**利用实时时钟技术的加密算法设计**

信息与通信工程学院信息对抗技术专业 13050541班江润东

指导教师：张丕状

# 前言

随着电子设备的广泛使用，信息安全成为了现代社会的重要一环。信息安全关系到了每一个人，无论是在日常生活方面还是在工作和学习方面，无论是在常规的门禁系统还是关系到财产安全的银行系统，我们都需要安全的信息环境。我们经常能看这样的新闻：银行ATM自动提款机门口被装上了复制磁条的设备，然后输入密码的键盘上方被安装上了摄像头，这样不法分子就能复制出受害者的银行卡，并通过拍摄到的密码窃取受害人的财务；汽车的遥控信号被不法分子复制，然后等车主走远后重新将信号发出，打开车门盗取车内财物。保证信息安全已经成为一个研究热点。

通常采用的保证信息安全传输的做法就是进行加密传输，但是传统的加密通信方法通常使用固定的密钥对数据进行加密，容易被收到攻击，就像前面讲到的银行卡和汽车遥控的例子一样。目前，RFID技术被应用到汽车开锁领域，用户不需要拿出钥匙就能解锁汽车[1]；还有使用了双向通信和跳频通信方式的汽车开锁方式[2]。本文针对汽车开锁信号易被重放这一情况，设计了一种利用实时时钟的加密算法，使用AES算法，利用动态密钥对信息进行加密和解密，从而避免了遭受到重放攻击。

针对信息安全问题，本文提出一种使用动态密钥的安全技术方案，研究了基于时间同步技术的动态密钥产生方法及其时间的同步技术。

# 2．动态密钥

## 2.1 动态密钥的产生

密钥是在明文转换为密文或将密文转换为明文的算法中输入的参数，在加密算法中，使用密钥对明文进行加密或者对密文进行解密。传统的加密或者解密都使用固定的密钥，这就出现了一些安全隐患。以前面的汽车开锁为例，汽车钥匙发送的遥控的信号很容易被周围的设备接收到，一旦有人接收到信号并将信号重新发送，就也能打开汽车锁。针对汽车这种容易遭受到重放攻击的情况，本文提出使用动态密钥对数据进行加密和解密。即每隔一段时间就更换一个密钥，使得攻击者无法进行重放攻击。

动态密钥的产生是本文的重点。在本设计中动态密钥的产生需要满足以下特点：1.无规律性；2.低重复率。无规律性是指产生的相邻两个密钥或者多个密钥没有规律，攻击者就算通过唯密文攻击获得了密钥，也无法知道下一次加密或者解密时将采用的密钥是什么。重复率指相邻两次产生的密钥的相同位上的重复比例，低重复率就是相邻两个密钥的对应位相同的个数少。低重复率能够极大地提升攻击的难度。

本文中动态密钥的产生方法是将时间通过一个非线性线性系统，该系统的输出作为加密和解密的动态密钥，如图1所示。由于动态密钥需要具有无规律性和低重复率，所以想到利用时间和随机数来产生动态密钥。在本文中动态密钥的产生方法为：将当前时间乘以一个随机数，然后将结果扩展或者压缩至16位，把该16位的结果作为密钥。



图1 动态密钥的产生

使用MATLAB对该动态密钥产生算法进行分析。首先以当前时间为2017年5月23日18时46分37秒为例，取，在以后的1000秒中模拟在每10秒的时间间隔中使用该算法产生动态密钥，并对密钥的变化率和产生的随机性进行分析，其中随机数使用rand()函数产生。这是重复周期很长的伪随机数产生函数，在使用中基本可以认为其产生的是随机数，而且在动态密钥的产生中还添加了时间因素，所以本设计中动态密钥基本可以认为是不重复的。分析结果如图2和图3所示。图2中在不同的时间内产生的动态密钥都不相同,而且密钥的分布几乎是随机的，没有两个完全一样的密钥。而且所产生的动态密钥几乎没有任何规律可言。

