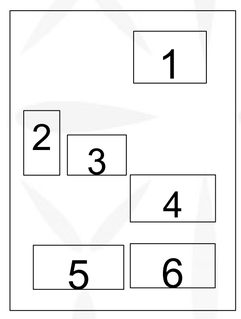
首届致远学术节
学生科研成果展示

基于量子随机数的远程安全控制系统及方法

孙轲 刘煜 指导老师：金贤敏

本项目提出一种基于量子随机数的一次一密远程加密控制方案，首次实现了对物联网通信系统的加密控制，为密码学中应用伪随机数向真随机数的革新提供了思路。



图例

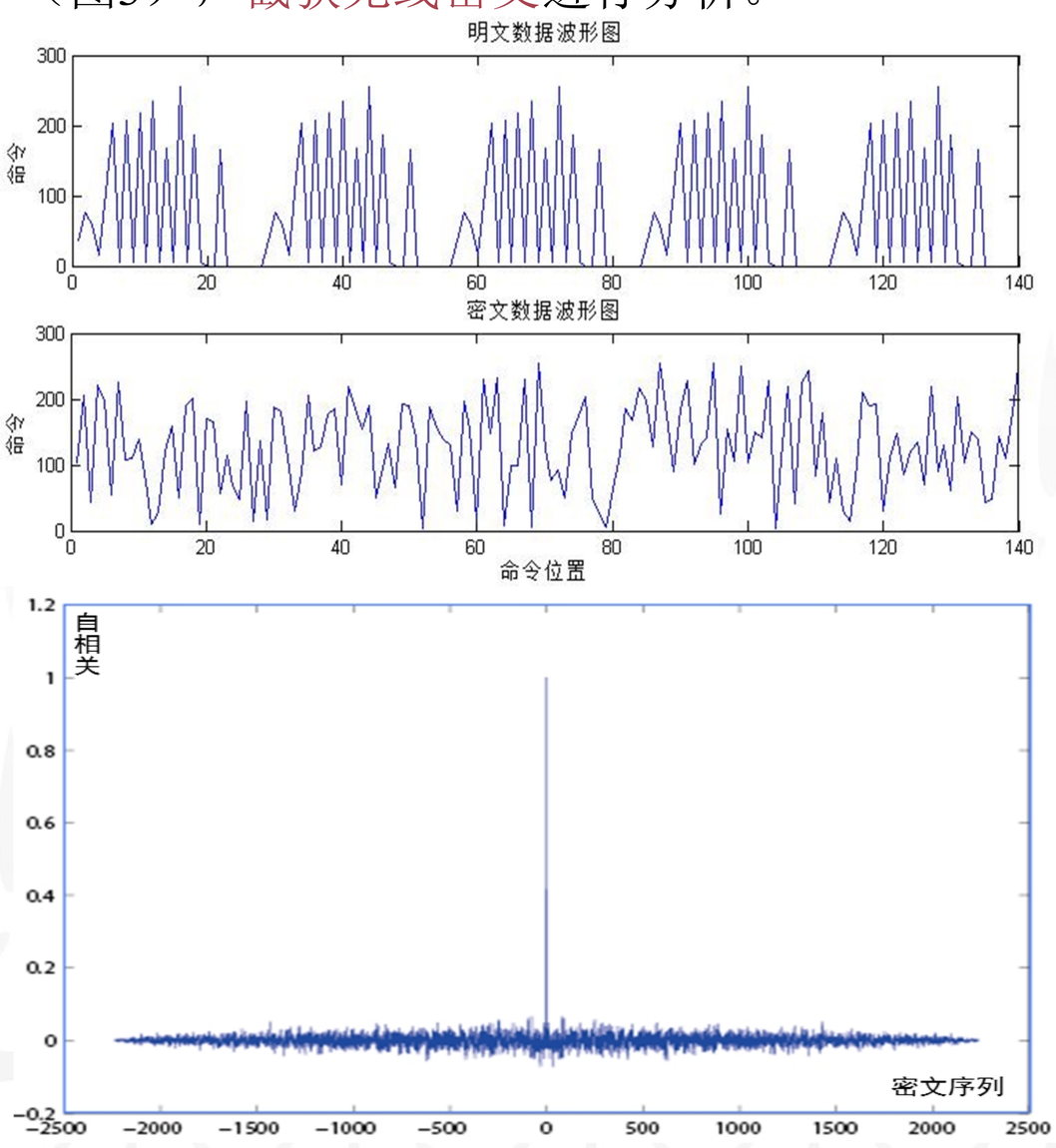
✦ 项目背景：

已有的量子真随机数的移动终端保密系统，保证了日常通信的绝对安全，但是仅限于移动互联网通信，目前没有类似将一次一密加密技术应用于远程安全控制的具体应用。

本课题致力于物联网远程控制领域的绝对安全，并在无人机上演示一次一密结合量子随机数的加密控制。

✦ 具体实现：

在无人机通信系统（图1）上增加密钥存储、密钥管理、加密、解密、密钥同步等模块。用量子随机数发生器（图2）产生量子随机数作为一次一密加密密钥。编写程序控制单片机（图3），截获无线密文进行分析。



✦ 数据分析：

加密前指令确定且重复，加密后杂乱无章，因此理论上完全不可破解(图4)。用NIST随机数测试对秘钥进行随机性检验(图5)，结果显示秘钥随机性良好。对加密后指令进行自相关性分析(图6)，结果更加验证了加密后指令的随机性。

检测手段	P值	检测结果	检测手段	P值	检测结果
频率检验	0.397	成功	Maurer的通用统计检验	0.053	成功
块内频数检验	0.104	成功	线性复杂度检验	0.903	成功
游程检验	0.039	成功	序列检验	0.039	成功
块内最长游程检验	0.683	成功	近似熵检验	0.362	成功
二元矩阵秩检验	0.626	成功	累加和检验	0.363	成功
离散傅里叶变换检验	0.326	成功	随机游动检验	0.221	成功
非重叠模块匹配检验	0.831	成功	随机游动状态频数检验	0.314	成功
重叠模块匹配检验	0.445	成功			

✦ 总结展望：本项目首次实现了基于量子随机数的一次一密远程安全控制，理论上完全不可破译。同时预言了量子随机密钥的长度可以远小于信息本身长度，结合量子密钥分发，具有重大应用价值！

个人信息：孙轲（物理学）
邮　　箱：ke.sun621@outlook.com