doi :10.3969/j.issn.1671-1122.2013.11.014

一种基于 AES 的智能手机门禁系统方案

崔杰，张庆阳，程珂，崔仁杰
（安徽大学计算机科学与技术学院，安徽合肥 230039）

摘 要：在数字技术、网络技术飞速发展的今天，门禁产业也向新一代便携式身份验证门禁控制架构方向发展。AES 是全世界范围内所使用的流行的对称密钥加密算法之一。文章设计了一种基于 AES 的智能手机门禁系统，大幅度提高了门禁系统的安全性，极大简化了硬件设备，同时也使传统门禁系统功能得到了保留和完善。

关键词：AES；智能手机；门禁系统
中图分类号：TP309 **文献标识码：**A **文章编号：**1671-1122（2013）11-0054-04

A Scheme of Smart Mobilephone Access Control System based on AES

CUI Jie, ZHANG Qing-yang, CHENG Ke, CUI Ren-jie
(*School of Computer Science and Technology, Anhui University, Hefei Anhui* 230039,*China*)

Abstract: Nowadays, with the rapid development of digital technology and network technology, the access control industry is developing into a new generation of portable authentication access control architecture. Widely used around the world, AES is one of the popular symmetric key encryption algorithms. This paper presents a AES-based smart mobilephone access control system, which largely improves the security of the system and greatly simplifies the hardware devices, as well as makes the functions of the traditional access control system preserved and improved.

Key words: AES; smart mobilephone; access control system

0 引言

在数字技术、网络技术飞速发展的今天，门禁技术也得到了迅猛发展。当前人们已经进入到一个移动增强、应用先进且安全威胁日益增加的时代，门禁产业也向新一代便携式身份验证门禁控制架构方向发展。

目前市面上基于智能手机的门禁系统大多需要配备一系列特有的软硬件设备，成本高昂，使得推广应用十分困难，并且很多产品没有有效的安全防护机制。本文设计了一种基于 AES 的通过智能手机蓝牙通信功能与门锁进行交互的门禁系统，极大简化了硬件设备，并且在各方通信时均进行了有效加密处理，大幅提高了系统安全性。同时开发出一套门禁管理系统，使得传统门禁系统的功能得到保留和完善。

1 AES 加密算法模型

AES 加密算法的密钥长度和分组长度均可独立指定为 128 位、192 位或 256 位，算法相应要进行 10 轮、12 轮或 14 轮加密运算 [1]。每轮运算由 4 个变换组成：S 盒替换（ByteSub）、行移位（ShiftRow）、列混合（MixColume）、轮密钥加（AddRoundKey）。算法由轮密钥加开始进行 9 轮迭代，最后一轮迭代不包含列混合。本文采用的 AES 加密算法的分组长度和密钥长度均为 128 位。下面以一轮加密过程为例解释其数学模型。

1.1 S盒替换

S 盒替换是一个独立作用于状态字节的非线性变换，简记为 S[2]。包括有限域 $GF(2^8)$ 中的求逆运算和 $GF(2)$ 域中的仿射变换两个步骤。

收稿日期：2013-08-18
基金项目：国家自然科学基金 [61173188、61173187]、国家自然科学基金数学天元基金 [11126174]、安徽省高校自然科学研究重点项目 [KJ2013A017]、安徽大学博士科研启动经费项目
作者简介：崔杰（1980-），男，河南，讲师，博士，主要研究方向：网络与信息安全；张庆阳（1992-），男，安徽，本科，主要研究方向：网络安全；程珂（1993-），男，安徽，本科，主要研究方向：网络安全；崔仁杰（1993-），男，安徽，本科，主要研究方向：信息安全。

1）在有限域$GF(2^8)=\frac{Z_2[x]}{(x^8+x^4+x^3+x+1)}$中求乘法的逆运算，即输入$\omega\in GF(2^8)$，求$\upsilon\in GF(2^8)$，使得满足：

$$\omega*\upsilon=1 \bmod (x^8+x^4+x^3+x+1)$$

于是有：

$$\upsilon=\omega^{-1}=\begin{cases}\omega^{254} & \omega\neq 0\\ 0 & \omega=0\end{cases} \quad (1)$$

2）令$x=v$在$GF(2^8)$中的元素分量为$(x_7,x_6,x_5,x_4,x_3,x_2,x_1,x_0)$，仿射变换如下：

$$y=La\times x+'63'=\begin{bmatrix}1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\\1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\end{bmatrix}\begin{bmatrix}x_7\\x_6\\x_5\\x_4\\x_3\\x_2\\x_1\\x_0\end{bmatrix}+\begin{bmatrix}0\\1\\1\\0\\0\\0\\1\\1\end{bmatrix} \quad (2)$$

