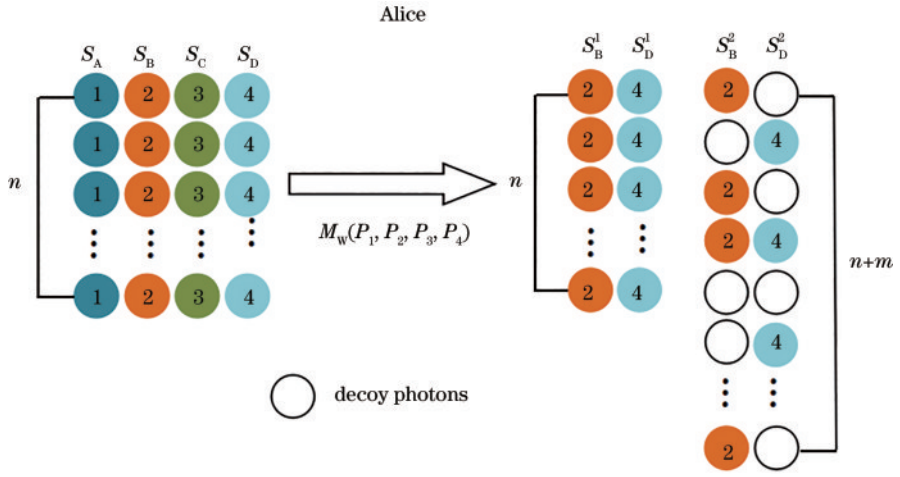

图1　量子态的制备与传输

Fig. 1　Preparation and transmission of quantum states

3）窃听检测阶段

Bob收到S_B^2、S_D^2之后，通过经典信道告知Alice。Alice确定Bob收到粒子后，公布诱骗态粒子的位置与测量基。Bob利用正确的测量基对诱骗态粒子进行测量，并且将测量的结果告诉Alice。Alice对比测量结果与诱骗态粒子的初始状态，计算错误率，如果错误率低于阈值则进行下一步，如果高于阈值则重新开始协议。窃听检测如图2所示。

4）测量阶段

Bob将S_B^2、S_D^2中的诱骗态粒子去除，还原为S_B^1、S_D^1，并且对S_B^1、S_D^1执行量子测量翻转操作，即$M_r(P_{r1},P_{r2},P_{r3},P_{r4})$操作，从而得到$S_B$、$S_D$。然后Bob对其进行联合Bell测量，并记录测量结果。同时Alice对序列S_A、S_C进行联合Bell测量，记录测量结果。

