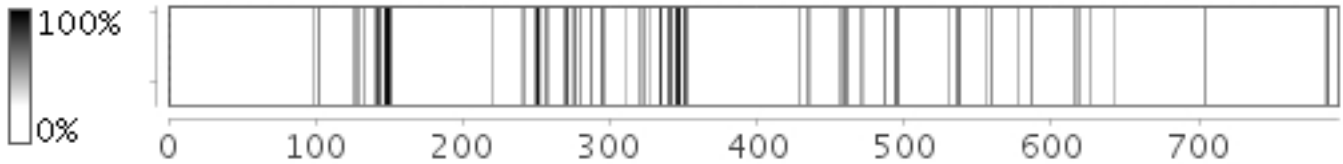
PaperPass专业版检测报告
简明打印版

比对结果（相似度）：
总　体：19 % *（总体相似度是指本地库、互联网的综合比对结果）*
本地库：18 % *（本地库相似度是指论文与学术期刊、学位论文、会议论文数据库的比对结果）*
期刊库：12 % *（期刊库相似度是指论文与学术期刊库的比对结果）*
学位库：15 % *（学位库相似度是指论文与学位论文库的比对结果）*
会议库： 3 % *（会议库相似度是指论文与会议论文库的比对结果）*
互联网：6 % *（互联网相似度是指论文与互联网资源的比对结果）*

编　号：593CF49B869FAZSWU
版　本：专业版
标　题：基于实时时钟技术的加密算法设计
作　者：江润东
长　度：24700 字符(不计空格)
句子数：794句
时　间：2017-6-11 15:43:23
比对库：学术期刊、学位论文（硕博库）、会议论文、互联网资源
查真伪：http://www.paperpass.com/check

句子相似度分布图：



本地库相似资源列表（学术期刊、学位论文、会议论文）：
1. 相似度：5％篇名:《EPON中数据安全性的研究》
   来源：学位论文 河南理工大学 2010 作者:李宗杰
2. 相似度：2％篇名:《银行身份认证系统设计与实现》
   来源：学位论文 山东大学 2012 作者:朱晓礼
3. 相似度：1％篇名:《AES算法研究》
   来源：学术期刊 《洛阳师范学院学报》 2011年8期 作者:曹晓丽 王爱强
4. 相似度：1％篇名:《新一代移动安全存储控制SoC芯片设计》
   来源：学位论文 天津大学 2013 作者:于哲
5. 相似度：1％篇名:《镇政府电子政务平台的设计与实现》
   来源：学位论文 厦门大学 2011 作者:周先进

6. 相似度：1％ 篇名:《基于被扰动的Lorenz系统和AES相结合的加密算法》
来源：学术期刊 《军民两用技术与产品》 2015年4期 作者: 李莉 方杰
7. 相似度：1％ 篇名:《关于Noekeon算法的研究》
来源：学术期刊 《网络安全技术与应用》 2015年11期 作者: 刘培鹤 田传凤 杨伟 张晓菲 何文才
8. 相似度：1％ 篇名:《基于SVO逻辑的网络安全协议形式化分析》
来源：学位论文 贵州大学 2009 作者: 周鹏
9. 相似度：1％ 篇名:《基于数据库水印的电子商务安全研究》
来源：学位论文 湘潭大学 2011 作者: 毛新清
10. 相似度：1％ 篇名:《基于中间件的分布式电子健康档案系统的研究与实现》
来源：学位论文 东华大学 2014 作者: 张鑫
11. 相似度：1％ 篇名:《H.264/MPEG AVC视频加密与四差分偏振键控通信方式》
来源：学位论文 上海大学 2007 作者: 王继东
12. 相似度：1％ 篇名:《基于xml的电子商务安全研究与应用》
来源：学位论文 贵州大学 2009 作者: 吴丽华
13. 相似度：1％ 篇名:《基于Objective-C的企业平台文件管理软件的设计与初步实现》
来源：学位论文 复旦大学 2012 作者: 施欣楠
14. 相似度：1％ 篇名:《基于AES的跳频序列技术研究》
来源：学位论文 西安电子科技大学 2015 作者: 田文智
15. 相似度：1％ 篇名:《G-AES算法》
来源：学术期刊 《密码学报》 2014年2期 作者: 张诗永 陈恭亮 范磊 李建华
16. 相似度：1％ 篇名:《SSL VPN中访问控制的研究以及教学实验的实现》
来源：学位论文 上海交通大学 2010 作者: 张宇
17. 相似度：1％ 篇名:《Instlink 客户端加密媒体信道的设计与实现》
来源：学位论文 西安电子科技大学 2012 作者: 张建伟
18. 相似度：1％ 篇名:《具有较高算法覆盖率的可重用模块》
来源：学术期刊 《北京电子科技学院学报》 2015年2期 作者: 王九林 夏潇 董秀则 茅方毅
19. 相似度：1％ 篇名:《AES算法的硬件优化实现及应用研究》
来源：学位论文 厦门大学 2014 作者: 郑行
20. 相似度：1％ 篇名:《电视机I2C总线控制器研究及实现》
来源：学位论文 电子科技大学 2007 作者: 李春川
21. 相似度：1％ 篇名:《基于文件系统过滤驱动的透明加解密技术实现》
来源：学术期刊 《广东工业大学学报》 2010年3期 作者: 周峰 凌捷 黄万民 袁肃蓉
22. 相似度：1％ 篇名:《基于AES的Flash加密实现》
来源：学术期刊 《电脑编程技巧与维护》 2014年22期 作者: 邹蕾
23. 相似度：1％ 篇名:《英语幽默语的话语分析》
来源：学术期刊 《科技信息》 2009年24期 作者: 李杰 马铁川 邱晓爱
24. 相似度：1％ 篇名:《基于无线网络WEP密钥的安全分析》
来源：学术期刊 《科技信息》 2009年24期 作者: 董屹 李佳 焦方源
25. 相似度：1％ 篇名:《AES算法的结构分析与优化实现种》
来源：学术期刊 《吉林大学学报（理学版）》 2008年5期 作者: 袁巍 胡亮 林宇 张云龙 黄瑞 李宏图
26. 相似度：1％ 篇名:《基于共振解调技术的便携式数据采集器研究》
来源：学位论文 北京工业大学 2008 作者: 逄涛
27. 相似度：1％ 篇名:《基于智能手机的图像加密算法研究》
来源：学位论文 华中师范大学 2015 作者: 王伟

28. 相似度：1％ 篇名:《个人数据安全保护系统设计研究》
来源：学位论文 电子科技大学 2011 作者: 王亚杰
29. 相似度：1％ 篇名:《数据加密在嵌入式系统升级中的应用》
来源：学术期刊 《工业控制计算机》 2014年4期 作者: 卢鹰斌
30. 相似度：1％ 篇名:《彩电基板自动检测调整系统的研究》
来源：学位论文 上海交通大学 2001 作者: 陆晾
31. 相似度：1％ 篇名:《基于MFC的AES可视化试验平台的设计与实现》
来源：学术期刊 《郑州轻工业学院学报（自然科学版）》 2011年6期 作者: 乔子芮 周彦伟

互联网相似资源列表：

1. 相似度：5％ 标题：《分组加密算法的研究和实现.doc》
http://max.book118.com/html/2015/1111/29157521.shtm
2. 相似度：2％ 标题：《银行身份认证系统设计与实现》
http://www.docin.com/p-789382135.html

全文简明报告：

毕业设计说明书

基于实时时钟技术的加密算法

设计

学生姓名： 学号： 信息与通信工程学院

1305054145

江润东

学 院： 信息对抗技术

专 业： 张丕状

指导教师：

2017年6月

基于实时时钟的加密算法

摘 要

{45％： 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国家安全方面，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

需要安全的网络环境。 {47%：传统的加密算法通常使用固定的密钥对数据进行加密，容易被收到攻击。} 本设计针对传统加密算法易于受到攻击的特点，采用了使用一次一密的基于实时时钟的加密算法，增加了攻击者攻击的难度。 该技术可以广泛应用于生活中的各个方面，比如汽车遥控和小区门禁系统等等。

本文首先分析了传统方式下通信加密传输的缺点，即易于遭受到攻击者的攻击，比如重放攻击、冒充终端的攻击等。 然后，本文对AES加密算法进行了简单介绍，并采用了一种基于实时时钟产生的动态密钥生成算法，利用该算法产生一个用于AES加密的动态密钥。 最后，以汽车遥控开锁为例，使用 STM32 F103单片机以及 GPS、GSM等模块设计了一个以实时时钟加密算法为基础的系统， 在保证用户端和终端时钟同步的情况下，约定使用相同的算法每十秒钟产生一个新的密钥， {44%：该系统能够抵挡攻击者的重放攻击以及攻击者冒充终端对用户的欺骗攻击。}

关键词： 动态密钥，加密，信息安全

Real Time Clock Based Encryption Algorithm Designing

Abstract

With electronic devices wildly being used, information security now has become one most important part of modern society. The security of information has influence every one of us, no matter in our daily life or some aspects related to national security; no matter entrance guard system or the bank system related to property security, what we need it a secure network environment. Traditional encryption algorithm use fixed secret key to encrypt data, and will easily be hacked. Aiming at the property that traditional encryption algorithm is very easy to be attacked, this design arises an encryption algorithm that use different key every time, which improves the difficulty of attacking for attackers. This algorithm can be used in every aspects of our daily life, such as car remote control and community access control etc.

