基于 RFID 二次认证加密的智能识别系统设计*

臧俊斌[1,2],白 洋[2]
(1.中北大学 仪器科学与动态测试教育部重点实验室,山西 太原 030051;
2.中北大学(朔州校区),山西 朔州 036000)

摘 要:针对目前智能安防系统低成本、便捷的应用需求,为提高 RFID 在实际应用中既要方便易实现又要安全、稳定的性能,设计了一种基于 RFID 二次认证加密的智能识别系统。该系统主要是基于 MIFARE-S50 卡的密钥存储分区和任意一个数据分区,借助哈希码算法的不可逆性,结合 UID(User Identification)完成智能识别系统的密钥认证实现。只有当数据和 UID 同时通过系统两次认证后,系统才能识别智能卡,从而做出相关识别动作,同时可有效识别并阻止复制卡认证。该系统支持 3 种工作模式:注册模式、工作模式、注销模式,可有效地确保用户的隐私和信息安全。经实验测试结果表明,该系统安全性高、稳定好、方便易操作,具有较高的应用和实践价值,可应用于学校、小区、公司等中型 RFID 智慧安防系统中限制非法人员的入侵。

关键词:RFID;MFRC522;认证加密;智能识别系统
中图分类号:TN911 **文献标识码**:A DOI:10.16157/j.issn.0258-7998.200237

中文引用格式:臧俊斌,白洋. 基于 RFID 二次认证加密的智能识别系统设计[J].电子技术应用,2021,47(6):77-81.
英文引用格式:Zang Junbin,Bai Yang. Design of twice authentication and encryption intelligent recognition system based on RFID[J]. Application of Electronic Technique,2021,47(6):77-81.

Design of twice authentication and encryption intelligent recognition system based on RFID

Zang Junbin[1,2],Bai Yang[2]
(1.Key Laboratory of Instrumentation Science & Dynamic Measurement,Ministry of Education North University of China,Taiyuan 030051,China;
2.North University of China,Shuozhou 036000,China)

Abstract:According to the low cost and convenient application demand of current intelligent security system, a novel identification system is designed in order to improve the convenience and stability of RFID in practical application based on RFID secondary authentication and encryption.The system is primarily come out of the key storage partition of MIFARE-S50 and any data partition, used the irreversibility of hash code algorithm, and UID is used as the authentication part in the key of intelligent recognition system.Only when the data and UID are authenticated twice by the system, then the smart card can be recognized and made relevant identification actions. At the same time, if system encounter a copy card, it can effectively identify and prevent the authentication. The system supports three working modes that are the registration mode, operating mode and logout mode, which can effectively ensure the privacy and information security of users.Actual experimental results show that the system has high security,good stability, and is convenient and easy to operate. And it has high application and practical value,and can be used in schools,communities, companies and other medium-sized RFID intelligent security systems to limit the invasion of illegal personnel.

Key words:RFID;MFRC522;authentication and encryption;intelligent recognition system

0 引言

自国内启动“金卡工程”以来,非接触式 IC 卡技术的发展及应用取得了一定的效果,例如小区门禁管理系统、家庭门禁管理系统以及办公室门禁管理系统等智能识别系统已经广泛的应用到人们的日常生活中[1-2]。但是仍然存在很多安全隐患,例如:(1)如果用户不慎丢失 IC 卡,或者由于某种情况被非法分子通过某种手段获取到 IC 卡号,然后将 IC 卡号复制到空白卡中,这有可能会造成用户信息泄露,甚至威胁到用户财产安全;(2)所有用户数据存储在服务器,管理员可以掌握所有

*基金项目:国家自然科学基金青年基金项目(62001430);校级基金项目(SZ2019003);教育部产学合作协同育人项目(201802022059);山西省研究生教育创新项目(2020BY101)