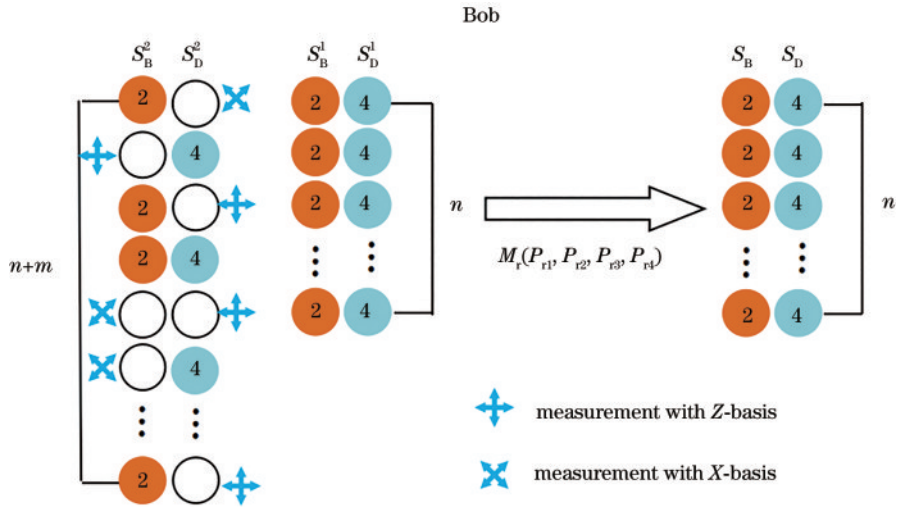

图 2　窃听检测

Fig. 2　Eavesdropping detection

5) 密钥生成阶段

Bob 对自己的测量结果施行 CNOT 操作，以 B 为控制位，以 D 为目标位，之后再对 B 位进行一次 H 门操作，得到两个粒子，并依据式(3)所示的编码操作进行编码。Alice 对自己的测量结果施行 CNOT 操作，且以 A 为控制位，以 C 为目标位，之后再对 A 位进行一次 H 门操作得到两个粒子，并依据式(3)所示的编码操作进行编码。此时，Bob 可以根据自己的两位编码结果对照式(1)对 Alice 的两位编码结果进行推测，Alice 也可以使用同样的操作对 Bob 的两位编码结果进行推测。最后，Alice 与 Bob 可以得到 A、B、C、D 位的编码结果，并从中提取出 A 位与 B 位所代表的编码，得到长度为 $2n$ 的共享密钥。Bell 测量与密钥协商如图 3 所示，其中 BM 表示 Bell 测量。

例如，假设当 $n=1$ 时，Bob 的测量结果为 $|\phi^+\rangle$。应用式(3)的编码方法并对照表 1 可以得到 B、D 位所对应的编码为“00”。依据式(1)，Bob 可以推测 Alice 的测量结果为 $|\phi^-\rangle$，对照表 1 可以得到 A、C 位所对应的编码为“10”。此时，Bob 可以得到 A、B、C、D 位的编码结果“1000”，并从中提取 A、B 位所对应的共享密钥“10”(Alice 的操作类似)。最终，Alice 与 Bob 共享密钥“10”，完成此次密钥协商。测量结果与最终共享密钥的关系如表 2 所示。

表 2　测量结果与最终共享密钥

Table 2　Measurement results and final shared key

Measurement result	Coding results (ABCD)	Key (AB)
$\|\phi^+\rangle_{AC}\|\phi^-\rangle_{BD}$	0100	01
$\|\phi^-\rangle_{AC}\|\phi^+\rangle_{BD}$	1000	10
$\|\phi^+\rangle_{AC}\|\psi^+\rangle_{BD}$	0011	00
$\|\psi^-\rangle_{AC}\|\psi^-\rangle_{BD}$	1111	11

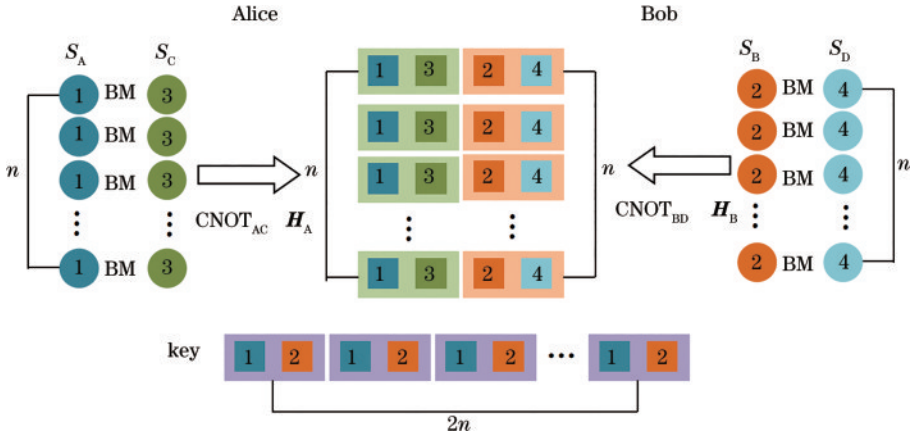

图 3　Bell 测量与密钥协商

Fig. 3　Bell measurement and key agreement

4　安全性分析

为分析 Alice 与 Bob 密钥协商过程的安全性，假设 Eve 是攻击者。

1）抗退相干性

在此协议中，由于 Alice 对序列 S_B、S_D 执行弱测量操作，令部分 $|1\rangle$ 态演化为 $|0\rangle$ 态，从而使得序列在通过振幅阻尼信道时，受到环境的影响大大降低。之后，Bob 执行的量子翻转操作，使被影响的 $|0\rangle$ 态还原为 $|1\rangle$ 态。因此，本协议中信息传输受振幅阻尼信道的影响会显著降低，且弱测量强度越大受到的影响越小。