常量 '63' 的选择确保了 S 盒没有不动点$S(a)=a$和对立不动点$S(a)=\bar{a}$，输入位的线性组合与输出位的线性组合之间的最大平凡相关性是2^{-3}，异或差分表的非平凡最大输出差分概率是2^{-6}，S 盒具有抵抗线性攻击和差分攻击的能力[3,4]。

1.2 行移位与列混合

通过 S 盒替换得到 4×6 字节矩阵，其中$S_{i,j}$是第i行第j列的字节，$0\leqslant i\leqslant 3, 0\leqslant j\leqslant 5$。行移位变换使矩阵的第$i$行左移$i$个字节：

$$\begin{bmatrix}s_{0,0}&s_{0,1}&s_{0,2}&s_{0,3}&s_{0,4}&s_{0,5}\\s_{1,0}&s_{1,1}&s_{1,2}&s_{1,3}&s_{1,4}&s_{1,5}\\s_{2,0}&s_{2,1}&s_{2,2}&s_{2,3}&s_{2,4}&s_{2,5}\\s_{3,0}&s_{3,1}&s_{3,2}&s_{3,3}&s_{3,4}&s_{3,5}\end{bmatrix}\rightarrow\begin{bmatrix}s_{0,0}&s_{0,1}&s_{0,2}&s_{0,3}&s_{0,4}&s_{0,5}\\s_{1,1}&s_{1,2}&s_{1,3}&s_{1,4}&s_{1,5}&s_{1,0}\\s_{2,2}&s_{2,3}&s_{2,4}&s_{2,5}&s_{2,0}&s_{2,1}\\s_{3,3}&s_{3,4}&s_{3,5}&s_{3,0}&s_{3,1}&s_{3,2}\end{bmatrix}$$

列混合变换对每列进行独立操作以达到混淆的目的。把每列中的每个字节映射为新值，此值由该列中的 4 个字节通过函数变换得到。变换如下：

$$\begin{bmatrix}s'_{0,0}&s'_{0,1}&s'_{0,2}&s'_{0,3}&s'_{0,4}&s'_{0,5}\\s'_{1,0}&s'_{1,1}&s'_{1,2}&s'_{1,3}&s'_{1,4}&s'_{1,5}\\s'_{2,0}&s'_{2,1}&s'_{2,2}&s'_{2,3}&s'_{2,4}&s'_{2,5}\\s'_{3,0}&s'_{3,1}&s'_{3,2}&s'_{3,3}&s'_{3,4}&s'_{3,5}\end{bmatrix}=D\begin{bmatrix}s_{0,0}&s_{0,1}&s_{0,2}&s_{0,3}&s_{0,4}&s_{0,5}\\s_{1,0}&s_{1,1}&s_{1,2}&s_{1,3}&s_{1,4}&s_{1,5}\\s_{2,0}&s_{2,1}&s_{2,2}&s_{2,3}&s_{2,4}&s_{2,5}\\s_{3,0}&s_{3,1}&s_{3,2}&s_{3,3}&s_{3,4}&s_{3,5}\end{bmatrix}$$

其中，

$$D=\begin{bmatrix}02&03&01&01\\01&02&03&01\\01&01&02&03\\03&01&01&02\end{bmatrix}$$

1.3 轮密钥加

轮密钥加就是输入与轮密钥异或，简记为$Y=X\oplus K$，其中K是轮密钥。

1.4 密钥调度算法

密钥调度算法由两个模块组成：密钥扩展和轮密钥选择。N_b、N_k分别表示分组长度和密钥长度，单位是 4 字节字。N_b=分组位数 /32，N_k= 密钥位数 /32。R表示加密轮数。

对于 AES-128，N_b=4，N_k=4，R=10。AES-128 的密钥扩展是将 4 个 4 字节字的密钥扩展成 44 个 4 字节字密钥 W[·]，其中 W[0]，　　，W[3] 为原始密钥。扩展算法如下：

```
for(i=4;i<44;i++){
    if (i%4=0)
        W[i]=W[i-4] ⊕ BS(RotByte(W[i-1]) ⊕ const(i/4);
    else W[i]=W[i-4] ⊕ W[i-1]}
```

