光通信研究
Study on Optical Communications
ISSN 1005-8788,CN 42-1266/TN

《光通信研究》网络首发论文

题目：　使用正交乘积基的量子密钥协商
作者：　李璇冰，陈云，李帅
网络首发日期：　2025-05-26
引用格式：　李璇冰，陈云，李帅．使用正交乘积基的量子密钥协商[J/OL]．光通信研究．
https://link.cnki.net/urlid/42.1266.tn.20250523.1716.012

网络首发时间：2025-05-26 11:51:04　网络首发地址：https://link.cnki.net/urlid/42.1266.tn.20250523.1716.012

使用正交乘积基的量子密钥协商

李璇冰，陈 云，李 帅

（宁夏大学 信息工程学院，银川 750021）

摘要:【目的】在物联网(IoT)中，设备众多，通信频繁，安全的密钥协议至关重要。多方量子密钥协商(MQKA)是一种基于量子通信的密钥协议。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，MQKA 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，该协议在 IoT 环境中的部署可构建多设备间安全密钥协商机制，有效保护设备间的通信和数据交换的安全性。【方法】在 MQKA 中，多个通信参与者使用量子通道进行交互，通过发送和测量量子态来协商一个共享密钥。文章提出了一种基于正交乘积态和量子秘密共享过程的 MQKA。结合正交乘积态的特性和混淆操作，类似于量子秘密共享的过程，密钥中心将密钥发送到量子网络中的不同目标节点，目标节点通过相互身份认证后协同工作，恢复共享密钥。【结果】相比于现有的大多数 MQKA 通过纠缠态实现，文章提出的协议基于正交乘积态，规避了纠缠资源制备的高成本和维持的困难性，同时，协议过程包含了参与者的身份认证，增强了协议的安全性。结合量子通信技术和密钥协议，MQKA 为物联网网络安全提供了新的可能性。【结论】协议安全性已通过系统评估，结合与现有量子协议的对比分析，验证表明所提协议可实现无秘密信息泄露条件下的安全多方密钥协商。

关键词：多方量子密钥协商；正交乘积态；身份认证；物联网网络安全

中图分类号：TN929　**文献标志码：**A

Quantum Key Agreement Using Orthogonal Product Bases

Li Xuan-bing, Chen Yun, Li Shuai

(School of Information Engineering, Ningxia University, Yinchuan, 750021, China.)

Abstract:【Objective】In the Internet of Things (IoT), where there are many devices and frequent communication, a secure key agreement is crucial. The Multi-party Quantum Key Agreement (MQKA) protocol is a quantum communication-based cryptographic scheme. Unlike classical protocols reling on mathematical hard problems, the MQKA protocol guarantees security through quantum mechanical principles, which provides unconditional security. When deployed in IoT environments, it establishes secure inter-device key negotiation mechanisms to protect communication integrity.【Methods】In the MQKA protocol, participants communicate via quantum channels to agree on a shared key through quantum state transmission and measurement. In this paper, we propose an MQKA protocol integrating orthogonal product states with quantum secret sharing.By combining state orthogonality and obfuscation operations, the protocol enables the key center to distribute keys to target nodes in the quantum networks. These nodes collaboratively recover the key after mutual authentication, analogous to quantum secret sharing processes.【Results】Compared to most of the existing MQKA protocols realized through entangled states, the protocol proposed in this paper is based on orthogonal product states, which circumvents the high cost of entanglement resource preparation and the difficulty of maintaining it, and at the same time, the process of the protocol includes the authentication of the participants, which enhances the security of the protocol. Combining quantum communication technology and key protocol, MQKA protocol provides new possibilities for IoT network security.【Conclusion】The security of the protocol has been systematically evaluated, and combined with the comparative analysis with the existing

基金项目：宁夏自然科学基金资助项目（No.2020AAC03035）

作者简介：李璇冰（2000-），女，河北石家庄人。硕士，主要研究方向为量子密码学。

通信作者：李帅，副教授。E-mail: lis@nxu.edu.cn

quantum protocols, the verification shows that the proposed protocol can realize secure multi-party key negotiation under the condition of no secret information leakage.