2）参与者攻击

假设 Alice 与 Bob 中有一个不诚实的参与者，他想独自确定共享密钥。但由于密钥的共享是由双方分别进行 Bell 态测量才能确定，且测量的结果是由等概的四种情况组成的，所以不诚实参与者攻击成功的可能性为 $(1/4)^n$（当 n 足够大时，概率接近 0）。

3）拦截-重发攻击

假设外部攻击者 Eve 拦截并保存 S_B^2、S_D^2，同时将自己伪造的序列发送给 Bob，然后她对拦截到的 S_B^2、S_D^2 进行联合 Bell 测量。由于 Eve 并不知道诱骗态粒子的位置，以及 Alice 对哪些粒子进行了弱测量，所以她的行为会在窃听检测阶段被检测到而无法成功。假设在传输过程中插入了 m 个诱骗态粒子，此时，Alice 与 Bob 可以检测到 Eve 的概率为 $1-(1/2)^m$（m 足够大时，概率接近 1）。

4）测量-重发攻击

假设 Eve 对 S_B^2、S_D^2 进行测量-重发攻击，当 Eve 对 S_B^2、S_D^2 进行联合 Bell 测量后，会使粒子坍缩成为确定的四种态之一 $\left\{|\phi^+\rangle, |\phi^-\rangle, |\varphi^+\rangle, |\varphi^-\rangle\right\}$。由于 Eve 无法知道 S_B^2、S_D^2 中所插入的诱骗态粒子的位置，以及哪些粒子进行了弱测量，因此她的测量行为会使诱骗态粒子的状态发生改变，在窃听检测阶段，Alice 与 Bob 可以检测到 Eve 的概率为 $1-(3/4)^m$。当 m 足够大时，概率接近 1，因此，Eve 无法通过窃听检查。

5）纠缠-测量攻击

假设 Eve 想通过纠缠测量攻击获取相关信息。在该协议中，Eve 可以截获 S_B^2、S_D^2，然后用提前准备好的辅助态 $|E\rangle$ 对 S_B^2、S_D^2 进行纠缠，并且在 Alice 与 Bob 进行完流程之后，对自己的辅助粒子进行测量，获取相关信息。由于 Eve 并不知道诱骗态粒子的位置，因此，Eve 所进行的操作不仅会与 S_B^2、S_D^2 序列中的信息粒子形成纠缠，还会与诱骗态粒子形成纠缠。假设 Eve 的操作为 U_E，那么 Eve 的纠缠操作对四种诱骗态的影响如下：

$$U_E|0\rangle|E\rangle = a|0\rangle|E_{00}\rangle + b|1\rangle|E_{01}\rangle, \tag{6}$$

$$U_E|1\rangle|E\rangle = c|0\rangle|E_{10}\rangle + d|1\rangle|E_{11}\rangle, \tag{7}$$

$$\begin{aligned} U_E|+\rangle|E\rangle &= 1/\sqrt{2}\,U_E(|0\rangle+|1\rangle)|E\rangle = \\ &(a|0\rangle|E_{00}\rangle + b|1\rangle|E_{01}\rangle + c|0\rangle|E_{10}\rangle + d|1\rangle|E_{11}\rangle) = \\ &1/2|+\rangle(a|E_{00}\rangle + b|E_{01}\rangle + c|E_{10}\rangle + d|E_{11}\rangle) + \\ &1/2|-\rangle(a|E_{00}\rangle - b|E_{01}\rangle + c|E_{10}\rangle - d|E_{11}\rangle), \end{aligned} \tag{8}$$

$$\begin{aligned} U_E|-\rangle|E\rangle &= 1/\sqrt{2}\,U_E(|0\rangle-|1\rangle)|E\rangle = \\ &(a|0\rangle|E_{00}\rangle + b|1\rangle|E_{01}\rangle - c|0\rangle|E_{10}\rangle - d|1\rangle|E_{11}\rangle) = \\ &1/2|+\rangle(a|E_{00}\rangle + b|E_{01}\rangle - c|E_{10}\rangle - d|E_{11}\rangle) + \\ &1/2|-\rangle(a|E_{00}\rangle - b|E_{01}\rangle - c|E_{10}\rangle + d|E_{11}\rangle)。 \end{aligned} \tag{9}$$

