计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(5):56−64 [doi: 10.15888/j.cnki.csa.006365]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于 RSA 算法的智能锁设计①

王思远[1], 朱敏玲[2], 温智博[3], 王　胜[3]

[1](北京信息科技大学 计算机学院 计算机科学与技术系, 北京 100101)
[2](北京信息科技大学 计算机学院, 北京 100101)
[3](北京信息科技大学 计算机学院 软件工程系, 北京 100101)
通讯作者: 王　胜, E-mail: 1028742881@qq.com

摘　要: 提出了一种可通过手机远程分享钥匙的智能锁模型, 并提供了一套能使系统完整运行的硬件模型. 在如今的智能锁领域, 普遍只是将指纹、密码、刷卡、蓝牙开锁功能相结合, 却少有钥匙分享功能. 为了保障钥匙分享过程中钥匙的保密性和时效性, RSA 算法可以较好的满足要求. 为了保证系统的完整性, 对硬件系统 (指纹、刷卡解锁) 也提出了一套基于 STM32F103 型低功耗单片机为控制器的可执行设计方案. 实验结果表明系统可以较好的实现钥匙分享的功能.

关键词: STM32; RSA; HC-05; 智能门锁; 智能钥匙分享

引用格式: 王思远,朱敏玲,温智博,王胜.基于 RSA 算法的智能锁设计.计算机系统应用,2018,27(5):56–64. http://www.c-s-a.org.cn/1003-3254/6365.html

Design of Intelligent Lock Based on RSA Algorithm

WANG Si-Yuan[1], ZHU Min-Ling[2], WEN Zhi-Bo[3], WANG Sheng[3]

[1](Department of Computer Science and Technology, Computer School, Beijing Information Science &Technology University, Beijing 100101, China)
[2](Computer School, Beijing Information Science and Technology University, Beijing 100101, China)
[3](Department of Software Engineering, Computer School, Beijing Information Science &Technology University, Beijing 100101, China)

Abstract: This paper presents a description of the intelligent-lock model which could remotely share its key through smart phones. It also provides a set of hardware models that make the whole system function normally. The facility of sharing the keys is surprisingly rare in today's field of intelligent locks. Instead, the combination of different means, such as passwords, access cards, fingerprints, and Bluetooth, is widely used to unlock intelligent locks. But as is shown in this paper, the RSA algorithm makes a better effect on realizing the keys' confidentiality and timeliness while sharing the keys. As for hardware system, for instance, used for unlocking through fingerprints or access cards, we can also find a workable design based on the controller made by low-power STM32F103 single chip. The result shows that the system can actualize the function of sharing keys well.

Key words: STM32; RSA; HC-05; intelligent door lock; intelligent key sharing

电子密码锁是在传统机械密码锁的基础上改进的采用密码输入控制电路或控制芯片实现开锁、闭锁的电子密码锁产品. 电子密码锁从性能、安全性、稳定性以及用户的受欢迎程度远远高过传统机械密码锁: 电子密码锁保密性好,密码选样更多 (密码数量远高于传统机械密码锁), 破解密码的可能性很低. 电子密码

① 基金项目: 北京信息科技大学 2017 年人才培养质量提高经费 (5111723400)
收稿时间: 2017-09-09; 修改时间: 2017-09-30; 采用时间: 2017-10-17; csa 在线出版时间: 2018-04-23

锁的安全性更高, 更好地保护用户的生命财产安全.

从锁的发展趋势上出发, 目前主要向刷卡、手机 APP 等方向进行, 特别是目前智能家居产业的蓬勃发展, 其发展趋势与智能家居相融合, 功能性上越来越人性化. 再加上近年以来, 随着国家对物联网的极大支持和投入, 物联网这个产业也再飞速的发展. 互联网的发展更是推动了安全产业的技术革新. 所以, 我们的安防系统则是变得更加的智能化. 人工智能、云计算、嵌入式芯片、智能处理功能等等将要大量投放到和安防相关的产品中去.

本文的其余部分安排如下: 在第 1 节中, 介绍系统整体设计架构; 在第 2 节中, 介绍了系统功能的实现; 在第 3 节中, 进行了系统测试说明和实验结果分析; 在最后一节, 对本系统功能及研究功能进行总结.

1 系统设计及架构

1.1 系统设计

硬件方面, 利用 ST 公司生产的 STM32 单片机控制, 通过射频卡、指纹、手机蓝牙等方式实现开锁, 从而实现家居开锁的智能性和简便性. 本设计要求利用 STM32 作为主控芯片完成主控电路的设计, 辅助电路要求包括射频刷卡电路、蓝牙电路、电源电路等.

手机端方面, 利用 Android Studio 软件设计 APP, 使其完成添加 (电子) 钥匙、分享钥匙、使用钥匙的功能.