Key words: MQKA；Orthogonal product states；Authentication；IoT network security

0 引言

计算机和物联网（Internet of Things, IoT）技术的快速发展给网络数据安全传输带来了挑战。传统加密机制因算力提升存在被破解的风险，量子密码基于量子力学原理，为信息安全提供了新方向，其中多方量子密钥协商（multi-party quantum key agreement, MQKA）协议因为能在多个设备间建立共享密钥而备受关注[1-7]。

BB84 和 B92 协议利用非纠缠的粒子实现量子密钥分发（quantum key distribution, QKD）[8-9]。研究表明，局部不可区分正交乘积（locally indistinguishable orthogonal product, LIOP）态在局域操作和经典通信（local operations and classical communication, LOCC）下无法被完美区分，为信息提供了天然保护[10-12]。研究者逐步开发了 LIOP 态在 QKD[13-15]、量子秘密共享（quantum secret sharing, QSS）[16-17]及可信支付协议[18-19]中的应用。

多数 MQKA 协议仍依赖纠缠态实现，而纠缠资源的制备与维护成本较高，限制了实际应用。此外，现有方案常忽略参与者身份认证环节，可能引入冒充攻击。QSS 作为安全多方计算的核心分支，可通过分布式秘密恢复机制增强协议可靠性[20-22]。本文提出一种基于 LIOP 态与 QSS 过程的 MQKA 协议。通过将密钥信息编码为 LIOP 态，协议实现密钥在量子网络中的安全分发与协同恢复，无需依赖纠缠资源。目标节点在通过身份认证后参与密钥重建，从而抵御非法访问。剩余结构安排如下：第一节阐述量子位正交乘积态的特性，第二节详述提出的 MQKA 协议，第三节给出一个简单示例，第四节进行协议论证，第五节总结成果。

1 量子位正交乘积基

正交乘积基是一组相互正交的乘积态，在$\left(\mathbb{C}^2\right)^{\otimes p}$量子体系中有以下大小为$\left(p+1\right)$的局部不可区分的正交乘积基，其中$p\geq 3$，下标表示第$i$子系统$\left(1\leq i\leq p\right)$。

$$
\begin{aligned}
&|\phi_1\rangle = |0\rangle_1 |0\rangle_2 |0\rangle_3 \cdots |0\rangle_p \\
&|\phi_2\rangle = \frac{1}{2}\left(|0\rangle - |1\rangle\right)_1 |1\rangle_2 \cdots |1\rangle_{p-1} \left(|0\rangle + |1\rangle\right)_p \\
&|\phi_3\rangle = \frac{1}{2}\left(|0\rangle + |1\rangle\right)_1 \left(|0\rangle - |1\rangle\right)_2 |1\rangle_3 \cdots |1\rangle_p \\
&|\phi_4\rangle = \frac{1}{2}|1\rangle_1 \left(|0\rangle + |1\rangle\right)_2 \left(|0\rangle - |1\rangle\right)_3 |1\rangle_4 \cdots |1\rangle_p \\
&\cdots \\
&|\phi_{p+1}\rangle = \frac{1}{2}|1\rangle_1 \cdots |1\rangle_{p-2} \left(|0\rangle + |1\rangle\right)_{p-1} \left(|0\rangle - |1\rangle\right)_p
\end{aligned}
\tag{1}
$$

在文献[23]中证明了这些态不能由 LOCC 完全区分，它们有以下属性：即使得到$(p-1)$个正交积态的粒子，也无法确定其确切形式；每个粒子都可以独立传输；对其中一个粒子的操作不会影响到其他粒子。当$p=3$时，上述 LIOP 态表示为：

$$
\begin{aligned}
&|\phi_1\rangle = |0\rangle_1 |0\rangle_2 |0\rangle_3 \\
&|\phi_2\rangle = \frac{1}{2}\left(|0\rangle - |1\rangle\right)_1 |1\rangle_2 \left(|0\rangle + |1\rangle\right)_3 \\
&|\phi_3\rangle = \frac{1}{2}\left(|0\rangle + |1\rangle\right)_1 \left(|0\rangle - |1\rangle\right)_2 |1\rangle_3 \\
&|\phi_4\rangle = \frac{1}{2}|1\rangle_1 \left(|0\rangle + |1\rangle\right)_2 \left(|0\rangle - |1\rangle\right)_3
\end{aligned}
\tag{2}
$$

2 多方量子密钥共享机制

本文提出的多方量子密钥协商机制需要一个诚实的密钥中心 Center 作为中间方。Center 随机生成经典序列X，作为原始密钥，使用（1）式的 LIOP 态作为量子态编码载体，将X编码后发给量子密钥协商的参与者$L_1, L_2, \cdots, L_p$，参与者通过相互认证后协作恢复原始密钥，再对原始密钥处理后得到最终的共享密钥。提出的 MQKA 协议具体步骤如下。