如果 Eve 不想诱骗态发生改变，必须满足以下条件：

$$\begin{cases} b=0, |a|^2+|b|^2=1 \\ c=0, |c|^2+|d|^2=1 \\ a|E_{00}\rangle - b|E_{01}\rangle + c|E_{10}\rangle - d|E_{11}\rangle = 0 \\ a|E_{00}\rangle + b|E_{01}\rangle - c|E_{10}\rangle - d|E_{11}\rangle = 0 \end{cases}。 \tag{10}$$

满足式（10）的条件，解得 $a=d=1$，$b=c=0$，$|E_{00}\rangle=|E_{11}\rangle$。由于量子信道中传输的是 S_B^2 和 S_D^2，同时 Eve 无法知道诱骗态粒子的位置，因此她只能通过上述方程得到的结果进行纠缠操作，否则将会改变诱骗态的初始状态，从而无法通过窃听检测阶段。

此时 Eve 对 S_B^1、S_D^1（S_B^1、S_D^1 是 S_B^2、S_D^2 分别去掉诱骗态之后得到的序列）中经过弱测量操作而发生状态改变的粒子所进行的纠缠操作如下：

$$\begin{aligned} U_E|\Psi\rangle_B|E\rangle &= 1/2(|0\rangle+|0\rangle+|0\rangle-|0\rangle)|E\rangle = \\ &|0\rangle|E_{00}\rangle, \end{aligned} \tag{11}$$

$$\begin{aligned} U_E|\Psi\rangle_D|E\rangle &= 1/2(|0\rangle+|0\rangle+|0\rangle-|0\rangle)|E\rangle = \\ &|0\rangle|E_{00}\rangle。 \end{aligned} \tag{12}$$

Eve 对 S_B^1、S_D^1 中经过弱测量操作而状态未发生改变的粒子所进行的纠缠操作如下：

$$\begin{aligned} U_E|\Psi\rangle_B|E\rangle &= 1/2(|0\rangle+|0\rangle+|1\rangle-|1\rangle)|E\rangle = \\ &|0\rangle|E_{00}\rangle, \end{aligned} \tag{13}$$

$$\begin{aligned} U_E|\Psi\rangle_B|E\rangle &= 1/2(|0\rangle+|1\rangle+|0\rangle-|1\rangle)|E\rangle = \\ &|0\rangle|E_{00}\rangle。 \end{aligned} \tag{14}$$

由式（11）～（14）可知，Eve 无法分辨两种不同的初始状态，因此她无法通过此种纠缠操作获得任何有效信息。综上所述，Eve 无法通过纠缠测量攻击获得有效信息。

5　效率分析

本文使用 Cabello[23] 提出的计算量子比特效率的方法，其量子比特效率公式为 $\eta=\frac{c}{q+b}$，其中，c 为共享密钥的比特数量，q 为使用的量子比特数量，b 为解码信息时需要交换的经典比特数量。因此，本文协议的量子比特效率为 $\eta=\frac{c}{q+b}=\frac{2n}{4n+2m}$。这是因为

在本文协议中，当共享长度为 $2n$ 的密钥时，协议共使用了 $4n$ 个信息粒子和 $2m$ 个诱骗态粒子，且本协议在解码信息时不需要交换经典比特。当 $m=n$ 时，此协议的量子比特效率 $\eta=1/3=33.3\%$。对比文献[5]、[10]、[18]、[24]所提出的密钥协商协议，本文所提出的协议由于使用了四粒子团簇态并配合式(3)所示的编码操作，协议过程中所用冗余量子态较少，因此在量子比特效率方面具有一定优势。本文提出的协议与其他协议的比较如表3所示。根据表3可以看出，本文所提出的协议具有更加简单的测量方法以及较高的量子比特效率。