This essay first analysis the disadvantages of traditional communication encryption, namely, it is very easy to be attacked, such as reply attack, defraud the terminal and then cheat the users, etc. Then, there is a brief introduce of Advantage Encryption Standard, adapting a dynamic key generation algorithm which is based on real time clock. Finally, use car remote control as an example, using STM32 F103 series MCU as well as GPS module and GSM module to design an encryption algorithm based on real time clock. Guaranteeing user device and terminal device have the same time, both the user device and terminal device arrange to use a same algorithm to generate a same dynamic key every ten seconds. This system can resist reply attack and attack that implement by attacker who fake the terminal device to cheat users.

Keywords: Dynamic keys, Encryption, Information Security

{63%：中北大学2017届毕业设计说明书}

目 录

第一章 绪论

1.1 研究背景和意义

{54%： 随着现在科技的进步以及信息化程度的越来越高，人们对于计算机以及计算机网络的依赖程度越来越

高，｝｛46％：各类电子产品已经渗透进了我们生产生活中的各个领域，成为现代社会中不可或缺的一部分。｝｛44％：但是随之而来的是各种安全问题，黑客程序、邮件炸弹、远程侦听、病毒等成为我们必须面对的问题[1]。｝｛51％：近几年发生的美国“棱镜门”事件使人们再一次意识到信息安全的重要性，｝“棱镜门”事件揭露了信息安全的严峻形势，如何保证机密信息不受到黑客的入侵已经成为现在信息化社会健康发展所必须要考虑的重要议题[2]。

｛71％：信息加密就是把人们能够读懂的消息变化成不易被读懂的消息从而达到使窃听者无法理解消息的内容同时又能让合法用户把变换的结果还原成能够读懂的消息[3]。｝｛46％：密码技术能够提供保密性、完整性和不可否认性的特点，还能提供访问控制、身份认证等安全服务[4]。｝

本设计是基于实时时钟的加密算法。 传统的加密算法使用固定的公密钥和私密钥，在明文不发生改变的情况下加密产生的密文也是固定的，能够实现对数据的加密，但是在消息的传递过程中容易受到攻击。 比如在使用有线传输的情况下架设空明线或者使用特定设备作为中继便可对密文进行复制， 同理，在无线传输过程中密文也容易被窃取和复制，攻击者可以轻易实施重放攻击。 此外，攻击者可以通过冒充用户来欺骗终端或者冒充终端来欺骗用户，进而进行自己的下一步计划。 ｛43％：基于时间的加密算法能够有效抵抗攻击者的重放攻击、穷举等攻击。｝

本设计以时间和密码共同作为解锁的明文，密码由用户保存，时间则存在于硬件当中， 用户设备与服务设备共同约定一个时间，只有在用户提供的密码和时间与服务设备中所保存的密码和服务设备中的时间相一致的时候才能认定用户是其本人。 本设计的意义在于，即便硬件设备被攻击者盗取，攻击者也无法使用；｛42％：攻击者在仅仅复制出硬件而不知道密码的情况下也无法正常使用；｝在攻击者仅仅复制出硬件而且已知用户密码的情况下，攻击者也无法正常使用，因为硬件内置加密电路，在仅仅存在硬件的情况下是无法使用的。 本设计可以广泛运用于安全级别较高的地方，比如银行卡、小区的门禁系统以及一些身份认证系统。 总的来说，这是一种安全的加密技术[3][4]。

1.2 相应技术及其发展

基于实时时钟的加密算法实际上是一种信息安全策略，它能够保证在身份认证中的安全、数据传输的安全和访问控制中的安全等。 其中，它包含了信息对抗的策略以及思想，从攻防的角度上对传统的技术进行完善。

｛44％：信息在传输的过程中很容易受到攻击，从而导致信息的泄露。｝从防守的角度来看，出现了将信息转化成别人看不懂的信息再传输再转换成别人能看懂的信息的密码学[5]； 出现了将信息在不同时间从不同的频率发送出去的捷变频技术。 从进攻的角度来看，出现了捕获发送方信号再冒充发送者使用捕获的信号欺骗目标的重放攻击； 出现了在传输线路上通过接入或侵入中继设备的中继攻击等。 ｛52％：简单地说，防守就是保护数据的可用性保密性和完整性，攻击就是破坏数据的可用性、保密性、完整性。｝

｛43％：早在公元前1世纪就出现了最早的单字母代换密码——凯撒密码；｝｛57％：公元9世纪，通过分析密文字母符号出现的频率来破译密码的技术出现；｝｛46％：在第二次世界大战初期，德国使用了一种命名为“恩尼格玛”的密码机，能够产生220亿种不同的密钥组合[6]；｝｛59％：1977年美国政府宣布DES算法为联邦资料的处理标准，并授权在非密级政府通信中使用，之后该算法便在国际上广泛流传开来[7]；｝｛50％：2001年11月26日美国国家标准与技术研究院在FIPS PUB 197上发布高级加密标准，用来替代原先的DES[6]；｝现在的加密技术有很多比如基于数学难题的RSA、ECC等，以及MD5、SHA-3、SHA-128等等，这些技术被广泛运用于银行系统、互联网系统、访问控制、身份认证等众多领域。 ｛49％：1993年， May首次提出 TRE基于时间释放的加密技术，这是一种由发送者指定未来特定解密时间的密码原语，｝｛86％：其所具备的时间相关特性在许多具有时间敏感性的

现实应用场景如电子投标、分期付款、在线考试、电子机密档案等均有着十分重要的应用价值[8][9]。 }

在对信息进行攻击方面，早期的主机与用户之间、用户与用户之间使用有线的方式进行联络， 其中就存在许多泄密漏洞，攻击者可以通过架设空明线对电话内容窃听[10]。 在第二次世界大战中无线电技术广泛使用，通过架设天线收取目标频率的信息再通过密码学的方法对信息解密的技术从而获取情报的技术也运用广泛。 随着现在技术的发展，以及通信线路深埋地下，通过搭线窃取的方式变得困难，但是近年来在移动通信上面出现了通过伪基站中继进行攻击方式[11]； 同时国外新出现了通过获取计算机周围声音信号分析出计算机CPU运行情况进而获取信息的方式； {51％：现在的通信安全问题将在第二章被详细讲述。 }

从防守的角度来看，为了抵御攻击者的攻击，各种系统需要使用各种方式来验证所登录的用户就攻击者本身。{92％：身份认证是信息系统根据设定的身份认证技术审查用户身份的过程，通过审查来确定该用户是否在该信息系统中具有某种资源的访问权限和使用权限。 } {100％：在真实世界中，验证一个用户身份的主要途径有以下三种方式：}

{58％：1) 根据用户所知道的信息再证明用户身份，即基于信息秘密的身份认证。 }

{66％：2) 根据用户所拥有的东西来证明用户身份，即基于信任物体的身份认证。 }

{69％：3) 根据用户的本身独一无二的体态特征来证明用户身份，即基于生物特征的身份认证，例如：} 人的指纹、笔迹、人脸、DNA等[12]。

{100％：在信息系统中，身份认证方式主要有：} {90％：基于密码的身份认证、基于地址的身份认证、基于生物特征的身份认证，基于交互通信协议的认证等[12]。 } {100％：在安全程度上，密码的身份认证方式安全程度不高，容易被盗取或破解。 } {100％：近年来银行互联网业务开展，UK认证和电子证书认证已经被渐渐认可。 } {88％：目前有关认证系统的实际应用有着多种相关的规范，如X.509，PKCS10，PKCS7，PKCS12等[13][14]。 }

{45％：总之，现在信息安全技术在不断提升，信息安全的防御体系也正在不断完善。 }

1.3 分析现在信息传输存在的问题

通常，信息传递的模型如下图1.1所示。 设备之间通过信道相互传送数据。 这样的信息传递方式在生活中广泛运用，比如日常生活中的电视遥控、汽车开锁、网上支付等各个方面。