1.2 系统架构

该系统的主要设计思路如图 1 所示. 当使用 IC 刷卡时, 单片机单片机读取 RFID 数据: 若是刷卡成功, 则蜂鸣器不响, 单片机通过驱动电磁锁驱动电路控制电磁锁开锁; 若是刷卡失败, 蜂鸣器鸣报警. 当使用指纹开锁时, 指纹模块采集指纹信息: 若是匹配成功, 则蜂鸣器不响, 单片机通过驱动电磁锁驱动电路控制电磁锁开锁; 若是匹配失败, 蜂鸣器鸣报警. 当使用蓝牙开锁时, 此时手机 APP 连接系统的蓝牙模块, 并且向蓝牙模块向蓝牙模块发送数据. 蓝牙模块与单片机之间使用串口通信, 当单片机接收到数据以后, 校验数据是否准确, 当数据正确时, 单片机通过驱动电磁锁驱动电路控制电磁锁开锁.

1.2.1 单片机选型

单片机系统电路设计中单片机的选型至关重要, 对于一个已经规划好明确模块和任务指标的系统来说, 可以根据它的模块与要实现的功能去选择所需要的单片机的型号. 在选型的过程中, 倘若选取了功能较少的机型, 那么该单片机搭建的系统电路就可能不能完成预定的控制任务; 倘若选取的机型功能非常强大, 超出了系统设计方案的实际需求便会造成功能资源的浪费, 这样非但没有必要还白白的增加了设计的成本. 综合对成本和实用性的考虑, 本设计拟选择意法半导体公司生产的 STM32F1xx 系列单片机.

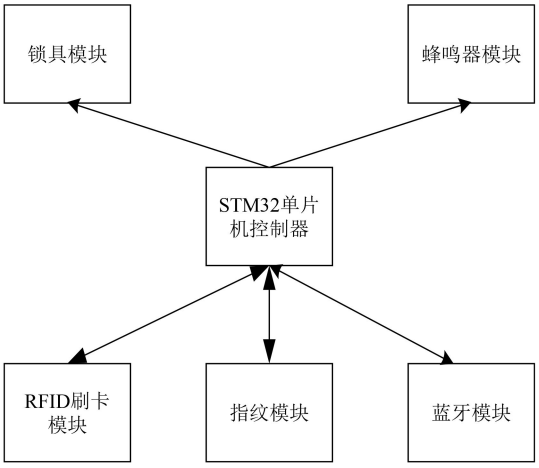

图 1 系统架构

STM32F1xx 系列单片机处理器大致可分为标准型和增强型两个大类. STM32F101 系列型单片机为标准型, 工作频率在 36 MHz; STM32F103 系列型单片机为增强型, 工作频率在 72 MHz, 而且具有更好的性能和更完善的内部模块以及支持更多拓展的外部设备. STM32F103 系列单片机是首款搭载 ARMv7-M 内核的 32 位标准 RISC(精简指令集) 单片机控制器, 它既能满足高性能的使用要求, 又可以保持低功耗的用电状态, 既能适应低预算低成本的小设施的开发, 又能满足复杂应用高端市场的性能要求, 而且便宜适宜的价格绝对物超所值[1].

ST 公司生产的 STM32F103 芯片具有低功耗、运行速度快、成本低, 抗干扰强等功能, 该芯片运行主频可达 72 MHz, 能够满足系统的处理需要. 该芯片集成多个定时器, 可以满足采集系统信息的需要.

1.2.2 RFID 刷卡模块选型

方案一. 采用 Mfrc522 刷卡模块. 该模块使用常用的 MFRC522 模块进行设计, 同时具有板载天线, 能够在读卡时对 IC 卡片进行充电处理. 同时由于该模块在市场上应用较广, 其模块可以成本价格较低的基础上实现灵敏刷卡、写卡等操作. 同时, 由于该模块的广泛应用, 目前其设计方案、使用方案的都相对成熟, 购买

渠道广泛. 该芯片为汽车级芯片, 可以满足家居的使用环境.

方案二. 采用 RDM6300 ID 卡读卡器. 模块采用 125 kHz 通信, 其与单片机通信为串口通信. 该模块具有识别灵敏的特点, 在一些工控场合应用较多. 该模块在使用时需要外接电线, 才能实现对 IC 卡的通信、充电. 由于该模块应用较少, 购买渠道相对单一.

方案一的成本只有方案二的 1/3, 同时方案二需要外接天线才能使用, 使用较为麻烦. 综合考虑设计的成本、操作的实用性和可靠性、传感器的灵敏度等因素, 本设计选择采用 Mfrc522 刷卡模块作为我们的野外定位系统的传感器.