2 基于 AES 的智能手机门禁系统实现方案

2.1系统加密原理

系统使用 AES 加密算法，同时联合时间戳，引入了第二个因子，提高了加密算法的可靠性。同时，为了便于传输识别，将 AES 的加密结果每 4 位转换成一个 0~9 或 A~Z 的字符进行传输。加密的各个过程具体涉及的加密算法如下。

1）手机端资格认证部分

手机获取到手机原始标识码后，使用某一固定 16 位字符串进行 AES 加密，再在其后连接通信口令，形成新的字符串。该新字符串再通过一次 AES 加密就能得到资格认证服务中需要的密文，使用的密钥为经过补充的 16 位当前时间戳。二次 AES 加密示意如图 1 所示。

图1 二次AES加密示意图

2）服务器端资格认证部分

服务器端通过开锁资格认证后，准备返回字符串。首先获取与锁控制器商量好的明文开锁命令，同时随机生成一串字符串作为密钥对开锁命令进行 AES 加密。加密后，将密钥混淆进入密文中，混淆方法类似海明码，即在其第$2^i(i=0,1\cdots)$位的位置插入密钥字符。当插入密钥字符的位置大于当前待混淆密文字符串长度时，则将剩余密钥字符串直接拼接在待混淆密文后。混淆密文流程示例如图 2 所示（由于 128 位密钥太长，故使用 40 位密钥做说明）。

图2 混淆密文

混淆最后一个字节密钥时，此时密文长度不足 15 字节，故 E 直接跟在密文之后。

得到这样的开锁密文后，再在其后连接新的用户通信口令，经过以补充时间戳作为密钥的 AES 加密得到最终密文，然后将其返回给手机设备。

2.2 多端通信原理

多端通信原理以手机开锁动作的整个流程为例进行说明，通信多方如图 3 所示。实际操作中，可以使用一台不关机或定时开机的计算机作为服务器。

1）用户通过手机应用程序进行开锁操作，应用程序自动向服务器完成资格认证操作。

2）资格认证通过后，服务器将开锁密文以及下次该用户

的通信口令打包并再加密后发回手机应用程序。

3）手机应用程序解析服务端返回信息后，将开锁密文通过蓝牙发送给锁的控制设备，并将当前通信口令替换为接收到的通信口令，以备下次通信使用。

4）锁的控制设备将收到的混淆密文逆向解析后，得到密文和密钥，对其解密后，得到明文。将其与设备内置的开锁命令进行匹配，匹配成功后，进行开锁动作并返回成功信息。如果匹配不成功，返回错误信息给手机。

5）手机应用程序收到锁的控制设备的反馈信息后，将该次操作的成功信息反馈给服务器端，完成一套开锁动作并记录。

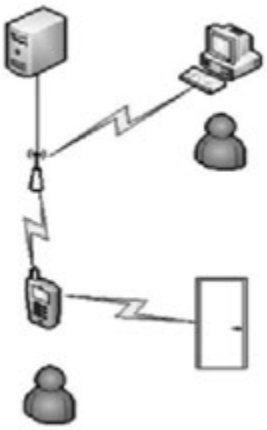

图3 多端通信示意图

2.3 系统总体实现方案

系统共分成 3 个部分来实现：手机端、服务器端和门锁。如图 4 所示，整个软件一共分为 3 个模块。

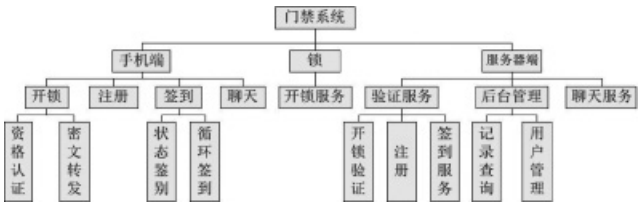

图4 系统框架图

1）手机端。手机端应用程序使用 SOAP 协议 [5] 与架设在服务器上的 WCF 服务 [6] 进行交互。手机的特殊标识码经过加密算法加密后，传输给服务器端进行资格认证。将得到的返回数据进行解密，获取下次通信口令以替换当前口令，并将开锁密文通过蓝牙模块的 SPP 协议 [7] 转发给门锁控制器，执行开锁服务。根据开锁情况，将结果反馈给服务器端。于此同时，在手机未进行注册的情况下，手机应用程序将提供一次性注册服务，该服务可将手机信息发往服务器进行资格注册。手机内还寄宿着一个服务，当监测到连接上 Wi-Fi 服务时，将会自动判断是否存在签到服务，如果存在，将进行后台循环签到。此功能联合服务器端提供的后台查看功能，做到粗略的对房间人员的考勤。同时，应用还提供一个实时聊天功能，方便使用人员内部交流。在通信过程中使用双重加密算法加密，防止消息被监听导致信息泄露。