图1.1 信息传递模型

一般在数据的传输的过程中需要对数据进行加密，以密文的形式传输数据，从而保证数据的安全性，但是即使使用了普通的加密算法，还是会存在一些问题。

在图1.2中，用户设备将数据加密后通过信道将加密后的数据传送给终端，终端解密后再对数据进行处理。

图1.2 通常带有加解密的传输模型

图1.2的传输模型看上去没有什么问题，但是如图1.3，如果有攻击者的设备处于同一信道当中， 能轻松得到

用户设备发送的加密数据，从而为攻击提供了可能的条件，比如使用暴力破解出用户数据，如果用户加密使用的是不安全的算法如 DES，{41%：则攻击者就很可能通过现有技术从密文中得到明文。} 而且，如果这样的传输模型使用在遥控开锁等方面的时候，攻击者就可以在信道中获得发送的数据包，然后进行简单的重放，就也能达到开锁的目的。

图1.3 攻击者对用户的攻击

就算用户设备与终端都使用了安全的加密算法如 ECC、AES、RSA等，攻击者依然可以利用从信道中得到的数据包进行一些攻击，比如说冒充用户设备对终端发送指令。如图1.4所示。用户向终端发送密文，终端接收到密文，嗅探信道的攻击者也收到密文，假如用户向终端发送的是汽车的开锁信号或者是账号的登录信息，则攻击者在想开锁或者登录用户账号的时候只需向终端发送接收到的就能达到目的。

图1.4 攻击者的攻击示意图

在现实生活中有很多这样的例子，比如说小区升降杆的遥控、早期的汽车摩托车的遥控开解锁，因为使用的是无线遥控装置，遥控信号向四周辐射，只要周围有一台攻击者的接收设备，通过将信号放大、滤波等一系列操作就能复制出控制信号。汽车和摩托车的开解锁也是同样的道理。

此外，除了对信道进行攻击之外，攻击者还可以通过对用户设备和终端进行攻击。比如，冒充用户设备或者冒充终端设备。通过复制用户设备获取用户信息的方式达到目的，比如在电视上常见的在银行 ATM前面加装特殊设备复制用户的卡片，再通过摄像头拍摄用户按下键盘的情况获取用户密码，从而达到盗取用户钱财的目的。还有一种方法就是冒充终端设备欺骗用户，得到用户的密码等信息，比如常见的在网络上制作一个假的购物网站，然后诱导用户进入这个假网站。{41%：在用户购买商品时，用户需要输入用户名、密码以及支付密码，假网站就会得到这些用户数据，} 然后找个理由说找不到服务器等借口使用户不起疑心，最后用骗取到的用户信息再冒充用户向终端提起一系列请求。

1.4 解决问题的方案

1.4.1 防止重放攻击的方法

若要使数据不被窃取和盗用，则用户端向终端发送的加密信息应该是每一次都不相同的，而且，加密的数据不容易被破解。常用的方法是在发送的消息中嵌入不能被复制的信息或者不怕被复制的元素，比如在加密的数据中嵌入时间信息。

图1.5 当前时间为t时的数据传输

如图1.5所示，用户设备和终端都添加上时间信息，在时间为 t的时刻，用户向终端发送包含了时间信息的密文，{45%：终端接收到密文，同理攻击者也接收到密文。} 攻击者在接收到窃取的数据包后立刻重放的做法是没有意义的，通常重放攻击是与事件有一定时间间隔才进行的，所以当攻击者在时刻通过信道向终端重新发送密文时，终端本机的时间已经变成了，存在的时间差，如图1.6所示，只有密文才能使终端进行正常操作，{44%：终端通过判断时间因素是否正确来确定是否接收此数据。} 从而达到抵抗重放攻击的目的。

图1.6 当前时间为时的数据传输

1.4.2 防止冒充用户设备和终端的方法

防止冒充用户设备和终端的方法最直接也是最有效的方法就是用户设备验证终端的真实合法性、终端设备验证用户设备的真实合法性。 比如通过握手协议来进行相互验证。 在用户设备和终端制作完成时就相互约定一套验证的方案，例如 TCP/IP协议中的三次握手协议，用户设备先发送一个包含控制位的数据包， 终端收到之后对数据包按照约定的方案进行处理再发回给用户端，用户端与协议内容比对，如果符合协议内容则说明终端时真实的，然后用户端再对收到的数据包按照协议处理后发回给终端，终端也进行一次判断，符合协议后说明用户端是本人， 然后再开始随后的通信。

当用户端和终端都采用带有数据处理功能的芯片后，对设备的复制就变得困难了， 仅仅对硬件进行复制很简单，但是芯片里的程序基本是无法被复制的，与仅有磁条的银行卡相比， 设备在硬件上就安全级别就高了一个层次。 其次，使用攻击者无法通过正常手段得到的信息作为验证信息，例如虹膜信息等。

1.5 本设计采用的方案

本文设计出一种方案，使得攻击者无法进行重放攻击，无法冒充用户设备和终端。 设计模型如图1.7所示。本设计算法选择对称密钥的AES算法。 AES算法在现在的条件下能够抵御已知的所有攻击。 {50％：在设计中，使用AES算法对用户设备和终端之间传输的数据进行加密。}

数据加密解密模型如图1.7所示，加密前，控制位、数据以及时间共同构成一个特定格式的数据帧，对数据帧加密后进行发送； 接收方接收到之后进行解密，并从中分离出数据、控制位和时间，从而进行下一步的处理。

图1.7 加密解密模型

首先用户端向终端提出连接请求之前先输入密码，再密码正确再向终端提出请求，然后用户端和终端相互验证如图中①所示； {41％：然后验证成功后终端向用户手机发送验证码短信如图中②所示；} 最后用户接收到验证短信后向通过用户设备向终端发送验证码如图中③所示。

图1.8 设计模型

{45％：从机（发送端）使用时间和序列号作为明文，使用和主机约定好的密钥对明文进行加密，} {44％：主机在接收到密文后，使用密钥对密文进行解密，使用与从机相反的算法对解密后的数据进行处理，} 得到时间和密码数据，再将时间与当前时间进行比对，密码与约定好的密文进行对比， {56％：若二者一致，则可认为身份认证成功，否则身份认证失败。} 在这种方法下，即使硬件丢失，在没有密码的情况下任何人都无法成功进行身份验证，其次，即便攻击者复制到了发送出的信号，进行重放攻击，在主从机时间的频繁变化下也将失败。 在主机身份认证成功后，主机向从机发送一个验证成功信号，从机在接收到该信号后再开始对主机进行进一步操作[15][16]。

在设计中，首先用户与终端在最初协商一个密码，即终端使用这个密码作为密钥对用户发来的数据进行解密，所以用户设备在最初使用时需要正确输入这个密码，否则终端将不能通过解密得到正确的数据。

然后用户端与终端使用约定的方式进行相互验证，验证的数据收发采用无线传输完成。 在传输的数据中加入实时时间，无论是用户设备还是终端，每次接收到数据包时都要将数据包中的时间与当前时间进行比对，从而有效防止重放攻击的发生。 在用户设备和终端相互验证的过程中，对于攻击者来说，攻击者无法得知用户端与终端相

互验证的协议， 所以也无法通过复制用户端与终端相连接或者冒充终端与用户端进行连接， 从而冒充用户设备和终端设备的情况就不会发生了。

{41%：最后，在验证成功后用户端再通过基于时间的验证码进行进一步验证，通过手机接收终端发送的验证码。} {42%：这样可以防止用户设备被攻击者窃取，而攻击者又知道用户密码的情况出现。} 因为设备丢失与手机丢失同时出现的情况出现概率很小，所以在设计中选择手机作为验证的一环。

1.6 论文组织结构

{65%：本文分为七章，各章内容简单介绍如下。}

第一章主要介绍了本文的研究背景以及发展现状，从总体上介绍了基于实时时钟加密的重要性和必要性以及作用等。

第二章分析了现在通信中消息传输时存在的一些问题和漏洞，如重放攻击、穷举等，以及对系统的设计思路和设计方案。

{42%：第三章则对AES加密算法的过程进行了简单的分析，包括每个步骤的计算方法。}

{48%：第四章讲述了硬件设计，包括硬件的组成和应用。}

{48%：第五章是软件设计的部分，讲述了设计的软件设计思路。} {58%：包括用户端和服务器端的程序流程和整个系统的工作流程。}

第六章是对系统调试的讲述。 即各个模块单独调试的方法以及现象和整个系统调试的过程和现象。

第七章是对全文的总结与展望。

第二章 AES算法

高级加密标准（英语： Advanced Encryption Standard，缩写： {91%：AES），在密码学中又称Rijndael加密法，是美国联邦政府采用的一种区块加密标准。} {100%：这个标准用来替代原先的DES，已经被多方分析且广为全世界所使用。} {97%：经过五年的甄选流程后，高级加密标准由美国国家标准与技术研究院（NIST）于2001年11月26日发布于 FIPS PUB197，} 并在2002年5月26日成为有效的标准。 {97%：2006年，高级加密标准已然成为对称密钥加密中最流行的算法之一[17]。}