Step 1：Center 生成随机序列X，作为原始密钥序列。协议将不同的m位序列表示为$a_1 = 00\ldots00$，$a_2 = 00\ldots01$，$a_3 = 00\ldots10$，$a_4 = 00\ldots11$，$\cdots$，$a_{2^m} = 11\ldots11$，其中$m = \lfloor \log_2(p+1) \rfloor$。Center 将$X$分成$n$组：$x_1, x_2, \cdots, x_n$，其中$x_i \in \{a_1, a_2, \cdots, a_{2^m}\}$，$i = 1, 2, \cdots n$，再对$X$编码，记为量子序列$|S\rangle$，编码规则如（3）式：

$$a_i \mapsto |\phi_i\rangle \left(i = 1, 2, \cdots 2^m\right) \tag{3}$$

如果 $p+1 > 2^m$，那么 $|\phi_{2^m+1}\rangle \sim |\phi_{p+1}\rangle$ 用作诱饵态，否则诱饵态取自集合 $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$。

Step 2：Center 将编码量子序列 $|S\rangle$ 制作 p 份，并将 $|S\rangle$ 按照量子系统分成 p 个子系统：$|S\rangle := \{|S_1\rangle |S_2\rangle \cdots |S_p\rangle\}$，其中 $|S_i\rangle (1 \le i \le p)$ 由编码量子态第 i 粒子组成。

Step 3：Center 将 p 个相同序列的子系统顺序打乱，得到 p 个新的序列：

$$\begin{aligned} |M_1\rangle &= \{|S_1\rangle |S_2\rangle |S_1\rangle \cdots |S_1\rangle\} \\ |M_2\rangle &= \{|S_2\rangle |S_3\rangle |S_2\rangle \cdots |S_2\rangle\} \\ &\cdots \\ |M_p\rangle &= \{|S_p\rangle |S_1\rangle |S_p\rangle \cdots |S_p\rangle\} \end{aligned} \tag{4}$$

Step 4：Center 将诱饵态随机插入 $|M_i\rangle$ 形成 $|M_i'\rangle (i = 1, 2, \cdots, p)$，随机将 $|M_i'\rangle$ 发给参与者，并记录为 L_i。

Step 5：L_i 收到 $|M_i'\rangle$ 后向 Center 发送确认。Center 同时宣布诱饵态在 $|M_i'\rangle$ 中的位置和测量基（Z 基：$\{|0\rangle, |1\rangle\}$，X 基：$\{|+\rangle, |-\rangle\}$）。L_i 测量诱饵态并公布测量结果，Center 根据测量结果检测窃听。如果未检测到窃听，则继续执行下一步。否则，协议从 Step 1 重启。

Step 6：窃听检测结束后 L_i 移除诱饵态粒子，将 $|M_i'\rangle$ 恢复为 $|M_i\rangle$。参与者各自制作包含 $(m+1)n$ 位的量子序列，其中量子比特来自集合 $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$，后 n 位是他们事先在 Center 处注册的秘密身份码。参与者将制备的量子序列完整插入每组子序列中，粒子顺序固定，插入位置随机，同时记录粒子在子序列中的位置和测量基。Center 公布参与者的顺序，L_i 将第 $j (j = 1, 2, \cdots, p)(j \ne i)$ 组子序列发给 L_j。

Step 7：参与者公布各自插入粒子的位置和前 mn 位粒子的测量基，同时根据其他参与者公布的信息分离出他们制备的量子序列，并对前 mn 位粒子进行测量，随后将剩余的 n 位粒子发给 Center。Center 按照各个参与者注册身份码的测量基测量后对比结果和对应的身份码，公布各个参与者的合法性。Center 随机挑选 $1 \sim mn$ 中的一些位作为校验位，参与者分别

公布他们制备的量子序列中校验位对应的值，检测是否存在内部恶意攻击。如果没有恶意节点的攻击，他们对自己和得到的其他参与者制备粒子的前 mn 位进行编码，将编码后的序列表示为 $R_{L_1}, R_{L_2}, \cdots R_{L_p}$ 。编码规则是：若量子态是 $|0\rangle$ 或 $|+\rangle$，则编码为 0；否则编码为 1。

Step 8：Center 公布序列 $|S\rangle$ 的测量基，参与者测量后得到原始密钥 X 。

Step9：Center 随机公布一些粒子的位置和量子态，以检测可能的窃听。如果没有窃听，$L_1, L_2, \cdots, L_p$ 得到共享密钥： $K = X \oplus R_{L_1} \oplus R_{L_2} \oplus \cdots \oplus R_{L_p}$ 。