该模块使用飞利浦公司生产的 MFRC522 射频芯片为核心生产的. 该模块是 13.56 MHz 的感应式高集成度的射频刷卡芯片, 其芯片外部电路简单, 成本较低, 能支持 14443A 兼容应答器信号. 其供电电压为 3.3 V, 工作电流为 13~26 mA, 功耗相对较小. 在空闲状态下工作电流只有 10 mA 左右, 能够满足使用时续航的要求. 同时该芯片能够满足 S50、S70 等多种 IC 卡, 其兼容性可以满足该系统要求[2,3].

1.2.3 指纹模块选型

指纹模块按其指纹识别方式可以分为 3 类: 光学指纹模块、电容指纹模块和射频指纹模块 (刮擦指纹模块). 其中使用最普遍的为前两类, 其中在成像能力上基本相同, 但在汗液较多和较脏的手指光学指纹模块可成较模糊的像; 在分辨率上, 两者表现相当; 在耐用性上, 光学指纹模块更是胜过电容指纹模块; 同时光学指纹模块还具有耗电量少的有点. 所以, 本系统决定选择光学指纹模块.

1.2.4 蓝牙模块选型

该设计采用 HC-05 蓝牙模块进行蓝牙数据传输. 蓝牙采用分散式网络结构以及快跳频和短包技术, 支持点对点及点对多点通信, 工作在全球通用的 2.4 GHz ISM(即工业、科学、医学) 频段. 其数据速率为 1 Mbps. 采用时分双工传输方案实现全双工传输, 使用方法简单方便, 运行可靠稳定. 硬件上使用串口 RX\TX 与单片机通信.

2 系统功能的实现

2.1 系统硬件功能的实现

在该设计中, 系统在初始化完毕以后, 需要等待执行 RFID 刷卡任务, 指纹适配任务以及蓝牙串口通信任务等, 当刷卡成功, 指纹配对成功或者蓝牙通信成功以后, 驱动电磁锁进行开锁等任务. 如图 2 所示.

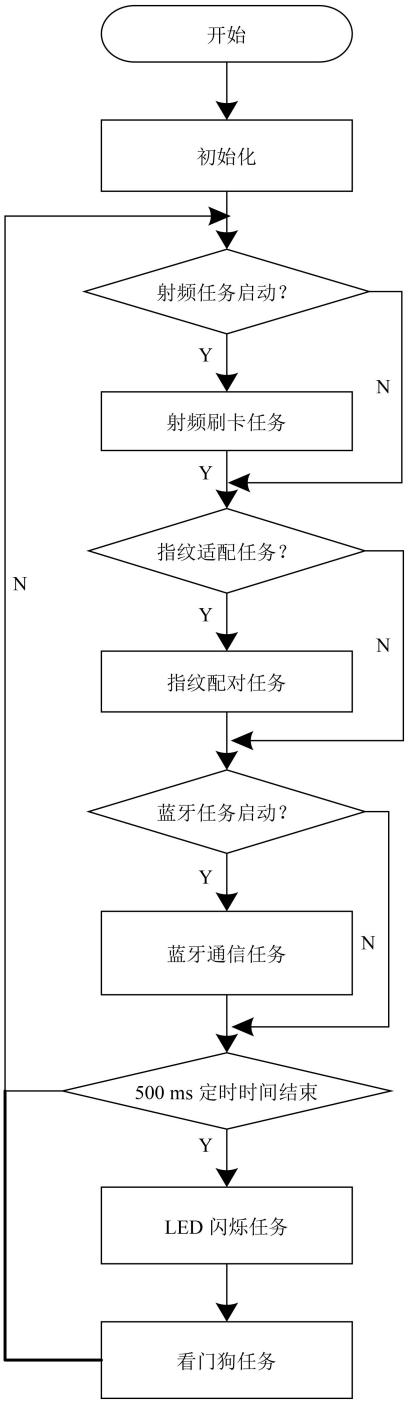

图 2 系统功能

系统初始化任务主要包括定时器初始化、蓝牙串口初始化、RFID 初始化、LED 初始化、蜂鸣器初始化以及电磁锁初始化等.

2.1.1 RFID 开锁实现

当有标签接近阅读器时, 进行检测, 读取标签内信息与系统信息匹配. 匹配成功时, 调用函数开锁, 失败时通过蜂鸣器报警.

2.1.2 指纹开锁的实现

通过 USB 接口与电脑连接, 通过上位机软件对指纹进行录入, 对每一枚指纹录入 2 次, 分别将采集到的指纹图像生成特征指令文件存于 CharBuffer1Img2Tz()/CharBuffer2Img2Tz() 中, 调用 RegMode() 特征合成模板,同时通过 Store() 指令, 指纹存储成功.

进行指纹匹配时, 通过指纹头光学传感器, 采集要验证指纹图像, 通过 GenImg() 指令读图像, 调用 Search() 与模块中的指纹模板进行匹配比较, 模块给出匹配结果 (通过或失败). 控制器与指纹模块通过通讯协议完成交互.