图2.1 加密以及解密的流程

2.1 利用动态密钥产生AES密钥

{86%：在最原始的Rijndael算法中，分组的长度和密钥长度全都能被独立指定为128位、192位或者256位。} {72%：但是在AES加密算法中，分组的长度只能为128位，而密钥长度则可以使用128位、192位或256位中的任意一个。} {40%：需要加密的轮数与使用的密钥长度有关，使用的密钥长度不同，需要进行加密的轮数也不同，具体的密钥长度、加密轮数与分组长度之间的关系见下表。}

密钥长度（32bit）

分组长度（32bit）

加密轮数

AES-128

10

AES-192

12

AES-256

14

{63％： 表2.1 分组长度、密钥长度和加密轮数的关系}

{50％： 首先，将密钥K与输入的明文分组P划分为16个字节，记作和。} {80％： 一般来说，明文分组用以字节为单位的正方形矩阵进行定义，称之为状态矩阵。} {80％： 在算法的每一轮中，状态矩阵中的内容不断变化，最后输出的结果就是密文。} {59％： 状态矩阵中字节排列的顺序为从上到下、从左到右依次排列，如图2.2所示。}

图2.2 状态矩阵的变换

{46％： 明文按照列的方向排成的矩阵，矩阵中每一列有4个字节，总共32bit。} {59％： 在密钥扩展的算法中，使用密钥编排程序使得该密钥矩阵扩展成为一个由44个字组成的序列、…}

{65％： 序列最初的4个元素、、、称为原始密钥，用于加密运算中的初始密钥加运算。} {79％： 后面的40个字被分为10个组，每组4个字（128bit）分别参加10轮加密运算中的轮密钥加运算。}

2.2 密钥扩展算法简述

{56％： AES算法中的密钥扩展算法主要就是进行一系列的异或运算。} {54％： 首先，初始密钥按照列的顺序，被输入到一个矩阵中，这个矩阵中的每一列字节组成一个字，依次为、、、。} 它们构成了一个以字为单位的数组。 {77％： 随后，使用下面的算法使数组扩充40个新列，构成总共44列的扩展密钥数组。}

（1）

如果，那么第列就使用等式进行计算；

(2)

{63%：如果，那么第列就用等式确定，式中，是一个复杂函数。}

{75%：函数由字循环、字节代换以及轮常量异或3部分组成。}

字循环： {64%：对字中的4个字节进行循环左移1次，即把输入的字变换成；}

字节代换： {48%：使用AES的S盒对上一步的结果进行字节代换运算；}

轮常量异或： {96%：将前两步的结果同轮常量进行异或，其中表示轮数；}

{53%：轮常量是一个字，它的值由下表给出，如表2.2所示；} {69%：使用与轮数相关的轮常量是为了防止在不同的轮中产生的相似的或者对称的轮密钥。}

01000000

02000000

04000000

08000000

10000000

10

20000000

40000000

80000000

1B000000

36000000

表2.2 轮数和轮常量的关系

{49%：由表2.2可看出轮常量的右边3个字节无论在为何值时其总为0。} {81%：通常将轮常量最左边的字节称为，显然。} 的构造方法是： ，，。 其中“ ”是定义在上模的乘法。

{69%：轮密钥加运算就是对128位轮密钥状态中的数据进行按位异或运算的操作。} 其中轮密钥中的每个字、、、都是32bit，其包含4个字节的生成过程为密钥扩展算法。 {67%：轮密钥加的逆运算和轮密钥的加正向运算

结果完全一致。｝

2.3 AES算法中行移位简述

1）行移位操作

｛45％：在行位移的操作中，行移位只需要把字节矩阵进行简单的向左循环移位。｝｛55％：当AES算法密钥的长度为128bit时，行移位只需将状态矩阵的第行循环左移个字节，其中。｝｛77％：这使得矩阵的列完全进行了重新排列排，即在移位后的每列中都包含着未移位的前每列的一个字节。｝

2）行移位逆变换

｛59％：行移位的逆变换与行移位相反，就是将状态矩阵的每一列都执行与行移位相反的移位操作。｝｛57％：即，在128bit的AES中，状态矩阵的第行右移个字节。｝

2.4 AES算法中列混合运算简述

1）列混合

｛75％：列混合变换的实现是通过矩阵相乘来完成的，即行移位后的状态矩阵与固定矩阵进行乘法运算，从而得到混合后的状态矩阵。｝ 状态矩阵中的第列（）的列混合可以表示为

｛46％：其中，矩阵元素的乘法和加法都是定义在基于的不可约多项式构造的有限域上的运算，其中加法等于2个字节的异或，乘法运算则是按照下面的规则运行：｝ 对一个8位的二进制数来说，使用有限域上的乘法乘以10B等于左移一位，再根据情况同11011B进行异或运算。 即，假如，则执行异或运算，否则不执行。

2）列混合逆运算

｛71％：逆向列混合变换可由下式的矩阵乘法定义：｝

｛88％：显然，逆变换矩阵同正交变换矩阵的乘积恰好为单位矩阵。｝

｛78％：列混合变化的矩阵系数是根据最大距离线性码的理论进行设计的，这让列混合具有了良好的扩散性。｝

2.5 轮密钥加运算简述

｛70％：轮密钥加运算就是将128位轮密钥与状态矩阵中的数据进行按位异或运算。｝ 密钥中的每个字、、、总共32bit，包含四个字节的生成过程。 ｛89％：该过程可以看成是字按位异或的结果，也可以看成在字节级别或者位级别的运算。｝

｛56％：图2.3 轮密钥加部分算法图｝

｛75％：由于没有使用 Feistel结构， AES的解密过程和加密过程是不同的，需要使用相应变换的逆向变换，｝

{66%：并且各个变换的使用顺序也不一样，分为轮密钥加、逆行移位、逆列混合和逆字节代换。}

1）交换逆行位移和逆字节代换

{84%：逆行移位虽然影响状态矩阵中的字节顺序，但是并不改变字节的内容，同时也不由字节的内容来决定它的变换。} {84%：然而逆字节代换影响代换矩阵中的字节内容，但是不会改变字节的顺序，同时也不依赖字节的顺序来进行它的变换。}

{93%：2）交换轮密钥加和逆列混合}

{96%：轮密钥加和逆向列混合都不会改变状态矩阵中字节的顺序。} {88%：如果将轮密钥加看成是由字组成的序列，那么轮密钥加和列混合的逆运算每次都是对状态矩阵的一列进行操作。}

2.6 AES算法安全性分析

{80%：尽管一些专家认为存在可以利用该算法使用的数学结构来攻击该算法的可能性，但实际上到现在还没有一种攻击方法能攻击AES；} {77%：另一方面，它采用的是非线性的S盒，结构简单，便于分析设计，也使该算法的安全性不受到威胁。} {100%：由于AES采用的Rijndael算法利用了掩码技术，因而AES能有效防止能量攻击和计时攻击。}

第三章 动态密钥

前面已经提到，本设计使用的是基于对称密钥加密的AES高级加密标准，AES算法现在正广泛运用于各个领域。

在现在信息技术发展迅猛的条件下，使用固定的密钥很容易遭到攻击，即使是十分安全的加密算法。 在消息传递的过程中，只要加密使用的密钥固定，在较长时间没有更改密钥的情况下， 攻击者就有足够的时间而且能够拥有足够多的密文进行分析，通过使用各种方法对密码进行攻击， 从而得到密钥，进而进行下一步的攻击。 无论是什么算法，在长期使用固定密钥的情况下，都为被攻破提供了可能。 所以，较为安全的做法是时常更换密钥，最好是能做到一次一个密钥。 也就是使用动态密钥。 因此，本设计的核心是动态密钥的产生。 本设计的一系列设计都围绕动态密钥的产生进行设计[18]。