3 三方量子密钥协商示例

为了方便理解，本节给出不考虑窃听检测和身份认证过程情况下，有三个参与者，即 $p = 3$ 时的示例：密钥中心 Center 作为诚实的中间方，生成随机序列 $X = 0100011011$ 作为原始密钥，再根据（2）式的 LIOP 态编码后发给密钥协商的参与者：Alice、Bob 和 Charlie，后文简称为 A、B 和 C，他们相互协作恢复原始密钥，处理后得到最终共享密钥。图 1 为简化的流程图：

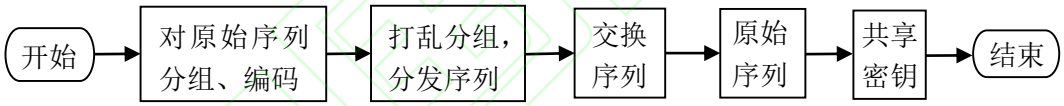

图 1 三方量子密钥协商简化流程图

Figure 1 Simplified flowchart of tripartite quantum key agreement

Step 1：Center 将 X 分组，其中每组长为 $m = \lfloor \log_2(p+1) \rfloor = 2$ bit，有 $n = 10/2 = 5$ 组：$x_1, x_2, \cdots, x_5$，其中 $x_1 = 01$，$x_2 = 00$，$x_3 = 01$，$x_4 = 10$，$x_5 = 11$。随后，Center 使用（2）式作为量子态编码载体对 X 编码，并记录量子态序列的测量基，编码规则如下：

$$00 \mapsto |\phi_1\rangle, 01 \mapsto |\phi_2\rangle, 10 \mapsto |\phi_3\rangle, 11 \mapsto |\phi_4\rangle \tag{5}$$

$X = 0100011011$ 经过编码后的量子序列记为 $|S\rangle$：

$$0100011011\mapsto\left|\phi_2\phi_1\phi_2\phi_3\phi_4\right\rangle:=\left|S\right\rangle=\\ \left\{\left|-\right\rangle_1\left|1\right\rangle_2\left|+\right\rangle_3\left|0\right\rangle_1\left|0\right\rangle_2\left|0\right\rangle_3\left|-\right\rangle_1\left|1\right\rangle_2\left|+\right\rangle_3\left|+\right\rangle_1\left|-\right\rangle_2\left|1\right\rangle_3\left|1\right\rangle_1\left|+\right\rangle_2\left|-\right\rangle_3\right\} \tag{6}$$

Step 2：Center 将量子序列$\left|S\right\rangle$制作 3 份，并将$\left|S\right\rangle$按照量子系统分成 3 个子系统：$\left|S\right\rangle:=\left\{\left|S_1\right\rangle\left|S_2\right\rangle\left|S_3\right\rangle\right\}$，其中序列$\left|S_i\right\rangle\left(i=1,2,3\right)$是量子态第 i 粒子的集合，即$\left|S_1\right\rangle=\left\{\left|-\right\rangle\left|0\right\rangle\left|-\right\rangle\left|+\right\rangle\left|1\right\rangle\right\}_1$，$\left|S_2\right\rangle=\left\{\left|1\right\rangle\left|0\right\rangle\left|1\right\rangle\left|-\right\rangle\left|+\right\rangle\right\}_2$，$\left|S_3\right\rangle=\left\{\left|+\right\rangle\left|0\right\rangle\left|+\right\rangle\left|1\right\rangle\left|-\right\rangle\right\}_3$。

Step 3：Center 将 3 个量子序列$\left|S\right\rangle$中的子系统顺序打乱，得到：$\left|M_1\right\rangle=\left\{\left|S_1\right\rangle\left|S_2\right\rangle\left|S_1\right\rangle\right\}$，$\left|M_2\right\rangle=\left\{\left|S_2\right\rangle\left|S_3\right\rangle\left|S_2\right\rangle\right\}$,$\left|M_3\right\rangle=\left\{\left|S_3\right\rangle\left|S_1\right\rangle\left|S_3\right\rangle\right\}$，分别发给 A，B，C。

