**东南大学-中国移动研究院联合创新中心**

**无线密钥生成关键技术研究**

**联合研发课题指南**

**中国移动通信有限公司研究院**

**2024年3月**

1. **课题基本信息**

|  |  |  |
| --- | --- | --- |
| 课题名称 | | 无线密钥生成关键技术研究 |
| 课题所属合作领域 | | 网络空间安全与区块链 |
| 课题周期 | | 课题任务合同书签订起——2025年12月31日 |
| 预期成果类型 | | ☑原型样机 □仿真平台 □软件/算法模型 □标准 □白皮书 ☑技术方案或研究报告 ☑专利  ☑论文 □论著 □其他 |
| 课题分级 | | □重大课题 ☑ 重点课题 □ 小而美课题 |
| 课题分类 | | ☑技术引领类 □平台验证类 |
| 中国移动课题联系人信息 | 课题接口人 | 程叶霞 |
| 联系电话 | 18701538566 |
| 电子信箱 | chengyexia@chinamobile.com |

1. **课题研究背景**

基于无线物理层加密的量子密钥无线分发方法，采用无线信道的随机性、互易性、去相关性等特点，在量子密钥应用终端与基站或WiFi热点之间的无线通信信道中产生具有信息论安全性的对称密钥，对分发的量子密钥进行加密传输保护，从而实现空口数据信息论级安全传输，解决量子密钥在“最后一公里”安全分发难题，为量子通信技术拓展QKD网络末端服务与应用范围提供策源技术。

针对无线物理层密钥技术，前期已开展了可行性研究，基于电脑形态的一对一的WLAN无线密钥生成原型系统、量子密钥分发原型系统，以及基于4G/5G的无线信道密钥生成技术，但是目前还存在一些问题。

其一，面向WLAN的无线密钥生成技术，原来仅仅适用一对一场景，而对于多用户、大规模的场景下无线密钥生成方法尚未涉及、技术路线不明确。其二，原来的原型系统是基于电脑形态，但是实际用户应用时，采用的形态为嵌入式平台、手机等终端形态。其三，面向4G/5G的研究限定在一对一单点场景的无线密钥生成，而针对无线物理层密钥技术与当前4G/5G通信协议融合以及现有安全机制融合的技术路线和方法尚未明确。

为解决上述问题，本期开展无线密钥生成关键技术研究，侧重在面向WLAN网络的多用户物理层密钥生成技术研究与验证，以及4G/5G下多用户物理层密钥生成技术及安全融合技术研究。

1. **研究目标及内容**

通过本课题，将实现以下目标：

本课题研究无线密钥生成关键技术，针对量子密钥“最后一公里”部署问题，通过进一步研究面向WLAN/4G/5G网络的物理层安全技术，利用无线信道的短时互易性，实现量子密钥的多用户、大规模分发。本课题从理论及工程角度证明量子密钥无线分发技术规模实施的可行性，为打造量子信息网络系统，构建量子应用服务体系提供终端侧的技术支撑。具体目标包括：

1. 面向WLAN网络的多用户物理层密钥生成技术研究，给出时分、空分的技术路线和技术方案；搭建基于嵌入式开发平台加WiFi芯片的物理层密钥技术验证系统，实现量子密钥无线分发；
2. 面向4G/5G通信网络，研究支持更多用户、更高频谱范围的多用户物理层密钥生成算法；将物理层密钥生成技术与4G/5G通信协议及现有安全机制融合，分析安全增量与实现代价，通过技术融合增强系统安全性，为用户提供更高级别的安全保护。

本课题的主要研究内容包括：

无线密钥生成关键技术研究的技术路线将围绕：面向WLAN网络的多用户物理层密钥生成技术研究及验证和4G/5G下多用户物理层密钥生成及安全融合技术研究两部分共3个任务展开。

任务1：面向WLAN网络的多用户物理层密钥生成技术研究及验证

a) 基于WLAN协议的多用户无线密钥生成前沿技术研究；

b) 移动环境下无线信道互易性增强技术研究；

c) 开发基于嵌入式开发平台加WiFi芯片的量子密钥无线分发系统;