{46%：动态密码通常是由专门的算法产生的随机数字组合，它的优点在于使用便捷而且安全。} {46%：如今，越来越多的企业采用动态密码保护网络设备、服务器等。}

3.1 动态密钥的来源

动态密钥是本系统实施的关键。 动态密钥的产生有多种方案，有基于时间的动态密钥，也有基于随机数产生的动态密钥等等。 {41%：可以使用随机数，比如VS2017环境下stdlib.h头文件中自带的rand()函数，这个函数是用来产生伪随机数的，} {41%：之所以称为其为伪随机数是因为其是用线性同余法实现的，它不是真的随机数，} 只不过是因为其周期特别长，所以在一定的范围里可看成是随机的，在不设定产生随机数的种子时， 默认使用0作为产生随机数的种子； 也可以利用计算机本机的时间信息来动态密钥。 每个通信设备都有自己的时间，在计算机中有两个时间，格林尼治时间和相对时间，可以将时间作为一个非线性系统的输入， 然后该非线性系统的输出便可以作为加密算法的动态密钥[19][20]。

总之，动态密钥的来源方式多种多样。

3.2 动态密钥的要求

现在的加密算法已经开始使用基于时间的加密算法，但是在目前还是存在一些局限性，比如时钟同步、动态密钥重复的概率等。 其中最主要的就是时钟同步的问题，现在的时钟设备无论怎么样始终会存在时间误差，一旦时间误差超过允许的范围就有可能导致解密时出现错误。 比如，汽车开锁。 汽车和钥匙各自都有一个时钟，使用基于时间的动态密钥，在两个设备之间的时间相同时加密和解密均能正常进行， 在一段时间之后，汽车和钥匙之间的时钟会产生一个时间差，如果时差较大，钥匙加密使用的密钥和汽车解密使用的密钥将会不同， 从理论上来说无法正确进行解密。 但是如果时间误差容许的范围太大，那么又很容易遭受重放攻击，即攻击者得到了钥匙发出的信号，随后将获取的信号再重放出去，从而打开汽车的锁。 假如攻击者得到了用户的一部分密文，并且花费了大量时间将密钥破解出来，但是， {41%：根据动态密钥的特性，攻击者无法从已破解得到的密钥推算出以后的时刻的密钥，} 所以对动态密钥的攻击需要花费大量时间和运算量，还不一定能够破解[21]。

所以本设计重点围绕动态密钥的产生以及时间同步的问题进行讨论。

3.3 本设计中动态密钥的时钟同步方案

前面已经提到，使用动态密钥进行加密需要严格的时钟同步，如果在短暂的时间内传输信息的两者之间就有较大时间差的话， {43%：传输的正确性就会大大降低，所以保证时钟严格同步是极其重要的。} 但是无论对于何种时钟，时差始终存在，这个是无法避免的，在产生误差的时候要能够对时差进行补偿。 本设计的设计方案以汽车开锁为例。 汽车通常行驶在马路上，或者是停在停车场中，汽车和钥匙内有一个实时时钟， 开锁时钥匙产生一个动态密钥，而汽车则基于汽车本机时间使用相同算法产生相同的密钥， 但是时间一长就会产生时差，从而产生的密钥也就不相同了。

根据汽车的特性，本设计使用GPS作为校准时间差的第三方。 {41%：GPS能够接收到卫星发射的数据，而这数据中就含有时间信息。} {45%：卫星上搭载有原子钟，美国的全球定位系统与俄罗斯的格洛纳斯系统搭载的是铯原子钟，} 欧盟的伽利略与中国的北斗导航系统搭载的是铷原子钟， GPS的时钟的天稳定度能够达到， 所以本设计使用 GPS模块对时钟进行校准[22][23][24]。

通常，汽车停在停车场时GPS无法接收到卫星发送的信号，但是汽车不能就因此而不工作，所以就需要一个能够保存时间的设备，即时钟模块。 时钟模块的选择首先是要选择精度高的模块。 本设计中时钟模块选用飞利浦公司的PCF8563，外部使用32.768KHz的晶振作为外部时钟院，官方给出的误差约为1s/天。 详细设计将在第四章中给出。

3.4 本设计动态密钥的产生

本设计中动态密钥的产生基于时间，即，将时间输入到一个非线性系统中，该系统的输出作为加密使用的动态密钥。 如图2.1所示。

图3.1 动态密钥的产生

在本设计中动态密钥的产生方法如下：

将当前时间乘上一个区间在的随机数，然后将上一步的乘积扩展到16位，即将乘积再乘以1000，最后去前一步结果的后十六位作为动态密钥。 即动态密钥的产生公式为，。

3.5 对动态密钥算法产生的结果分析

为了对该动态密钥所产生的安全性进行分析，使用 MATLAB编程，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、非线性进行分析。

图3.2 模拟时间产生动态密钥的散点图

图3.3 动态密钥产生的折线图

图3.2中的点是在当前时间所产生的密钥，由图3.2和图3.3可以看出， 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3.4 动态密钥的重复率

由图2.4可以看出当前时刻的动态密钥同前一次产生的动态密钥相比， 在1000次中重复率超过40%的只有三次，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10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，可以认为该产生动态密钥的算法是可靠的，不容易被攻击者所攻破的。 所以选择该算法作为产生动态密钥的算法。

{68%：第四章 保证系统实现的硬件设计}

{41%：本设计使用基于STM32F103系列单片机，配合外围电路，如时钟模块、GPS模块、GSM模块、nRF2401模块、按键模块等，构成整个系统。}

本设计采用STM32F103系列单片机，ARM Cortex-M3内核。 Cortex-M3是一个32位的核。 Cortex-M3采用了Tail-Chaining中断技术，其中断处理完全基于硬件进行，最多可减少12个时钟周期数，在实际应用中可减少70%中断。 其广泛运用于可穿戴设备、智慧城市的建设等方面。 {72%：属于中低端的32位ARM微控制器。} {54%：外部晶振8MHz，通过内部锁相环倍频到72MHz。} {55%：有I2C接口、USART接口、SPI接口、CAN总线接口、DMA控制器、12位AD转换器等。} 其中用户所使用的是STM32、nRF2401、GPS、时钟模块以及按键模块。 服务器端使用的是STM32、nRF2401、GPS模块以及GSM模块。 其中GSM模块在通信时所需要不少于5V、1A的供电[25][26]。

4.1 保证系统时钟稳定的实时时钟

在汽车遥控的应用中，当汽车长时间无法获得当前的实时时间时，这时就需要一个时钟， 在时钟校准后，即使接收不到时钟校准信号也依然能够较准确地继续保持时钟的运行。 {52%：在本设计中实时时钟选用NXP（恩

智浦）公司的PCF8563芯片。｝ PCF8563是一款CMOS低功耗实时时钟芯片。 ｛44％：在官方芯片手册中提到该芯片的时钟精度为也就是，精度能够满足设计的要求。｝ PCF8563提供可编程的时钟输出、中断以及低电压检测。 所有的地址和数据都通过双向的两线的IIC总线传输。 最大总线速度400kbit/s。 在读写数据时，当读写完成后，地址总线自动增加。 ｛40％：IIC是Inter-Integrated Circuit的缩写(集成电路总线），这是由飞利浦半导体公司在八十年代初设计的一种简单、二线制、双向、同步串行总线，该总线的主要作用是用来连接整体电路。｝ 多个IIC协议的芯片可以连接到同一总线结构下，同时每个芯片都可以作为实时数据传输的控制源，使用时只需要对某个芯片的使能端进行选通便可对其进行操作。 这种方式极大地简化了信号传输总线接口[27]。

图4.1 PCF8563实际接线图

IIC协议中器件与IIC总线的连接如图4.2所示。 SDA与SCL都是双向通信，与上拉电阻或者电流源相连接。 ｛66％：当总线空闲时两根线都被拉高；｝ ｛57％：连接到总线上的设备的输出极必须有一个开漏或开集电极的线与功能。｝ ｛46％：IIC总线上数据的标准模式下的传输速率能达到100 kbit/s，在快速模式下能达到400kbit/s，高速模式下能达到3.4Mbit/s。｝

｛56％：图4.2 标准模式下和快速模式下器件与IIC总线的连接｝

｛70％：在传输过程中，当时钟信号为高电平时，数据线上的数据必须保持稳定，只有当时钟线为低电平时数据线的电平才能发生改变。｝

｛54％：在IIC的程序执行中，一些特定的电平起伏被定义为起始和终止信号，如图4.3所示。｝ ｛60％：在时钟线为高电平时，数据线从高电平转为低电平的过程被称为IIC的起始状态。｝ ｛57％：当时钟线为高电平时数据线从低电平到高电平被称为IIC的结束信号。｝