Step 4：不考虑身份认证的情况下，A、B 和 C 各自制备包含$mn=2\times5=10$个粒子的量子序列：A：$\left|001+-11++0\right\rangle$，B：$\left|---+11001+\right\rangle$，C：$\left|+10001++-1\right\rangle$。随后 A、B 和 C 在每组子序列中插入制备的量子序列。A、B 和 C 持有的量子序列被记录为$\left|M_1\right\rangle'=\left\{\left|S_1\right\rangle_{\mathrm{A}}\left|S_2\right\rangle_{\mathrm{A}}\left|S_1\right\rangle_{\mathrm{A}}\right\}$，$\left|M_2\right\rangle'=\left\{\left|S_2\right\rangle_{\mathrm{B}}\left|S_3\right\rangle_{\mathrm{B}}\left|S_2\right\rangle_{\mathrm{B}}\right\}$，$\left|M_3\right\rangle'=\left\{\left|S_3\right\rangle_{\mathrm{C}}\left|S_1\right\rangle_{\mathrm{C}}\left|S_3\right\rangle_{\mathrm{C}}\right\}$，其中，字母下标表示子序列包含完整的对应的参与者制备的量子序列。Center 公布 A、B 和 C 的顺序是 1、2 和 3。A 将第二组子序列$\left|S_2\right\rangle_{\mathrm{A}}$发给 B，将第三组子序列$\left|S_1\right\rangle_{\mathrm{A}}$发给 C。B 将第一组子序列$\left|S_2\right\rangle_{\mathrm{B}}$发给 A，将第三组子序列$\left|S_2\right\rangle_{\mathrm{B}}$发给 C。C 将$\left|S_3\right\rangle_{\mathrm{C}}$发给 A，将$\left|S_1\right\rangle_{\mathrm{C}}$发给 B。图 2 展示了 A、B 和 C 相互交换子序列。

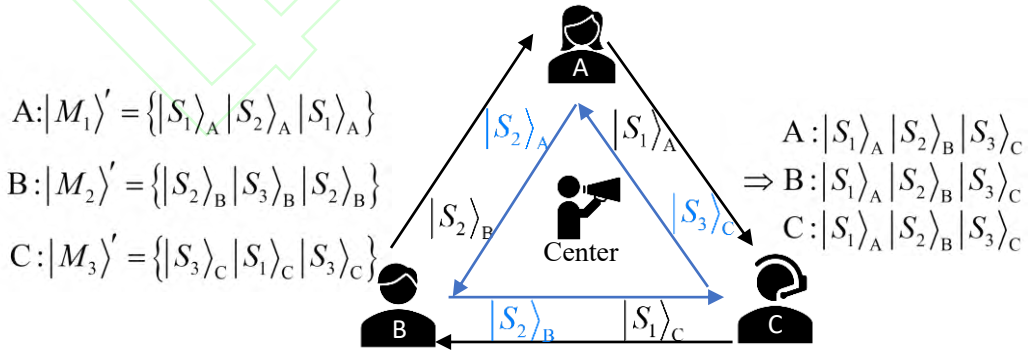

图 2 A、B 和 C 交换子序列

Figure 2 A, B and C exchange subsequences

Step 5：A、B 和 C 公布子序列中插入粒子的位置和测量基，分离出量子序列后测量，

A、B 和 C 得到 Step 4 中制备的量子序列，随后他们对量子序列编码，得到 $R_{\mathrm{A}}=0010111000$，$R_{\mathrm{B}}=1110110010$，$R_{\mathrm{C}}=0100010011$。

Step 6：Center 公布 X 的测量基，A、B、C 测量后得到原始密钥 X，最终共享密钥是 $K=X\oplus R_{\mathrm{A}}\oplus R_{\mathrm{B}}\oplus R_{\mathrm{C}}=1100000010$。

4 协议分析

本节对提出的协议进行安全性和效率分析。内部节点直接参与密钥协商过程，具有更强的攻击性，本节分析了内部节点的伪造攻击以及协议第三方 Center 可能发起的攻击。针对外部恶意节点，安全分析涵盖了拦截-重发(intercept-replay, IR)攻击、拦截-测量-重发(intercept-measure-replay, IMR)攻击和纠缠-测量(entangle-measure, EM)攻击三种典型攻击，表 1 对比了本文提出的协议和现有相关量子协议，其中 n 是用于检测窃听的粒子数。针对量子比特效率对所提协议进行了效率分析。