表3 所提协议与其他协议的比较

Table 3 Comparison between the proposed protocol and other protocols

QKA protocol	Quantum resource	Measurement basis	Qubit efficiency /%
Ref. [5]	Bell states	X-basis and Bell-basis	26.67
Ref. [10]	Cluster states	Cluster-basis	30.77
Ref. [18]	Bell states	Bell-basis	25.00
Ref. [24]	Bell states	Bell-basis	14.29
Proposed protocol	Four-particle cluster states	Bell-basis	33.30

6 结 论

本文提出了一个基于四粒子团簇态的抗退相干性的两方量子密钥协商协议。新协议使用了四粒子团簇态并配合受控非门与Hadamard门进行信息编码，同时协议使用了弱测量和量子测量翻转技术来抵抗振幅阻尼信道对量子态退相干性的影响，使得该协议不但可以适用于传统的理想量子信道，而且也可以适用于一般的振幅阻尼信道。安全性分析可以发现，新协议可以同时抵抗内部攻击与外部攻击，符合密钥协商的安全性需求。最后，效率分析表明，新协议具有较高的量子比特效率，约为33.3%，与其他协议相比具有一定优势，并且在新协议中通信双方只需要使用Bell基进行测量，测量方法也比较简单。

参 考 文 献

[1] Diffie W, Hellman M E. New directions in cryptography [J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[2] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings 35th Annual Symposium on Foundations of Computer Science, November 20-22, 1994, Santa Fe, NM, USA. New York: IEEE Press, 1994: 124-134.

[3] Grover L K. A fast quantum mechanical algorithm for database search[C]//STOC '96: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, May 22-24, 1996, Philadelphia, Pennsylvania, USA. New York: ACM Press, 1996: 212-219.

[4] Zhou N R, Zhang T F, Xie X W, et al. Hybrid quantum-classical generative adversarial networks for image generation via learning discrete distribution[J]. Signal Processing: Image Communication, 2023, 110: 116891.

[5] Gao H, Chen X G, Qian S R. Two-party quantum key agreement protocols under collective noise channel[J]. Quantum Information Processing, 2018, 17(6): 140.

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

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

[8] 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.

[9] Xu G B, Wen Q Y, Gao F, et al. Novel multiparty quantum key agreement protocol with GHZ states[J]. Quantum Information Processing, 2014, 13(12): 2587-2594.

[10] Yang Y G, Li B R, Li D, et al. New quantum key agreement protocols based on Bell states[J]. Quantum Information Processing, 2019, 18(10): 322.

[11] Zhou N R, Zhu K N, Zou X F. Multi-party semi-quantum key distribution protocol with four-particle cluster states[J]. Annalen Der Physik, 2019, 531(8): 1800520.

[12] 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.

[13] 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 states [J]. Chinese Journal of Lasers, 2022, 49(13): 1312001.

[14] Chang Y, Zhang S B, Li J, et al. Robust EPR-pairs-based quantum secure communication with authentication resisting collective noise[J]. Science China Physics, Mechanics & Astronomy, 2014, 57(10): 1907-1912.

[15] He Y F, Ma W P. Multiparty quantum secure direct communication immune to collective noise[J]. Quantum Information Processing, 2019, 18(1): 4.

[16] Ye T Y. Fault tolerant channel-encrypting quantum dialogue against collective noise[J]. Science China Physics, Mechanics & Astronomy, 2015, 58(4): 1-10.

[17] Chang L W, Zhang Y Q, Tian X X, et al. Fault tolerant controlled quantum dialogue with logical brown states against collective noise[J]. International Journal of

Theoretical Physics, 2020, 59(7): 2155-2174.
[18] Wang S S, Jiang D H, Xu G B, et al. Quantum key agreement with Bell states and cluster states under collective noise channels[J]. Quantum Information Processing, 2019, 18(6): 190.
[19] 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.
[20] He Y F, Ma W P. Two-party quantum key agreement against collective noise[J]. Quantum Information Processing, 2016, 15(12): 5023-5035.
[21] 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.
[22] Korotkov A N, Keane K. Decoherence suppression by quantum measurement reversal[J]. Physical Review A, 2010, 81(4): 040103.
[23] Cabello A. Quantum key distribution in the Holevo limit [J]. Physical Review Letters, 2000, 85(26): 5635-5638.
[24] 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.