使用到模块自带的指令: GenImg 录指纹图像; Img2Tz 图像转特征; Match 指纹比对; Serach 搜索指纹; RegModel 特征合成模板; Store 存储模板.

特征文件缓冲区: 特征文件缓冲区 CharBuffer1 或 CharBuffer2 既可以用于存放普通特征文件也可以用于存放模板特征文件. 其框架图如图 3.

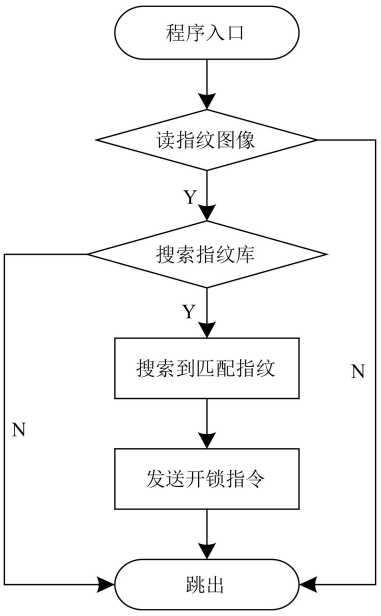

图 3 指纹开锁流程

2.1.3 射频程序设计

在该设计中, 需要先对 RFID 初始化, 其初始化分为两部分, 一部分对单片机 SPI 进行初始化, 另一部分是对 RFID 模块进行初始化. 其初始化程序如下:

```
Void RC522_Init(void){
  RC522_SPI_Config();
  MacRC522_Reset_Disable();
  MacRC522_CS_Disable();
}
```

初始化完毕后, 需要对在程序里检测是否有刷卡任务, 刷卡是首先驱动 RFID 模块进行寻卡, 若是寻卡成功, 则进行防冲撞处理. 防冲撞处理主要是防止多张卡进入刷卡范围, 造成刷卡冲突或者失误. 若是有多张卡进入刷卡范围, 防冲突机制会从其中选择一张卡进行识别通信. 当通信成功后, 单片机读取卡的序列号, 然后将该序列号与程序内置的序列号进行比较, 若是该序列号正确, 则说明该卡是家庭内部卡, 然后驱动继电器开锁. 若是卡识别错误, 则进行报警处理[4,5].

2.1.4 软件定时处理任务

在该设计中, STM32 单片机需要定时采集卡片、指纹信息、执行看门狗任务等, 并且在定时器内闪烁 LED 灯表示系统状态正常, 在该设计中, 系统定时采用定时器 0 进行系统定时. 在初始化时, 单片机定时器 0 被设置为 10 ms 定时中断, 即单片机每 10 ms 进入一次定时中断. 当单片机每次进入定时中断时, 系统使用一个定时器中断计数变量对 10 ms 定时中断进行计数, 当该变量累加到 10 的倍数时, 说明该系统已经过去 100 ms, 将 100 ms 定时标志置一. 同理, 加到 50 的倍数即 500 ms 定时到来[6].

2.1.5 软件抗干扰设计

为了系统能够正常的运行, 外界干扰的因素应该受到高度的重视, 所以本装置中设置了软件抗干扰的程序.

为防止程序陷入死循环, 系统采用了“看门狗”这一软件设计. 很多时候, 由于一些不可避免的干扰因素,系统主程序或者中断子程序会处于卡机或者当机的状态, 整个系统就不能照常的进行监控, 会危害到人生财产安全. 因此, 在本装置中进行了这方面的设置. “看门狗”技术就是本次系统设计的软件设计, 其工作原理为: 当系统上电运行后, “看门狗”计时器随之启动, 在系统正常工作过程中, “看门狗”计时器自动计时, 正常状态下, 计时器在达到设定的数值后自动清“看门狗”; 如果一段时间内“看门狗”没有被清零而导致溢出的话, 说明系统陷入非正常工作状态, 这时系统会自动复位, 从而重新进行工作. 看门狗工作流程图如图 4 所示.

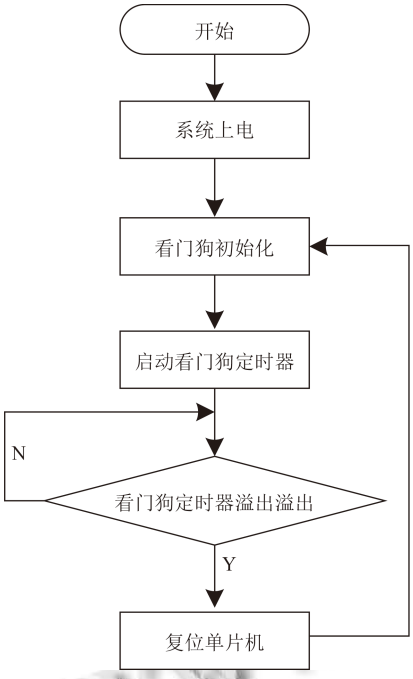

图 4 看门狗程序

2.2 手机 APP 端软件功能的实现

2.2.1 软件开发工具

Android Studio (PC 端安卓应用开发软件)