4.1 内部攻击

伪造攻击：内部节点的伪造攻击主要发生在量子态发送阶段，恶意节点有机会在 Step 6 参与者相互发送子序列时进行伪造。研究设定为有 p 个参与者（其中有 r 个恶意节点），其交换子序列的长度是 n 个粒子。分析首先考虑单粒子攻击场景：设原始粒子处于量子态 $|\psi\rangle$，恶意节点发送的伪造粒子处于量子态 $|\varphi\rangle$，如果 $|\varphi\rangle$ 与 $|\psi\rangle$ 正交，接收方一定能检测到伪造；如果 $|\varphi\rangle$ 与 $|\psi\rangle$ 相同，伪造粒子无法被检测，攻击成功；如果 $|\varphi\rangle$ 与 $|\psi\rangle$ 非正交，则伪造成功的概率取决于 $|\langle\psi|\varphi\rangle|^2$。$|\psi\rangle$ 和 $|\varphi\rangle$ 都取自集合 $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$，对于选定的 $|\varphi\rangle$，平均伪造成功的概率为

$$P(|\varphi\rangle)=\frac{1}{4}\sum_{|\psi\rangle\in\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}}|\langle\psi|\varphi\rangle|^2 \tag{7}$$

若恶意节点选择 $|\varphi\rangle=|0\rangle$，则 $P(|0\rangle)=\frac{1}{4}\left(|\langle 0|0\rangle|^2+|\langle 1|0\rangle|^2+|\langle +|0\rangle|^2+|\langle -|0\rangle|^2\right)=\frac{1}{2}$，

类似地，若恶意节点选择$|\varphi\rangle=|1\rangle$、$|+\rangle$或$|-\rangle$，平均伪造成功概率也都是$1/2$，因此对于一个粒子，一个恶意节点对其成功伪造的概率是$P_1=1/2$。对于长度为n的子序列，恶意节点对其成功伪造的概率是$P_2=(1/2)^n$。进一步地，由于 Center 是在参与者交换子序列完成后再公布正确的测量基序列，在此之前恶意节点并不能得到原始密钥的任何有用信息，这意味着由r个恶意节点共同产生伪造子序列只能增加错误率，此时成功伪造$r\times n$个粒子的概率为$P_3=P_2^r=(1/2)^{nr}$，随着r和n的增加，这个概率趋于 0。因此，本文提出的协议能抵抗内部恶意节点的伪造攻击。

Center 攻击：Center 在协议中扮演着重要的角色，但也可能成为潜在的攻击者。协议最终的共享密钥的构成，不仅包含 Center 生成的原始密钥，还融合了参与者在协议执行过程中各自随机生成的密钥成分。因此，如果 Center 不严格遵守协议规定的操作流程，参与者将无法达成一致的共享密钥，同时，Center 也无法从中获取任何有用信息。Center 若试图获取参与者协商的最终共享密钥，其机会仅限于参与者之间交换插入随机生成密钥的子序列的阶段。然而，参与者之间的子序列交换行为并不经过 Center，Center 若要发起攻击，其行为模式等同于外部攻击者。正如后续安全性分析中所证明的，本协议具备抵抗此类外部攻击的能力。但是，如果 Center 利用参与者在 Center 处注册的秘密身份码发起冒充攻击，目前的协议设计尚不能有效防御。因此，在未来的研究工作中，如何设计出更为完善的协议，以确保即使在 Center 不诚实的情况下，也能实现安全可靠的多方量子密钥协商值得探索。

4.2 外部攻击

IR 攻击：Eve 是一个窃听者，为了获取机密，他在 Step 4 或 Step 6 中拦截机密。Eve 截取序列$|M_i'\rangle$，同时将自己准备的序列发送给参与者。Eve 猜出 1 个粒子的概率是$P_4=1/4$，猜出n个粒子的概率是$P_5=(1/4)^n$，随着n的增加，概率接近于 0。除此之外，进行窃听检测时，对于一个粒子，Eve 使用正确制备基的概率是$1/2$，参与者得到错误测量的概率是$1/2$；Eve 使用错误制备基的概率是$1/2$，参与者得到错误测量的概率是$1/2$。参与者得到错误测量的平均概率是$P_6=(1/2)\times(1/2)+(1/2)\times(1/2)=1/2$，参与者放弃共享，Eve 窃听失败。

IMR 攻击：Eve 接收序列$|M_i'\rangle$并进行测量。测量后，将序列重发至参与者。分析考虑

被测序列中的一个粒子，如果真实的序列测量基与Eve的选择相同，Eve将获得序列测量基，这意味着 Eve 将获得一个粒子，概率是 $P_7 = 1/2$ 。然而，当 Eve 猜错了测量基，就会制备错误的粒子发给参与者，这个概率也是 $1/2$ 。Eve 无法区分密钥粒子和诱饵粒子，他猜出所有诱饵粒子测量基的概率趋近于 0，参与者会放弃此次密钥协商，因此 Eve 无法获得有用的密钥信息。