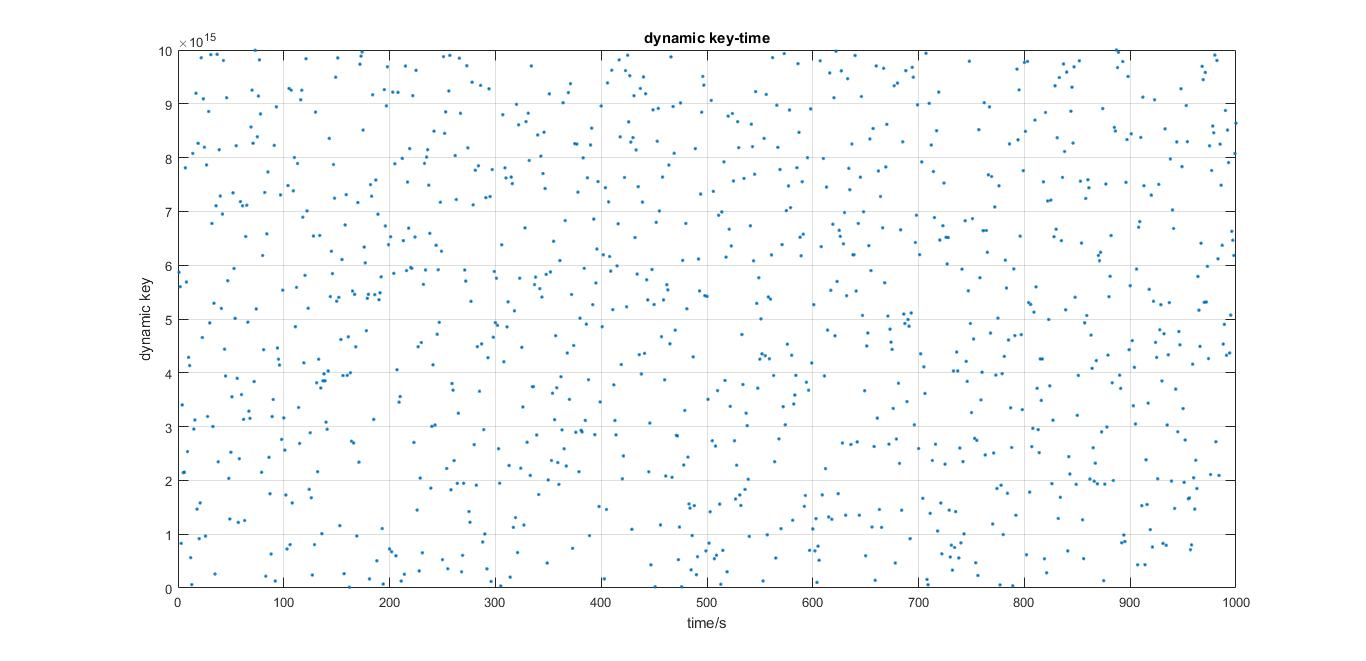


图2 模拟时间产生动态密钥的散点图

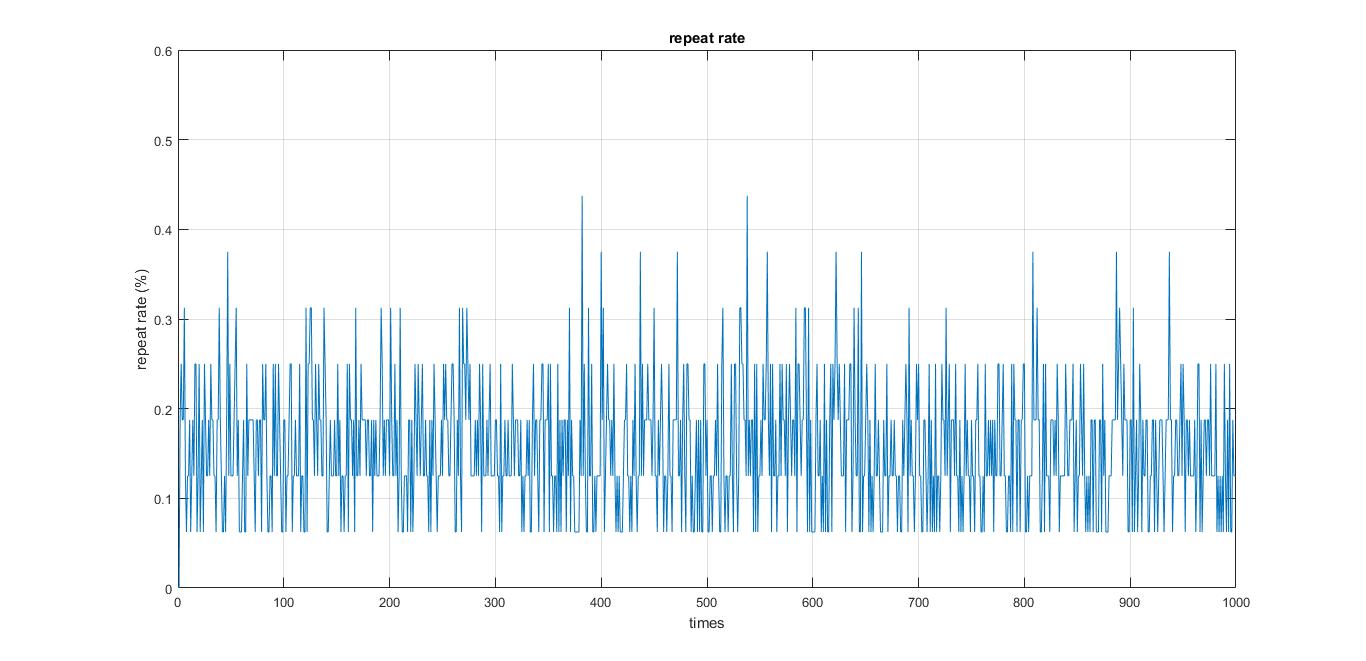


图3 动态密钥的重复率

图3中在1000次中重复率超过40%的只有两次，其他时候的重复率大多稳定在，也就是说在每次产生的16位密钥中最少只有9位与原来的密钥不同。在大部分情况下会有14位与原来的密钥不同。

所以，可以认为该动态密钥产生算法产生的动态密钥是安全的。

## 2.2 动态密钥的时间同步

利用实时时钟产生动态密钥进行加密和解密对时钟的同步有较严格的要求，虽然加密方和解密方的时间不可能完全一致，但是若加密方和解密方之间存在较大的时间差，则无法正确进行解密，从而也就无法正常进行通信。所以需要对加密方和接收方的时间进行校准。

时钟同步的方法有很多种，对于手表来说，可以通过地面设置的授时中心通过发送的电波进行时间同步；对于汽车导航仪和通信基站，通常使用GPS卫星对设备进行时间校准；计算机和手机则通常使用互联网进行时间同步。后两种时间同步方式为目前较为常用的方式，特别是使用GPS进行时间校准，基本不受地理环境的限制，只要在室外就能接收到时间，从而进行校准。

# 3．设计实现与验证

本文针对银行卡和车辆被盗等信息安全问题，研究了基于动态密码和双向信息验证等技术在信息安全的工作机理，并设计了一个简易的验证系统，该验证系统分为用户设备和终端设备。