2.2.2 软件功能升级

(1) 分享 (电子) 钥匙

用户在没有开锁的蓝牙钥匙时, 可以打开手机应用, 选择向好友 (户主) 索取钥匙的功能, 应用会根据 RSA 算法随机生成一对公钥密钥, 并将密钥隐藏存储在系统内部, 将公钥加入索取钥匙文本并加密, 向用户返回生成的索取钥匙文本. 用户向好友分享文本信息, 好友复制文本信息并打开应用, 通过应用解析并获得索取钥匙文本内包含的 RSA 公钥, 根据好友选择分享的钥匙加密后生成回执文本. 好友将生成的回执文本返回给用户, 用户复制回执文本信息后打开应用, 通过应用解析回执文本内的信息并通过之前生成的 RSA 密钥解密文本, 解密成功则由用户确认操作后将分享的钥匙加入数据库.

(2) 钥匙的时效性

应用在重启应用或完成一次钥匙分享或重新申请钥匙分享时, 都会重置本地的 RSA 私钥, 以此来保证门锁分享码不会产生混淆和滥用情况.

(3) 开启门锁

用户打开手机应用, 选择开启门锁功能, 应用检测门锁蓝牙状态并尝试连接, 连接成功则通过蓝牙向门锁发送开启门锁指令. 否则开锁失败.

(4) 关于分享门锁功能的补充

分享门锁时, 用户可以对分享门锁做出例如使用次数、使用时间段等限制. 开启门锁时, 应用通过每次启用该钥匙时查询该钥匙限制条件来确定是否发送开门指令 (对于使用时间段等限制使用时, 为了防止用户进行离线调整时间等操作, 应用强制用户在使用含有时间限制的钥匙时必须连接网络来确保时间正确). 好友与用户之间传送的文本信息可存放在二维码之中, 应用解析文本可改为应用识别二维码.

2.2.3 软件架构设计

本软件采用了三层架构, 将项目粗略划分为表现层、业务逻辑层和数据访问层.

表现层 (User Interface Layer, UIL): 用户操作界面. 将用户操作传输给业务逻辑层并根据用户逻辑层返回的数据对用户操作做出响应.

业务逻辑层 (Business Logic Layer, BLL): 功能实现模块. 通过数据访问层执行对数据的操作集合来达到功能的实现.

数据访问层 (Data Access Layer, DAL): 数据操作模块. 对存储的数据进行增删改查操作的简单模块.

具体软件架构设计以及各个分层之间的交互设计如图 5.

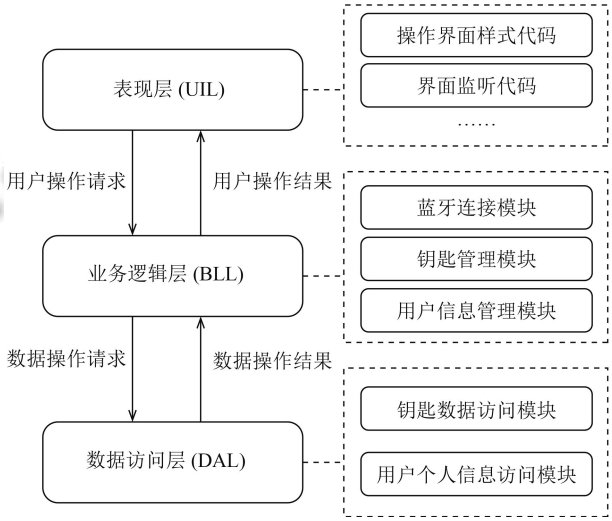

图 5 软件架构

2.2.4 相关知识及算法

(1) RSA 公钥加密算法

RSA 公开密钥密码体制. 所谓的公开密钥密码体制就是使用不同的加密密钥与解密密钥, 是一种“由已知加密密钥推导出解密密钥在计算上是不可行的”密

码体制, 因此可以极大的提高钥匙分享过程中的保密性. 在公开密钥密码体制中, 加密密钥 (即公开密钥)PK 是公开信息, 而解密密钥 (即秘密密钥)SK 是需要保密的. 加密算法 E 和解密算法 D 也都是公开的. 虽然解密密钥 SK 是由公开密钥 PK 决定的, 但却不能根据 PK 计算出 SK.

而带算法的实现基于一个十分简单的数论事实: 将两个大质数相乘十分容易, 但是想要对其乘积进行因式分解却极其困难, 因此可以将乘积公开作为加密密钥[7].