EM 攻击：在标准的纠缠测量攻击中，Eve 的目标是设计一个联合酉算符 U_E ，使其作用于传输的 LIOP 态粒子（系统 S）和 Eve 的辅助粒子（系统 E），从而在 S 和 E 之间建立纠缠关系，使得演化后的联合态为：$U_E|\psi_S\rangle|0_E\rangle \to \sum p_i|\psi_{S_i}\rangle|e_{E_i}\rangle$，其中，$|\psi_S\rangle$ 是传输的 LIOP 态，$|0_E\rangle$ 是 Eve 辅助粒子的初始状态，$|\psi_{S_i}\rangle$ 和 $|e_{E_i}\rangle$ 分别是系统 S 和 E 可能的后继状态，p_i 是概率幅。LIOP 态的局部不可区分性意味着，即使 Eve 获得了部分 LIOP 态粒子，也无法通过 LOCC 完全区分不同的 LIOP 态。更重要的是，任何试图区分 LIOP 态的操作，都必须是全局性的操作，这与 EM 攻击中 Eve 通常采用的局部操作相矛盾。此外，LIOP 态的子系统之间没有纠缠，Eve 试图引入纠缠的操作，在协议诱饵态检测步骤能够有效地检测到这种状态的改变。在本文协议中，为了成功进行 EM 攻击，Eve 需要截获所有参与者的粒子进行纠缠操作，这大大增加了攻击的复杂性和难度。

表 1 现有相关协议和本文提出协议的比较

Table 1 Comparison of existing related protocols and the protocol proposed in this paper

协议	量子资源	纠缠	身份认证	内部攻击成功的概率	外部攻击成功的概率
[3]	单光子	无	无	合谋攻击：$(3/4)^n$	IR 攻击：$(1/2)^n$
[4]	Bell 态、GHZ 态	有	相互认证	中间人攻击：$(1/4)^n$	冒充攻击：$(5/8)^n$
[5]	Bell 态	有	相互认证	伪造攻击：$(3/4)^n$	-
[6]	W 态	有	相互认证	-	IMR 攻击：$(1/3)^{2n}$
本文	乘积态	无	相互认证	伪造攻击：$(1/2)^n$	IR 攻击：$(1/4)^n$

4.3 效率分析

本文提出的协议效率随参与者数量的增加而降低。量子密钥协议的效率为 $\varepsilon = \frac{b_s}{q_t + b_t}$，其中 b_s 是参与者之间建立的共享密钥比特数，q_t 是传输的量子比特数，b_t 是传输的经典比特数[24]。最终共享密钥的总比特数也是 mn，因此，$b_s = mn$。量子通信发生在多个步骤中，在 Step 2 中，Center 生成了 p 个编码序列，每个序列包含 n 个量子态，每个量子态有 p 个量子比特，因此传输的量子比特总数为 $p \times pn$。Step 6 中，参与者交换的子序列包含的量子比特数是 $n + (m+1)n = (m+2)n$，传输的量子比特总数为 $p \times (p-1) \times (m+2)n$。Step 7 中，参与者将其他参与者的身份码发送给 Center，传输的量子比特总数是 $p \times (p-1) \times n$。因此，$q_t = p \times pn + p \times (p-1)(m+2)n + p \times (p-1)n = p \times n\left[p(m+4) - m - 3\right]$。本文方案除宣布粒子的位置和测量基外无其他经典比特传输，$b_t = 0$。因此，量子比特效率为

$$\varepsilon = \frac{mn}{p \times n\left[p(m+4) - m - 3\right]} = \frac{m}{p\left[p(m+4) - m - 3\right]} \tag{8}$$

5 结束语

本研究提出一种基于局部不可区分的正交乘积态和量子秘密共享过程的多方量子密钥协商协议，可支持物联网网络中的安全数据交换。该协议采用局部不可区分的正交乘积态作为量子态编码载体，避免了传统方案中使用纠缠资源制备成本高以及维护困难等问题，提出的协议只需发送和测量量子态，就能轻松实现多方参与者的密钥协议。安全性分析表明，本文提出的协议能够抵御来自内部恶意节点的伪造攻击，而局部不可区分的正交乘积态的性质证明了本文提出的协议能够安全地抵御现有的外部攻击。尽管如此，在现有量子通信基础设施中部署该协议仍面临挑战：量子通信基础设施（包括卫星量子密钥分发系统与光纤网络）的建立和维护需要高额成本；当前量子通信存在显著的距离限制，导致覆盖范围受限。未来需要解决上述实际部署难题，以促进量子密钥协商协议在现有量子通信基础设施中的广泛应用。

参考文献：

[1] Sihare S R. Dynamic multi-party quantum key agreement protocol based on commutative encryption[J]. International Journal of Theoretical Physics, 2022, 61(9): 242.