2）服务器端。根据需要分为 3 部分。第一部分是验证服务，主要负责手机端的服务验证，验证该手机是否具有开锁资格、新用户的注册以及签到服务。还负责通信过程中对于敏感信息进行加密处理，以防数据包被截获后很容易被破解，从而对整个系统造成破坏。第二部分是后台管理，主要负责新注册用户的权限管理以及注册用户的记录查询，可以做到监控当前时间房间是否有人以及有哪些人。后台管理还可以加入用户权限并使用 session 机制和 SQL 防注入处理以提高安全性 [8]。第三部分是聊天服务器，通过对 openfire[9] 的二次开发，提供一个实时的聊天服务，如果用户不在线，还会对聊天信息进行离线存储，用户下次登录时再进行推送。

3）门锁。使用 Arduino[7] 作为锁的控制器，并搭载蓝牙通信模块。将控制器与电机锁、供电设备以及稳压电路相连，形成整个门锁模块（如图 5 所示）。门锁模块通过蓝牙模块接收信息，经过解密得到开锁明文。将明文与设备内置的开锁命令进行匹配，匹配正确后，控制器控制电机锁开锁，并返回成功信号给手机。之后，电机锁自动进行上锁动作，若上锁未成功，会产生报警反应。

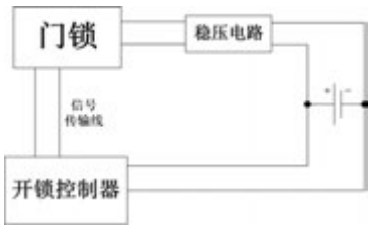

图5 门锁电路图

3 系统测试及安全性分析

3.1 系统测试

依据本文所述思想完成主要编码工作 [5]，其中后台管理模块完成登录、查看系统基本信息、查看单用户签到记录、查看在线用户、查看开锁记录、用户搜索、添加后台管理员、验证新用户和查看所有用户信息共 9 个功能。在对整个门禁系统反复测试过程中，出现如下问题：开锁过程中，若电池供电不足，手机蓝牙无法接收到开锁反馈，但是仍可打开门锁。其余注册和聊天功能以及后台管理系统一切运行正常，达到预计目标。

3.2 系统安全性分析

3.2.1 AES安全性分析

通过对已知的攻击方法（穷举攻击法、差分攻击法、线性攻击法、积分攻击法和内插攻击法）进行分析 [10-13]，可以看出 AES 算法对已知的攻击具有较好的免疫性，安全性比较高 [18-20]。

3.2.2 资格认证安全性分析

由于资格认证处于开放的网络环境中，所以它存在以下 4

种攻击：截获、中断、篡改和伪造。尽管中断和篡改会影响用户的开锁服务，但不会造成非授权用户的非法访问，因此我们这里只对截获与伪造攻击进行测试。修改应用程序模拟攻击者截获某次资格认证过程中的数据包，然后进行重发。在多次试验中均返回资格认证失败的信息，意味着此种攻击方式无法达到效果。主要原因在于动态口令[14]的引入，每次资格认证后，都会导致通信口令随之改变，截获的数据包中经过加密的通信口令已经与当前服务器端数据库中通信口令不同，故无法通过资格认证。

3.2.3 蓝牙安全性分析

蓝牙系统由于其网络开放性原因，在其连接的时候，分为链路层加密和服务层加密，分别在匹配前和匹配后进行[15]。在匹配时，攻击者无法知道其匹配 PIN 码，故 PIN 码提供了最简单的防护，此外我们还提高了 PIN 码的位数，以此来提高蓝牙模块的安全性。

假设攻击者截获了数据包，由蓝牙系统的安全性可知，其在每次传输数据的时候，均会动态生成一个密钥对数据进行加密[16,17]，故攻击者即使截获了数据包，也无法得到真正的明文，所以无法对用户行为进行模拟。

3.2.4 后台管理安全性分析

1）后台管理网站除登录页外全部采用 session 机制，用户浏览、操作其他页面必须先登录才行，有效防止非管理人员查看和管理网站。与 cookie 机制不同，cookie 机制是将用户信息保存在客户端并受浏览器设置限制，且不能防止 cookie 欺骗，session 机制是将用户信息保存在服务器端，与浏览器设置无关，从而有效防止他人获得 cookie 进行欺骗登入，大大提高网站安全度[9]。