RSA 的算法涉及三个参数, n、e_1、e_2. 其中, n是两个大质数 p、q 的积, n 的二进制表示时所占用的位数, 就是所谓的密钥长度.

e_1和e_2是一对相关的值, e_1可以任意取, 但要求e_1与$(p-1)*(q-1)$互质; 再选择e_2, 要求如下:

$$(e_2*e_1) \bmod (p-1)*(q-1)=1 \tag{1}$$

(n,e_1), (n,e_2) 就是密钥对. 其中(n,e_1)为公钥, (n,e_2) 为私钥.

RSA 加解密的算法完全相同, 设 A 为明文, B 为密文, 则:

$$A = B^{e_2} \bmod n \tag{2}$$

$$B = A^{e_1} \bmod n \tag{3}$$

公钥加密体制中, 一般用公钥加密, 私钥解密, $e1$ 和 $e2$ 可以互换使用, 即:

$$A = B^{e_1} \bmod n \tag{4}$$

$$B = A^{e_2} \bmod n \tag{5}$$

(2) 二维码传递信息

通常大家所说的二维码是指的是矩阵式二维条码, 是建立在计算机图像处理技术和组合编码原理等基础生的一种编码机制. 原理主要是在一个矩形的区域内, 通过白点黑点的排列组合来传递信息, 在某一个位置上, 白点 (空点) 代表二进制的“0”, 黑点代表二进制的“1”.

二维码的三个角上的方块叫做这个二维码的定位点, 有了这三个点, 不管二维码从哪个方向识别, 都能正确的识别出信息. 由于三点就可确定一个平面, 所以二维码的第四个角则节省出来以便存放更多的信息.

在三个定位点构成的三角形的两条直角边就叫做二维码的定位图形, 它决定二维码中模块的坐标. 分隔符则是围绕在定位点周围的空白线, 它的作用是将定位点与其他信息分割开.

每个二维码都有一个版本号, 这个版本号的信息则储藏在二维码左下角定位点的上方. 而二维码才用的编码格式信息则储藏在三个定位点的周边.

在二维码的其他区域存放的就是数据信息和纠错码信息, 当用户扫描二维码时, 不能保证扫描到所有信息都正确, 这时纠错码就起作用了.

此外, 当二维码被恶意撕毁时, 位于二维码中心位置的矫正图形则保证了没有被撕毁的部分仍然可以被正常读取.

一个普通二维码的基本结构如图 6 所示.

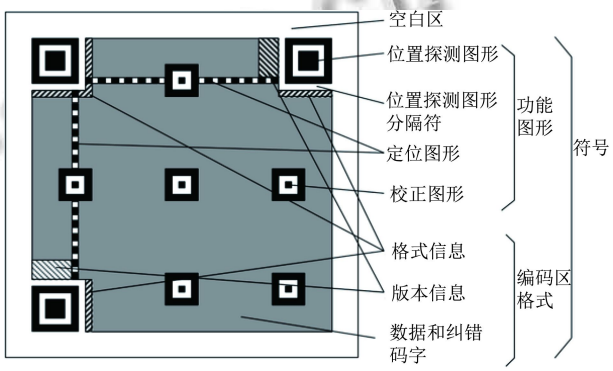

图 6 二维码结构图

3 测试及实验结果分析

3.1 系统测试

3.1.1 硬件系统

在该系统初始条件下, 电磁锁关闭, 如图 7.

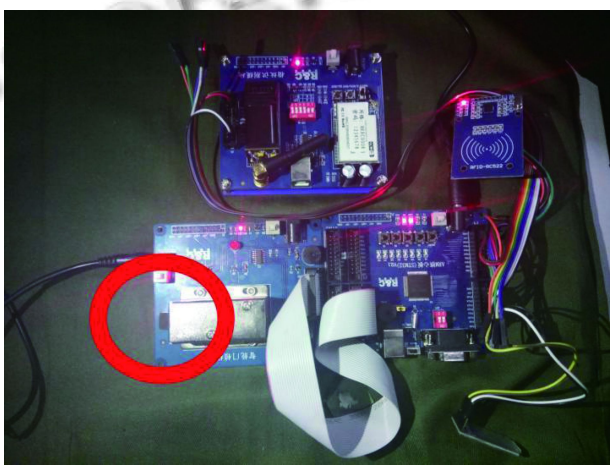

图 7 硬件初始状态

使用正确的 IC 卡刷卡, 识别成功, 锁开, 如图 8 所示.

维持 5 s 开启状态后, 电磁锁自动关闭, 接通指纹模块, 输入正确的指纹, 锁开. 如图 9 所示.