图4.3 IIC的起止状态

｛48％：起止信号总是由主机产生，当起始信号产生后总线进入忙状态，结束信号产生后进入空闲状态。｝ ｛43％：通过连入必要的硬件接口检测连接到总线的器件的起始状态十分容易，但是对于没有这样接口的微控制器来说，｝ 必须在每个时钟周期对数据线采样两次才能得到状态的转换。 所以，采用硬件IIC接口的微处理器在IIC数据的传输上具有更大的优势。

｛65％：数据线上的每个字节必须是8位，每次传输的字节数并不固定。｝ ｛49％：每个传输的字节都必须有应答位，如图4.4所示。｝ ｛53％：如果从机在执行一些其他功能时，例如系统进入内部中断，总线不能接受或者发送一个完整的字节，它将会拉低时钟线，强制使主机进入等待状态。｝ ｛72％：当从机准备好接受下一个数据或者释放时钟线时，数据传输继续进行。｝ 在程序设计中也需要根据这个特点进行设计，以增强程序的鲁棒性。

图4.4 IIC总线上的数据传输

带有应答的数据传输是必须的。 ｛51％：与应答相关的时钟由主机产生，发送方在应答时钟阶段释放数据线，｝ ｛49％：接收方在应答时钟内必须拉低数据线来保证在时钟线为高电平时保证稳定的低电平，｝ 如图4.5所示。 这也就是应答信号。

图4.5 IIC总线上的应答

4.2 遥控需要的无线传输模块

在汽车遥控的应用中，汽车通过钥匙遥控解锁，通常使用的就是无线遥控的方式，无线遥控具有便于携带和使用方便的特点，在本设计中同样选用无线模块进行遥控。

无线传输模块选用NORDIC公司的nRF2401芯片。 {43％： nRF2401是应用于超低功耗的2.4GHz带嵌入基带协议引擎的单芯片收发器件，工作频带2.4GHz-2.4835GHz。} {46％： 一个微控制器加上少量的外围元件就可以构成nRF2401的无线系统。} nRF2401通过串行外围总线（SPI）进行操作。 {88％： 这是一种全双工的、高速的、同步的通信总线，并且在芯片的管脚上只占用四根线，节约了芯片的管脚，同时为PCB的布局上节省空间，正是出于这种简单易用的特性，如今越来越多的芯片集成了这种通信协议。} {92％： nRF24 L01集成了一个完整的2.4 GHz射频收发器， RF合成器， } 和支持高速 SPI接口控制器的包括 Enhanced Shock Burst硬件协议的基带逻辑器件。 {69％： 不需要外部环路滤波器和压控振荡器，谐振器，变容二极管是必需的，只有一个低成本的±60ppm晶体，匹配电路，天线。}

SPI主机与从机的连接如图4.6所示。 SPI有主机模式和从机模式，当MSTR位置1时，SPI以主模式运行。 只有主机SPI模块才能启动传输。 {68％： 传输通过写入主SPI数据寄存器开始，如果移位寄存器是空，字节立即转移到移位寄存器。} {100％： 字节在串行时钟的控制下开始在MOSI引脚上移出。} {73％： 当SPI控制寄存器1中的MSTR位清零时，SPI工作在从模式。}

图4.6 SPI主从机传输原理图

CPHA=0，时图4.7显示了CPOL＝0和CPOL＝1的SCK波形。 由于SCK，MISO和MOSI引脚直接连接在主机和从机之间，所以该图可以解释为主机或从机时序图。 MISO信号是从机的输出，MOSI信号是主机的输出。 主器件的引脚必须为高电平或重新配置为不影响SPI的通用输出。

图4.7 CPHA=0时的SPI时序

图4.8为CPHA=1时SPI的时序，由于SCK，MISO和MOSI引脚直接连接在主机和从机之间，所以该图可以解释为主机或从机时序图。 MISO信号是从机的输出，MOSI信号是主机的输出。 线是从机的从选择输入。 {41％： 主机的引脚必须为高电平或重新配置为通用输出，并不影响SPI总线。}

图4.8 CPHA=1时的SPI时序

4.3 使用GPS模块进行时间校准

汽车在停在地下停车场时，钥匙与汽车之间的时间会或多或少存在时间差，时间一长就会影响到系统是佛偶能进行正常的开解锁。 通常汽车行驶的时候会使用到GPS，而GPS卫星上面就正好搭载了高精度的原子钟，所以，利用这个特性，本设计使用GPS作为校准时间的设备。

GPS使用u-blox公司的NEO-6M模块，使用GPS进行定位。 GPS使用NMEA-0183协议。 NMEA 0183是美国国家海洋电子协会（National Marine Electronics Association）为海用电子设备制定的标准格式。 目前业已成了GPS导航设备统一的RTCM（Radio Technical Commission for Maritime services）标准协议。 帧格式形如：
$aaccc，ddd，ddd，… ，ddd*hh(CR)(LF)。 使用的帧有5种，分别是$GPGGA ——GPS定位信息； $GPGSA

——当前卫星信息； $GPGSV ——可见卫星信息； $GPRMC ——推荐定位信息； $GPVTG ——地面速度信息； $GPGLL ——大地标信息； $GPZDA ——当前时间信息。 本设计仅使用$GPRMC帧，因为此帧包含了我们所需要的时间信息和日期信息。

4.4 使用GSM模块增加系统安全性

在现在各大网站登录的时候都会使用手机验证码作为登录验证的一部分，同样，本设计为了增加系统的安全性，也增加了验证码发送的部分，所以系统使用到了可以用来发送短信的 GSM模块。

GSM模块选用SIM800A模块。 {42%：SIM800A是一款两频GSM/GPRS模块工作频率为GSM/GPRS 900/1800MHz，可以低功耗实现语音、SMS和数据信息的传输。} {51%：此模块通过USART与MCU进行通信，MCU向模块发送AT指令控制GSM模块进行完成各种操作；} MCU通过串口接收GSM反馈回的数据，从而对GSM所处的状态进行判断。

{43%：在本设计中，使用GSM模块的发送短信功能，通过MCU控制模块向手机发送验证码。}

4.5 按键模块输入验证码

在本设计中，用户端需要通过按键输入接收到的验证码，然后用户端通过无线模块将验证码发送出去，所以，设计还需要按键输入的部分。

{74%：通常的按键有独立按键和矩阵按键等形式，在键盘中按键数量较多时，为了减少I/O口的占用，通常将按键排列成矩阵形式，如图4.9所示。} {100%：在矩阵式键盘中，每条水平线和垂直线在交叉处不直接连通，而是通过一个按键加以连接。} {48%：矩阵键盘接入单片机的列线的 I/ O口设置为普通推挽输出模式，} {41%：行扫描线设置为下拉输入，通过配置输出线的高低电平和检测输入线的高低电平来检测哪一个按键被按下，} 从而实现按键输入数据的功能。

图4.9 按键模块

{58%：第五章 保证系统实现的软件设计分析}

上一章对基于实时时钟加密系统的硬件部分进行了简单的描述。 本章对系统的软件部分进行叙述。 {42%：用户端和服务器端与MCU接口连接的情况分别如图5.1、图5.2所示。}

图5.1 服务器端外设与MCU连接示意图

在图5.1中，GPS、GSM、以及调试用的串口分别通过MCU的USART3、USART2、USART1进行连接。 GPS仅仅需要向MCU发送数据，MCU通过串口中断接收数据，然后对数据进行处理，得到包含所需要信息的数据包，即$GPRM数据包。 {41%：GSM模块和 MCU进行双向通信，MCU向 GSM发出 AT指令，GSM接收到后就开始执行相应步骤，} 执行结束后会产生一些状态信息，如错误信息等，MCU读取 GSM反馈回的状态信息，然后根据此进行判断是否进行下一步判断或者重新执行之前的操作。 调试串口向PC端单向发送数据，通过这样的方式在PC端显示出一些数据，从而实现调试的目的。 {43%：IIC与SPI接口分别与时钟模块和无线收发模块相连，双向收发数据；} {58%：通过对器件的寄存器进行读写操作从而达到控制器件的目的。}

图5.2 用户端外设与MCU连接示意图

{64%：用户端的连接基本同服务器端的连接一致。} {43%：按键模块是利用矩阵键盘行扫描和列扫描判断出具体是哪一个键被按下，以此来进行密码和验证码的输入。}

5.1 用户端程序主要流程

{49%：用户端程序主要分为主程序和中断服务程序两部分，服务器端程序仅有主程序部分。}

{66%：用户端主函数程序流程如图5.3所示。} {41%：函数的开头部分主要是对各个模块进行配置或者初始化，如配置外部中断、初始化串口、无线收发模块的SPI接口初始化、OLED的各个引脚初始化等。} 其中串口的波特率配置为9600Baud； 串口的输出都配置为复用输出； 输入为悬空输入； 传输的格式为字长为8位的数据格式； 接收数据通过串口的接收中断接收数据。 {41%：SPI接口使用MCU的硬件接口，SPI的波特率预分频值为8，数据大小为8位；} 在读写寄存器时都通过读取SPI的标志位来判断读写是否完成，增加了程序的鲁棒性。