[2] Yang H, Lu S, Zhou Q, et al. Efficient single-state multi-party quantum key agreement[J]. Quantum Information Processing, 2024, 23(4): 150.

[3] Cai B B, Guo G D, Lin S. [J]. International Journal of Theoretical Physics, 2017, 56: 1039-1051.
[4] Wu Y T, Chang H, Guo G D, et al. Multi-party quantum key agreement protocol with authentication[J]. International Journal of Theoretical Physics, 2021: 1-12.
[5] He Y F, Pang Y, Di M. Mutual authentication quantum key agreement protocol based on Bell states[J]. Quantum Information Processing, 2022, 21(8): 290.
[6] Yi H M, Zhou R G, Xu R Q. Semi-quantum key agreement protocol using W states[J]. International Journal of Theoretical Physics, 2023, 62(10): 212.
[7] Li G D, Cheng W C, Wang Q L, et al. A measurement device independent multi-party quantum key agreement protocol with identity authentication[J]. Quantum Information Processing, 2023, 22(12): 443.
[8] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing[J]. Theoretical computer science, 2014, 560: 7-11.
[9] Bennett C H. Quantum cryptography using any two nonorthogonal states[J]. Physical review letters, 1992, 68(21): 3121.
[10] 石飞. 量子非局域性与多体纠缠[D]. 安徽:中国科学技术大学,2022.
Fei S. Quantum nonlocality and multi-body entanglement[D]. Anhui: University of Science and Technology of China, 2022.
[11] Bennett C H, DiVincenzo D P, Fuchs C A, et al. Quantum nonlocality without entanglement[J]. Physical Review A, 1999, 59(2): 1070.
[12] Yu S, Oh C H. Detecting the local indistinguishability of maximally entangled states[J]. arXiv preprint arXiv:1502.01274, 2015.
[13] Guo G P, Li C F, Shi B S, et al. Quantum key distribution scheme with orthogonal product states[J]. Physical Review A, 2001, 64(4): 042301.
[14] Ghosal P, Ghosal A, Ghosh S B, et al. Locally unidentifiable subset of quantum states and its resourcefulness in secret password distribution[J]. Physical Review A, 2024, 109(5): 052617.
[15] Bej P, Jayakeerthi V. A secure quantum key distribution protocol using two-particle transmission[J]. arXiv preprint arXiv:2403.13634, 2024.
[16] Fu S J, Zhang K J, Zhang L, et al. A new non-entangled quantum secret sharing protocol among different nodes in further quantum networks[J]. Frontiers in Physics, 2022, 10: 1021113.
[17] Bai C M, Liu L, Zhang S. Verifiable quantum secret sharing scheme based on orthogonal product states[J]. Chinese Physics B, 2024, 33(7): 070302.
[18] Lin M M, Xue D W, Wang Y, et al. A new quantum payment protocol based on a set of local indistinguishable orthogonal product states[J]. International Journal of Theoretical Physics, 2021, 60: 1237-1245.
[19] Jiang W, Zhuang J. An improved quantum payment protocol based on group signature without entanglement[J]. Modern Physics Letters A, 2024, 39(04): 2350199.
[20] Senthoor K, Sarvepalli P K. Theory of communication efficient quantum secret sharing[J]. IEEE Transactions on Information Theory, 2022, 68(5): 3164-3186.
[21] Kuo S Y, Tseng K C, Yang C C, et al. Efficient multiparty quantum secret sharing based on a novel structure and single qubits[J]. EPJ Quantum Technology, 2023, 10(1): 29.
[22] Singh P, Chakrabarty I. Controlled state reconstruction and quantum secret sharing[J]. Physical Review A, 2024, 109(3): 032406.
[23] Xu G B, Wen Q Y, Qin S J, et al. Quantum nonlocality of multipartite orthogonal product states[J]. Physical Review A, 2016, 93(3): 032341.
[24] Cabello A. Quantum key distribution in the Holevo limit[J]. Physical Review Letters, 2000, 85(26): 5635.