d) 基于外挂WLAN芯片的多用户无线信道密钥生成算法研制及API开发。

任务2：4G/5G下多用户物理层密钥生成技术研究

a) 提出速率最大化的多用户物理层密钥生成方法，优化用户时频域资源分配，灵活适配多样化的通信场景；

b) 提出物理层密钥生成与4G/5G通信协议的融合方法，最小化密钥生成算法对通信协议造成的影响。

任务3：无线物理层密钥生成技术与4G/5G安全机制的融合技术研究

a）研究4G/5G安全协议与无线物理层密钥生成技术的兼容性；

b）提出物理层密钥在4G/5G安全机制中的融合方法，通过技术融合增强系统安全性。

其中上述内容的任务3部分由中国移动研究院研究人员开展研究，任务1和任务2部分由合作团队进行承担。

1. **预期成果及验收要求**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **成果名称** | **数量** | **类型** | **交付时间** | **考核指标** | **是否为核心成果** |
| 1 | 基于嵌入式开发平台加WiFi芯片的量子密钥无线分发系统 | 4 | 原型样机 | 2024年11月2套；  2025年6月2套 | 原型支持嵌入式开发平台加外挂芯片的量子密钥无线分发功能；同时，无线密钥成码率>1K比特/秒；无线密钥随机性测试通过率>10项(GM\_T 0005-2021标准)；量子密钥分发速率>1K比特/分钟 | 是 |
| 2 | 无线密钥生成技术方向论文 | 6 | 论文 | 2024年11月2篇；  2025年11月4篇 | 接收或发表，EI或SCI，其中移动一作或者通作至少3篇，其余论文移动署名前三 | 否 |
| 3 | 无线密钥生成技术相关专利 | 6 | 专利 | 2024年11月2项；  2025年11月4项 | 取得专利局申请受理通知书 | 否 |
| 4 | 《基于WLAN的多用户无线密钥生成技术研究报告》 | 1 | 研究报告 | 2025年11月 | 对所研究的内容和方法进行深入论述和展示；同时，针对移动环境下形成无线信道互易性增强技术方案 | 否 |
| 5 | 《面向4G/5G的多用户物理层密钥生成及安全融合技术研究报告》 | 1 | 研究报告 | 2025年11月 | 对所研究的内容和方法进行深入论述和展示；同时，针对4G/5G，形成整体解决方案及实现建议；针对6G，形成未来的展望方案及推进建议 | 否 |
| 6 | 《基于WLAN的无线密钥生成技术要求》 | 1 | 技术方案 | 2025年11月 | 对所研究及实现的内容和方案以技术要求的形式进行深入论述和展示 | 否 |
| 7 | 《面向4G/5G的多用户物理层密钥生成及安全融合技术要求》 | 1 | 技术方案 | 2025年11月 | 对所研究及实现的内容和方案以技术要求的形式进行深入论述和展示 | 否 |

1. **课题执行计划**

一、自课题任务合同书签订起-2024年12月，完成的任务和输出的成果：

1. 基于定制WLAN芯片的多用户无线信道密钥生成算法研究与验证；
2. 基于嵌入式开发平台加WiFi芯片的量子密钥无线分发系统2套（每套包含1台嵌入式开发平台和1部手机）；
3. 基于WLAN的多用户无线密钥生成技术研究报告初稿；
4. 面向4G/5G的多用户物理层密钥生成及安全融合技术研究报告初稿；
5. 基于WLAN的无线密钥生成技术要求初稿；
6. 面向4G/5G的多用户物理层密钥生成及安全融合技术要求初稿；
7. 输出无线密钥生成方向论文2篇；
8. 输出无线密钥生成相关专利2项。

二、2025年1月-2025年6月，完成的任务和输出的成果：

1. 基于WLAN的多用户无线密钥生成技术研究；
2. 4G/5G下多用户物理层密钥生成技术研究；
3. 无线物理层密钥生成算法与4G/5G通信协议的融合方法研究；
4. 基于嵌入式开发平台加WiFi芯片的量子密钥无线分发系统2套（每套包含1台嵌入式开发平台和1部手机）；
5. 输出无线密钥生成方向论文2篇；
6. 输出无线密钥生成相关专利2项。

三、2025年7月-2025年11月，完成的任务和输出的成果：

1. 基于WLAN的多用户无线密钥生成技术研究；
2. 无线物理层密钥生成算法与4G/5G通信协议的融合方法研究；
3. 无线物理层密钥生成技术与4G/5G安全机制的融合技术研究；
4. 基于WLAN的多用户无线密钥生成技术研究报告终稿；
5. 面向4G/5G的多用户物理层密钥生成及安全融合技术研究报告终稿；
6. 基于WLAN的无线密钥生成技术要求终稿；
7. 面向4G/5G的多用户物理层密钥生成及安全融合技术要求终稿；
8. 输出无线密钥生成方向论文2篇；
9. 输出无线密钥生成相关专利2项。
10. **合作团队与配套需求**

一、对合作团队的需求

1、教授3名、副教授5名，课题总投入96人月；

2、每年至少投入若干名研究生及以上学历的学生承担技术研究，课题总投入240人月。

二、对配套的仪器、设备、环境的需求

需要使用高性能计算机或服务器和相关测试仪表若干，用于完成模型设计、仿真模拟及测试。需要使用商用WiFi芯片模组搭建WLAN无线信道密钥生成系统并开展测试验证。

1. **知识产权要求**

本课题相关成果的知识产权要求如下：

1. 是否打算就课题成果发表论文：

□我方拟发表 □对方拟发表 ☑共同发表 □均不发表 □不确定

2、本课题所产生的课题成果（不含论文）知识产权归属为：

|  |  |  |
| --- | --- | --- |
| 成果列表 | 知识产权归属 | 成果形式 |
| 成果1：基于嵌入式开发平台加WiFi芯片的量子密钥无线分发系统（原型样机） | □归中国移动研究院独有  ☑双方共有 | □专利  ☑软件  □技术秘密  □集成电路布图设计  □其他 |
| 成果2：无线密钥生成技术相关专利 | □归中国移动研究院独有  ☑双方共有 | ☑专利  □软件  □技术秘密  □集成电路布图设计  □其他 |
| 成果3：基于WLAN的多用户无线密钥生成技术研究报告 | □归中国移动研究院独有  ☑双方共有 | □专利  □软件  □技术秘密  □集成电路布图设计  ☑其他 |
| 成果4：面向4G/5G的多用户物理层密钥生成及安全融合技术研究报告 | □归中国移动研究院独有  ☑双方共有 | □专利  □软件  □技术秘密  □集成电路布图设计  ☑其他 |
| 成果5：基于WLAN的无线密钥生成技术要求 | □归中国移动研究院独有  ☑双方共有 | □专利  □软件  □技术秘密  □集成电路布图设计  ☑其他 |
| 成果6：面向4G/5G的多用户物理层密钥生成及安全融合技术要求 | □归中国移动研究院独有  ☑双方共有 | □专利  □软件  □技术秘密  □集成电路布图设计  ☑其他 |

**注：知识产权说明以合同约定为准。**

**八、其他说明**

如无法顺利或及时获得定制芯片模组、开发资料和接口定义文件，课题组将基于能够完成手机外挂芯片的模组进行开发。