{41%：IIC接口同样使用MCU的硬件接口，SDA线和SCL线均采用开漏输出的方式；} IIC的自地址为0X0A，器件的地址为0XA3，写地址为0XA2，如果地址存在问题，则程序会一直卡在读取器件的应答信号上。

程序在初始化完成之后就开始接受 GPS数据包，相对于接受经纬度信息来说，时间信息和日期信息十分容易接收到， 在接受到包含时间信息的数据包后，对该数据包进行解析，提取出时间信息，并且将时间信息写入到时钟芯片上， 相当于完成了时间的同步。 {47%：然后系统不断进行时间的同步校准，等待中断的到来。}

图5.3 主程序流程图

程序所使用的中断为外部中断，通过安检触发。 {55%：按键被配置为上拉输入，通过下降沿触发外部中断。} {49%：中断的优先级和次优先级均为最高，中断服务程序的流程如图5.4所示。}

图5.4 中断函数的流程

进入中断后，先通过按键输入密码，该密码是对数据包加密和解密的密钥，如果密码错误服务器端将无法用事先约定好的密码解密出正常的信息， 从而无法完成解锁的步骤。 {45%：在密码输入后就开始进行握手操作，握手的流程如图5.5所示。} 用户端与服务器端采用类似 TCP三次握手协议建立连接，在第④步时，服务器向与用户端相关联的手机发送验证码， 用户输入验证码，当主机验证无误后建立连接，然后完成一系列的步骤。 {48%：其中，随机数的产生通过头文件中stdlib.h的rand()函数完成。} {57%：在通过 srand()函数设定种子之后就可以使用 rand()函数产生随机数了，但是 rand()所产生的随机数是伪随机数，} {82%：其是用线性同余法实现的，它不是真的随机数，只不过是因为其周期特别长，} 所以在一定的范围里可看成是随机的，这也就出现了一个问题，单片机每次上电或者复位后所产生的随机数都是一样的。 有几种解决方法，第一： 通过读取AD转换器的后面几位，后面几位不稳定的数可以认为是随机数； 第二： {47%：仿照windows上的随机数产生方式，即利用时间作为种子产生随机数。} 在这里我选用第二种方法，因为系统中正好含有时钟模块，使用时钟的秒读书作为种子信息，产生随机数，能保证在每一秒里所产生的随机数都不同。 从而能够有效防止攻击者在没有获取用户手机的情况下对系统的攻击。

图5.5 握手的流程图

数据包的格式如下表所示，其中硬件标识在数据发送和接收过程中不进行加密处理，以明文的方式直接传输，方便服务器端在接收到之后用于查找用户硬件标识所对应的密钥和手机号。 从而完成后面的加解密等过程。在加密之前，用户端通过读取时钟芯片中的时间，通过格式上的处理之后填充到帧上对应的位置； {51%：在加密时，用户端使用输入的密钥进行加密，然后将加密后的帧发送出去。}

硬件标识

SYN

ACK

SEQ

TIME

DATA(REQUEST)

1305054145

0/1

0/1

随机

time

data

表5.1 帧格式

5.2 服务器端程序的主要流程

{76%：图5.6 服务器端程序流程图}

{43%：服务器端在进入程序后首先对外围器件和接口进行初始化，初始化包括对时间的校准，} {41%：在初始化完成后就开始等待用户端发送数据包，每次接收到数据包后先要对数据包进行解密，} {43%：解密后得到的数据包中就包含用户端发送数据包时的时间戳，将服务器本机的时间与用户端发送数据包的时间进行对比，} {56%：根据时间差来判断是否存在有人重放攻击的情况。} 在不考虑用户端和服务器端硬件上的时间差的情况下，只有当接收到的数据包中的时间与当前时间相近时才可以认为这一系列的动作是实时的。 在重放攻击中，重放的时间是相对远离当前用户操作的时刻，所以，通过时间的对比判断能够有效解决重放攻击的问题。

5.3 本章小结

{56%：本章主要介绍了用户端和服务器端的工作流程。} 以信息对抗的策略对系统软件进行设计。 {47%：其中，握手环节是用户端和服务器端相互建立连接的重要环节。} {49%：在TCP/IP协议中为了保证可靠、安全的数据传送，在数据传送之前采用三次握手的方式建立连接。} {40%：主机在想要建立连接前先告知服务器端我要建立连接了，服务器端接收到后若同意则发送同意信号，} {41%：服务器用户端收到后再向服务器端发送相应信号，至此，一次会话就建立成功了。} 其次，验证码模块的设计也是系统重要的一环。 从攻击的角度来看，要想骗取服务器开锁就必须要有用户设备发送的基于实时时钟的信号， 重放攻击实施成功已经不可能了，那么，就必须要使用用户端的硬件设备。 若单纯地复制用户设备的硬件而不复制软件则也达不到目的； 如果用户端设备被盗，而盗窃者又知道用户密码的情况下，验证码的存在就发挥作用了。 因为同时丢失手机和设备的可能性很小。 所以，加入验证码是一种更加安全的设计。

第六章 对整个系统的调试

{41%：在完成了硬件和软件的设计之后，现在开始对系统进行调试。} 首先对单个模块进行调试，先熟悉各个模块的使用方法，然后再将所有模块组合成一个整体，再对整体功能进行调试。

6.1 GPS模块调试

图6.1 GPS模块向PC端发送的数据

{46%：图6.2 在上位机中对数据包解析后的情况}

{40%：GPS模块使用RS232模块直接将数据发送到PC端，如图6.1所示。} {43%：图中，数据包中就包含了时间数据、经纬度数据、日期数据和卫星数据等数据。} 在图6.2中的上位机软件上，软件将接收到的数据包解析后与地图直接联系起来，显示出当前的位置，可以看出定位的准确度还很高的。

6.2 GSM模块调试

图6.3 GSM模块发送短信

在调试GSM模块时，我通过GSM模块向10086发送话费查询请求，然后10086发送短信过来，读取短信，如图5.3所示。 图中，画上红色下划线的指令为模块向PC端反馈回的消息。 在对模块进行了一系列的检测，无误后，写入要发送的对象的电话号码，然后写上要发送的文字。 模块返回OK后说明短信发出，随后模块向PC端发送+CMTI: {43%：”SM”，1，表明收到一条短信，通过AT+CMGR=1读取第一条短信，并以UNICODE的形式发送回PC。} 如图6.4所示。

图6.4 读取短信

将读取的UNICODE通过软件转换成汉字，如图6.5所示。

图6.5 通过软件将UNICODE转换成汉字

6.3 整体调试

6.3.1 对服务器端进行调试

服务器端上电之后的情况如图6.6所示，图中可以看到系统进行了NRF2401模块与系统的连接检测、GSM模块状态的检测以及时间的检测和初始化。 {45%：在进行初始化之后系统开始等待用户端发送数据。}

图6.6 服务器端上电后的情况

{41%：在服务器与用户端握手成功后服务器端向用户手机发送验证码，如图6.7所示。} 其中验证码的产生是通过基于时间的随机数产生的。

图6.7 握手成功后向用户手机发送验证码

图6.8 用户端密码输入正确后服务器端显示开锁

{44%：用户在接收到验证码后输入接收到的验证码，服务器端在接收到之后进行比较，如果比较成功，则进行开锁指令。} 如图6.8所示。

6.3.2 对用户端进行调试

用户端上电之后，若不按下按键则一直显示GPS数据包，如图6.9所示。 在图中可以看到GPS数据包中仅包含时间和日期信息，在前面也提到过，GPS模块接收时间信息比接收经纬度信息容易很多。 在这里我们只使用时间和日期信息。

在请求按键按下之后，用户端需要输入密码，在这里，密码是对数据加密和解密的密钥。 {47%：如果密码输入错误，系统将无法正确对数据进行解密。} {46%：在用户输入完密码后，串口将用户输入的信息重新显示在屏幕上。} 密码输入之后便开始与服务器端进行握手，在图中可以看到握手成功，等待接收服务器端发送的验证码短信。