2）后台管理网站所有页面均对提交的表单内容进行过滤，防止 SQL 注入，且管理用户的密码采用 MD5+salt 方式存储，其安全程度远高于单纯的 MD5 加密，即使数据库泄露管理用户的密码也很难破解。

4 结束语

本系统采用 Arduino 作为控制器开发板，使用蓝牙技术作为板与系统之间的通信方式，采用 WCF 资格认证服务，并且配备后台管理系统。在系统安全性方面，通过在 AES 加密算法中引入动态口令，有效地提高了系统的安全性。并且使用智能手机本身具有的蓝牙功能进行通信，降低了硬件成本，有利于市场的推广。而且在系统中加入了签到功能，方便管理员查看当前在线用户以及某一用户的在线记录，进一步方便了管理。

在以后的工作中系统还可以在以下这些地方进行改进与优化：

1）控制器中加入存储器，使得通信过程不传递密钥，而只传递密文，且引入动态口令。

2）优化签到功能，使得签到时间更加精确。

3）服务器端提供加密算法选择，可以根据用户需要，选择安全性更高的加密算法。（责编 马珂）

参考文献

[1] Daemen J, Rijmen V. AES Proposal: Rijndael, Version2[EB/OL]. http://www.esat.kuleuvan.ac.be/ rijndael , 1999-09-03.

[2] 马虹博 , 刘连浩 . AES 的 S 盒和逆 S 盒的代数表达式 [J]. 计算机工程 , 2006, 32(18): 149-151.

[3] 何明星 , 林昊 . AES 算法原理及其实现 [J]. 计算机应用研究 , 2002, 19(12): 61-63.

[4] Yu SASAKI. Known-key attacks on rijndael with large blocks and strengthening shiftrow parameter[J]. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 2012, E95-A (1):21-28.

[5] 刘志都 , 贾松浩 , 詹仕华 . SOAP 协议安全性的研究与应用 [J]. 计算机工程 , 2008, 34(5):142-144.

[6] 李雪东 . 基于 WCF 面向服务架构的研究与应用 [D]. 长春 : 长春理工大学 , 2009.

[7] 郑昊 , 钟志峰 , 郭昊 , 许骏 . 基于 Arduino/Android 的蓝牙通信系统设计 [J]. 物联网技术 , 2012, (05):15-34.

[8] 卜英奇 . 网站安全技术的分析及应用 [D]. 长春 : 吉林大学 , 2007.

[9] 罗伟 . 基于 Android 平台的即时通讯系统的研究与实现 [D]. 长沙 : 湖南师范大学 , 2009.

[10] BRIAN GLADMAN. Implementations of AES(Rijndael) in C/C++ and Assembler[EB/OL]. http://fp.gladman. plus.com/cryptography_technology/rijndael/index.htm, 2000-10-15.

[11] 贾旭 . AES 算法的安全性分析及其优化改进 [D]. 长春 : 吉林大学 , 2010.

[12] 韦宝典 . 高级加密标准 AES 中若干问题的研究 [D]. 西安 : 西安电子科技大学 , 2003.

[13] 郑世慧 , 王小云 , 王美琴 , 张国艳 . SAFER++ 的差分分析 [J]. 计算机工程与应用 , 2005, 41(30):21-23.

[14] 韦广剑 . 基于 Android 令牌的动态密码认证系统的研究与实现 [D]. 武汉 : 武汉理工大学 , 2012.

[15] 眭俊华 , 张海盛 . 蓝牙技术安全性解析 [J]. 计算机应用 , 2002, 22(10):13-14.

[16] Bisdikian C. An overview of the Bluetooth wireless technology[J]. Communications Magazine, 2001, 39(12): 86-94.

[17] 陈立志 , 李凤华 , 戴英侠 . 基于动态口令的身份认证机制及其安全性分析 [J]. 计算机工程 , 2002(10): 48-49.

[18] Iqtadar Hussain, Tariq Shah, Muhammad Asif Gondal, Waqar Ahmad Khan. Construction of Cryptographically Strong 8x8 S-boxes[J]. World Applied Sciences ,2011, 13 (11): 2389-2395.

[19] Mohan H.S, A. Raji Reddy. Revised AES and Its Modes of Operation[J]. International Journal of Information Technology and Knowledge Management, 2012, 5 (01): 31-36.

[20] Marine Minier, Raphael C. -W. Phan, Benjamin Pousse. On integral distinguishers of Rijndael family of ciphers[J]. Cryptologia, 2012, 36 (2): 104-118.