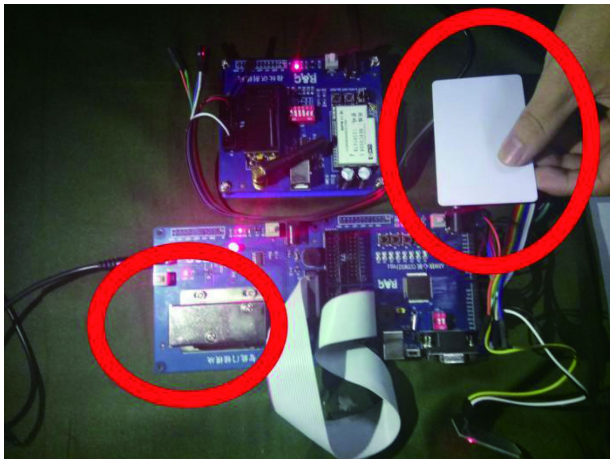

图 8 IC 卡开锁成功状态

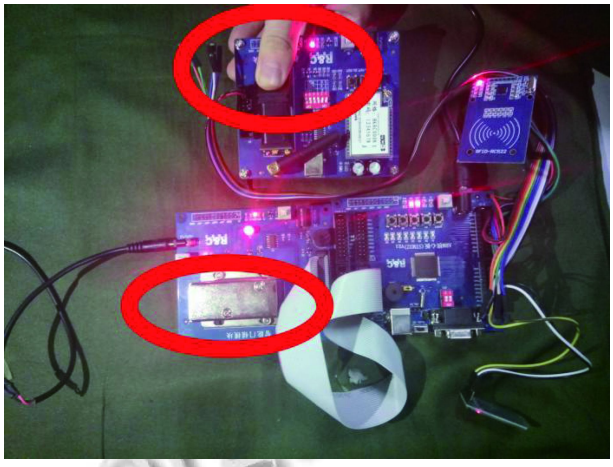

图 9 指纹开锁成功状态

3.1.2 手机端系统

表 1 给出了添加门锁设备测试用例, 表 2 给出了开锁测试用例, 表 3 是门锁索取测试用例, 表 4 是分享门锁的使用限制测试用例.

3.2 实验结果分析

经测试发现, 刷卡和指纹有效开锁次数可以达到 90% 左右, 失效情况发生在连续进行开锁操作时 (如连续刷卡, 指纹解锁等). 之后的改进中, 可通过对每次操作锁定, 来避免连续操作带来的冲突和开锁失效情况.

蓝牙信息传输的测试中, 蓝牙连接成功率在 95% 左右, 首次连接进行蓝牙开锁时, 发送开锁指令后, 会出现丢失指令的情况, 但是状态稳定后, 丢失指令的情况会消失. 经分析, 蓝牙初始状态下整个开锁流程不是很稳定, 但是具体原因还有待确定.

表 1 添加门锁设备测试用例

用例名称		添加门锁设备测试用例		
目的		测试搜索并添加门锁设备功能		
前提		用户给予应用蓝牙、GPS功能权限, 该门锁设备正常并在蓝牙搜索范围内		
流程	编号	操作	预期结果	实际结果
	1	打开APP	显示APP主界面	(同预期结果)
	2	点击“添加门锁”按钮	弹出门锁设备搜索界面	
	3	点击“搜索门锁”设备按钮	应用显示附近的蓝牙设备列表	(同预期结果)
	4	点击门锁对应蓝牙设备	跳转到蓝牙设备连接测试界面	(同预期结果)
	5	点击“连接测试”按钮	应用进行连接测试, 门锁在测试过程中会开关数次 测试结束后弹出对话框让用户确定是否门锁有反应.	(同预期结果)
	6	点击“门锁连接成功”按钮	跳转到门锁设备信息设置界面	(同预期结果)
	7	填写完门锁信息后点击 “完成”按钮	钥匙添加成功. 跳转到主界面, 并自动刷新门锁列表	(同预期结果)
	8	完成	门锁列表中含有刚刚添加的门锁设备	(同预期结果)
测试结果		该功能正常运作		

表 2 开锁测试用例

用例名称		开锁测试用例		
目的		测试开锁功能		
前提		门锁正常并在蓝牙连接范围之内, 且该门锁已经通过“添加门锁”功能添加成功		
流程	编号	操作	预期结果	实际结果
	1	打开APP	显示APP主界面	(同预期结果)
	2	点击门锁列表中要进行开锁操作的门锁设备	弹出该门锁信息界面	(同预期结果)
	3	点击“开门”按钮	弹出开门缓冲动画, 门锁开启	(同预期结果)