用户设备和终端设备都以STM32F103系列单片机最小系统作为基础、使用时钟模块作为产生动态密钥的时钟来源、GPS模块作为时间校准的设备，以确保在时钟模块产生误差时能够及时校准时间。此外用户设备还包含了按键模块和无线收发模块，终端设备还包含了GSM模块和OLED显示屏。

用户端和接收端使用GPS进行时钟同步，约定每隔十秒就重新产生一个密钥。在使用时，1.用户设备先产生一个使用动态密钥加密的请求信号；2.终端设备接收到信号后使用相同的密钥对信号进行解密，并对解密后的信息进行分析，在确定这是一个请求信号后，向用户设备发送一个使用动态密钥加密过的确认信号；3.同步骤2类似，用户设备确认无误后向终端发送一个建立连接的信号；4.当上面所有步骤都完成后，终端设备向用户手机发送验证码；5.用户在收到验证码后通过按键模块键入验证码，验证码使用动态密钥加密后通过无线模块发送；6.用户端在接收到后使用动态密钥进行解密，并对验证码进行比对，比对无误后进行解密，并在OLED屏幕上显示出解锁字样。

# 4．总结

使用利用实时时钟技术的加密算法能够解决银行卡被复制后窃取用户账户余额、汽车遥控开锁信号被复制并重放的问题。同时，该算法系统设计也为解决与此相类似类的问题提供了一种思想。

参考文献

[1] 胡威.基于RFID技术的汽车门禁系统设计[D].浙江理工大学,2015.

[2] 王立峰,陈旭东,陶乐文等.基于RF微功率芯片的智能汽车遥控系统[J].自动化技术与应用,2011,30(6):46-50.DOI:10.3969/j.issn.1003-7241.2011.06.013.