图6.9 用户端上电之后的情况

图6.10 用户接收到的含有验证码的短信

在接收到验证码后，通过按键输入验证码，验证码一共14位，通常收到的验证码是9位或者10位，输入后位数不够则用0补足。 在验证码输入正确后，服务器端显示开锁，如图6.10所示。 用户接收到的验证码短信如图6.10所示。 至此，解锁完成。

第七章 全文总结与展望

7.1 全文总结

在学习计算机对抗和单片机等相关理论知识的基础上，本文对基于实时时钟的加密算法进行了分析设计。 本文的研究主要按照信息对抗策略结合对信息的进攻和防御的角度来进行的，整个系统结合了密码学、电路学、信息对抗理论、控制理论等多学科知识。 基于实时时钟的加密算法是以站在信息安全的大环境下结合信息对抗理论，并以密码学为例子进行的一次实验。 在设计中，时间作为验证数据有效性的关键因素，以对称密钥加密算法进行加密解密，能够有效保证数据不被攻击者窃取。

但是由于受到时间等因素的限制，目前已经完成的工作还是比较基础的，还需要对硬件和软件的设计进行进一步的分析和完善。 并且，以下几个方面也值得深入的分析和探索：

(1)建立更加完整的软件系统，记录用户连接上服务器端之后的每一个信息，包括时间信息、操作过程、地理位置信息等， 这样方便在出现问题后能够有效地查看问题的究竟出在哪里以及解决方案。 同时建立更完善的用户管理系统，能够添加新用户，保存用户的各种信息，使系统不再单一地仅识别一个用户。

(2) 使用更加低功耗的设备。 在用户设备中， GPS模块消耗的电能较多，在应用于汽车开锁、门禁系统的时候不太理想， 需要一种更加节能能够使用时间更长的设备来维持使用，如更加低功耗的处理器等。

(3) 在电磁安全方面，使用无线传输特别是特定频率传输容易被攻击者探测到，从而被攻击的可能性提高，在未来可以使用捷变频的方式进行数据传输。

7.2 展望

在基于实时时钟加密方面，国外明显领先于国内。 但是现在还是存在很多问题。 首先在算法方面， AES在现在还是一种可靠的对称密钥的加密算法，但是密钥的保存困难是这种算法的缺点， {42％：而且随着现在计算机的运算速度的大幅提升，破解一种算法的能力大大提升，特别是量子计算机的出现，} 希望在未来能够有更加安全有效的加密算法。 其次，在信息对抗的角度上看，本设计使用的2.4 GHz模块只能在很窄的频段内工作，假如有攻击者实施压制干扰，服务器端将不能够接收到解锁的信息，如果仅有一种解锁或者开锁的方式， {81％：那么攻击者就能达到其攻击的目的。}

{41％：目前，国内信息对抗的水平较以前有了较大的发展，但是如果与发达国家如美国相比的话，仍然存在很大差距。} 近日出现的洋葱病毒就是通过互联网的端口渗透进入用户计算机，通过RSA算法对用户数据进行加密，从而勒索用户。 在现代科技条件下，如果用户没有私密钥则几乎无法对数据进行解密。 所以按照目前的形式，保护信息安全仍然是我国乃至全球需要考虑和解决的问题。

参考文献

[1] 李兴原，王旭，张文超等.现代加密技术简述[J].仪器仪表用户，2007，14(5): 121-122.DOI: 10.3969/j.issn.1671-1041.2007.05.075.

[2] 晏国勋.加密技术下的信息安全[J].网络安全技术与应用，2013，(8): 100-104.DOI: 10.3969/j.issn.1009-6833.2013.08.054.

[3] 冯登国，张阳，张玉清等.信息安全风险评估综述[J].通信学报，2004，25(7): 10-18.DOI: 10.3321/j.issn:1000-436X.2004.07.002.

[4] 沈昌祥，张焕国，冯登国等.信息安全综述[J].中国科学E辑，2007，37(2): 129-150.DOI: 10.3321/j.issn:1006-9275.2007.02.001.

[5] 郑东. 密码学——密码算法与协议[M]. 北京: 电子工业出版社， 2009.

[6] 邵丽萍. 计算机安全技术[M]. 北京: 清华大学出版社, 2012.

[7] Wikipedia. Data Encryption Standard[EB/OL]. https: //en.wikipedia.org/wiki/Data Encryption Standard.

[8] Wikipedia. Advanced Encryption Standard[EB/OL]. https: //en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[9] 袁科, 刘哲理, 贾春福, 马昊玉, 吕述望. TRE加密技术研究[J]. 计算机研究与发展, 2014, (06): 1206-1220.。

[10]吴开兴, 张荣华.加密技术的研究与发展[J].计算机安全, 2011, (6): 77-79.DOI: 10.3969/j.issn.1671-0428.2011.06.024.

[11]Kenneth, G, Paterson, and, Elizabeth, A, Quaglia. Time-Specic Encryption[C]. UK: ICT-2007-216676 ECRYPT II, 2007

[12] 苏海晏.信息战的常用战术和防范策略.信息网络安全, 2003, (12); 32-33

[13] 方禾, 许力, 苏彬庭, 林晖. 多信道无线网络中窃听与干扰攻击的对抗策略[J]. 四川大学学报(工程科学版), 2016, (01): 119-125.

[14] 张玉清, 王志强, 刘奇旭等.近场通信技术的安全研究进展与发展趋势[J].计算机学报, 2016, 39(6): 1190-1207.DOI: 10.11897/SP.J.1016.2016.01190.

[15]Wikipedia.Electronicauthentication[EB/OL].https: //en.wikipedia.org/wiki/Electronic_authentication.

[16]朱晓礼. 银行身份认证系统设计与实现[D].山东大学, 2012.

[17]中国科学技术协会.密码学学科发展报告[R].北京： 中国科学技术出版社, 2014-2015.

[18]张建伟, 李鑫, 张梅峰等.基于MD5算法的身份鉴别技术的研究与实现[J].计算机工程, 2003, 29(4): 118-119, 145.DOI: 10.3969/j.issn.1000-3428.2003.04.047.

[19]弟宇鸣, 陈荣桦, 左广霞等.基于AES算法的加密模块设计[J].电子设计工程, 2013, 21(2): 53-55.DOI: 10.3969/j.issn.1674-6236.2013.02.017.

[20] B.Lakshmi, T.N.Prabakar, E.Kirubakaran.Real time cryptography with dual key encryption[C].International Conference on Computing, Communication and Networking.US： IEEE, 2008

[21] Danfeng, Yao, Nelly, Fazio, Yevgeniy, Dodis, Anna, Lysyanskaya. IDBased Encryption for Complex Hierarchies with Applications to Forward Security and Broadcast Encryption[R]. Washington, DC, US: ACM, 2004.

[22]叶晰, 叶依如.基于MD5算法的动态口令技术的软件实现[J].计算机应用与软件, 2009, 26(11): 281-282.DOI: 10.3969/j.issn.1000-386X.2009.11.092.

[23] 贾小林， 刘帅， 孙大伟. GPS星载原子钟在轨性能评估精度分析[J]. 测绘科学与工程， 2016， 36(2): 1-4

[24]谢巍. 内嵌实时时钟的安全芯片以及校准其实时时钟方法[P]. 中国: 200510055892.6，2005年12月4日.

[25] 刘火良， 杨森. STM32库开发实战指南[M]. 北京: 机械工业出版社， 2013.

[26] 姚文详. ARM Cortex-M3权威指南[M]. 北京: 北京航空航天大学出版社， 2014.

[27] 代宇. 无线汽车门锁密码系统的研究与设计[D].哈尔滨工业大学，2013

致 谢

{64％： 在此论文完成之际，谨以此文献给所有关心、帮助和支持我的老师和同学。} {48％： 本论文是在信息对抗技术专业学科主任张丕状老师的精心指导下完成的。} {90％： 张老师渊博的知识，严谨求实的治学态度，一丝不苟的科研精神，高造诣的学术水平和宽广的胸怀给我留下了深刻的印象，使我受益匪浅。} {44％： 从论文选题到撰写的全过程，老师自始至终给予我具体的指导和帮助，使我的论文得以顺利的完成。} 这段时间，我也非常感谢所有帮助过我的老师们，对我提出的问题进行耐心的回答。 在此向所有老师表示我最诚挚的感谢和由衷的敬意！

{42％： 同时在本科学习期间，信息与通信工程学院的老师们在我的学习和生活等各方面给予了无微不至的关怀和帮助，在此我特别向老师表示深深的谢意！}

在此向多年以来一直无私的关心照顾我的父母和亲人致以真诚的谢意，感谢您们一直以来对我的支持和鼓励！

{57％： 最后，对评阅本论文的专家们表示衷心的感谢！}