表 3 门锁索取测试用例

用例名称	门锁索取测试用例			
目的	测试已配对门锁的索取功能			
前提	两部安装了该APP的手机索取门锁的为(索取方), 分享钥匙的为(被索取方)			
流程	编号	操作	预期结果	实际结果
	1	打开APP(索取方)	显示APP主界面	(同预期结果)
	2	点击“门锁索取”按钮(索取方)	弹出门锁索取对话框, 内包含该次门锁索取的索取码	(同预期结果)
	3	点击“分享索取码”按钮(索取方)	应用弹出分享途径选择框	(同预期结果)
	4	点击“通过QQ分享”, 并分享给好友(索取方)	索取码分享成功	(同预期结果)
	5	复制索取码后打开APP(被索取方)	显示APP主界面, 并弹出钥匙分享界面	(同预期结果)
	6	在门锁列表中选取要分享的门锁, 点击分享(被索取方)	弹出门锁分享对话框, 内包含通过索取码加密的分享码	(同预期结果)
	7	点击“返回分享码”按钮(被索取方)	应用弹出分享途径选择框	(同预期结果)
	8	点击“通过QQ分享”, 并分享给好友(被索取方)	分享码返回成功	(同预期结果)
	9	复制分享码后打开APP(索取方)	显示APP主界面, 并弹出门锁添加确定对话框	(同预期结果)
	10	点击“确定添加”按钮(索取方)	门锁添加成功, 跳转到主界面, 并自动刷新门锁列表	(同预期结果)
	11	完成(索取方)	门锁列表中含有刚刚确定添加的门锁设备.	(同预期结果)

表 4 分享门锁的使用限制测试用例

用例名称	分享门锁的使用限制测试用例			
目的	测试分享门锁时对门锁使用进行限制的功能			
前提	事先已添加了三个分别含有时间期限限制、使用次数限制、使用时间段限制的分享门锁, 三个分享门锁都不在使用限制允许的使用范围内. 该门锁设备正常运作并在蓝牙连接范围内			
流程	编号	操作	预期结果	实际结果
	1	打开APP	显示APP主界面	(同预期结果)
	2	点击门锁列表中要进行开锁操作的门锁设备(含有时间期限限制)	弹出该门锁信息界面	(同预期结果)
	3	点击“开门”按钮	弹出警告对话框, 提示该门锁已经过了时间期限	(同预期结果)
	4	点击“我知道了”按钮	跳转到APP主界面	(同预期结果)
	5	点击门锁列表中要进行开锁操作的门锁设备(含有使用次数限制)	弹出该门锁信息界面	(同预期结果)
	6	点击“开门”按钮	弹出警告对话框, 提示该门锁已经超过了允许的使用次数	(同预期结果)
	7	点击“我知道了”按钮	跳转到APP主界面	(同预期结果)
	8	点击门锁列表中要进行开锁操作的门锁设备(含有使用时间段限制)	弹出该门锁信息界面	(同预期结果)
	9	点击“开门”按钮	弹出警告对话框, 提示不在该门锁使用时间段内	(同预期结果)
	10	点击“我知道了”按钮	跳转到APP主界面	(同预期结果)

综上, 该系统在当前状态下, 基本实现了最初设计的要求, 但是在系统稳定性上还需要继续改进.

4 结束语

手机端 APP 应用在很多方面还是不能满足到用户在“方便、安全”方面的期待, 例如分享钥匙步骤的繁琐, 钥匙信息存储的不安全性, 以及不能实现用户信息在多个设备间的转移操作等.

针对这些情况, 可以后续建立该应用的云端服务器, 将安全性交给云端来保障. 将所有钥匙信息存储在云端, 来代替把钥匙信息存储在个人手机上的不安全局面. 同时可以实现钥匙只能被唯一购买者标识, 一个用户在多个平台上用户信息共享等目标.

另一方面, 通过云平台, 用户之间的交流也将更加

方便, 通过云端验证的钥匙分享操作也会更加安全.

云平台可以实现用户端不存储任何安全级别高的私密信息, 这对对于安全性要求极高的本应用来说会是个很大的提升.

参考文献

1 刘军. 例说 STM32. 北京: 北京航空航天大学出版社, 2011.
2 张颖, 苗全利, 刘小华, 等. 一种基于 RFID 技术的室内定位系统设计. 电子设计工程, 2011, 19(15): 50–53. [doi: 10.3969/j.issn.1674-6236.2011.15.019]
3 Kim K, Kim M. RFID-based location-Sensing system for safety management. Personal and Ubiquitous Computing, 2012, 16(3): 235–243. [doi: 10.1007/s00779-011-0394-0]
4 王亚平, 龚华军, 甄子洋. 基于 ARM 的 GPS/BD2 组合接收机设计与实现. 电子测量技术, 2012, 35(12): 67–70. [doi: 10.3969/j.issn.1002-7300.2012.12.018]
5 史向男, 巴晓辉, 陈杰. 北斗 MEO/IGSO 卫星 B1 频点信号捕获方法研究. 国外电子测量技术, 2013, 32(4): 19–21, 50.
6 柯熙政, 刘娟花, 李建勋. 多模式组合定时设备设计与研制. 仪器仪表学报, 2013, 34(6): 1209–1217.
7 胡云. RSA 算法研究与实现[硕士学位论文]. 北京: 北京邮电大学, 2010: 9–10.