用户的信息，而有些用户不愿意将个人信息安全交给某个管理员以防止泄密。这些问题都致使RFID技术的应用推广受到限制，同时也使其便捷、高效的优点难以展现，进而束缚了技术变革带来的经济和社会效益。但是RFID标准的初步形成，将极大地推动RFID的应用和研究[3-7]。因此，为进一步解决目前“金卡工程”所带来的安全隐患瓶颈与安全等级越高成本越贵技术难题，推动RFID技术的实用性发展，需加强对智能识别系统的设计与研究。对此，本文利用基于8051内核的STC89C52、MFRC522模块、MIFARE卡等构建射频识别模块架构设计，实现在该读写模块基础上进行二次开发认证加密的自动识别方法，旨在提供一个安全等级较高、便携使用的智能识别系统，以解决目前智慧安全系统的瓶颈问题。

1 安全隐患

市面上常规的IC卡可以轻易被复制。丢失若不进行注销权限，卡被别人捡到或者通过空白IC卡全盘复制的新卡也是可以通过验证轻而易举地进入，其这种行为有一定的风险，涉及个人及公共安全。此外，在一些注册系统中，因为没有持卡者和具体卡号的绑定关系，失主在注销丢失IC卡的权限时，也会遇到无法确定注销哪一张卡这种问题。

同样地，将用户数据存储在服务器中也存在一定的被窃取的风险，进而使得窃取了IC卡信息的不法人员制作特定信息的复制品，其同样可以通过验证。

2 RFID认证原理与实现

无线通信技术中的射频识别技术(Radio Frequency Identifica tion，RFID)主要是通过电感耦合(近场通信)或电磁反向散射耦合(远场通信)方式实现读写器和电子标签的无机械接触数据通信[8-11]。

综合应用场合与功能的需求，本文RFID认证系统的射频模块读写器采用MFRC522芯片，此芯片具有低电压、低成本、小尺寸等的优点，其工作频段为13.56 MHz、集成度较高，并与ISO/IEC 14443 A/MIFARE 3种型号都兼容，拥有强大而有效的解调和解码电路，可实现与任意类型卡的近场通信。数字部分可提供帧校验、奇偶校验和CRC校验等多种校验方式。此外，MFRC522还拥有SPI、UART、I^2C等丰富的外设资源，方便系统的二次开发[9-14]。

本系统采用的电子标签是MIFARE S50智能卡，拥有8 Kbit的EEPROM。本文将EEPROM分为16个扇区，每个扇区分成4个块(Block0~Block3)，每块有16 B。绝对地址Block0块用于存储IC卡制造商代码，Block3用于控制块。控制块包括密钥A、密钥B、访问控制条件三部分，访问控制条件决定密钥A和密钥B的使用以实现对数据的读(Read)、写(Write)、增值(Increment)、减值(Decrement)、转存(Transfer)、恢复(Restore)等控制操作，每个扇区的密钥和存取控制独立设置，可以根据实际需要自行设定密码和存取控制，只有同时满足访问控制条件和密钥认证，读写器才能访问标签内用户数据，这样可确保每个分区的数据安全。其访问控制条件如表1所示。

系统认证时只有读写器和标签相互认证且在访问控制允许下验证密码后才能进行下一步数据操作，以确保操作的安全性。而通用识别系统的用户ID号则可以由任意读写器读取[15]，倘若用户不慎丢失IC卡，非法分子可以使用“Chinese Magic Card”复制该IC卡，用户的所有信息将直接暴露给非法分子。因此，本文提出的二次认证加密智能识别系统可提高用户安全等级。

3 系统工作原理

3.1 系统运行模式

系统工作思想就是利用读写器和标签必须在相互认证且访问控制允许下验证密码通过后才能访问数据，同时配合UID作为识别系统的Key。意味着只有在通过第二个身份认证的情况下才能访问数据或者进行下一步操作。

本系统具有3种工作模式：注册模式、工作模式、注销模式。

(1)注册模式阶段：进入注册模式需要输入密码，此密码由系统管理员保管。首先，读写器在这种模式下开放注册，将用户新卡注册入系统。具体是：系统给需注册的IC卡分配一个SID(System-ID)，显示到LCD屏上，IC卡主需牢记SID号，同时系统将此SID码对应的Joaat哈希码写入到IC卡特定扇区的块中。SID同UID作为整体保存到EEPROM数据存储单元；将需注册的IC卡的某一分组的某一块填充具体数据，同时将IC卡内区尾部的密钥A和密钥B更改。所有用户的IC卡经注册加入系

表1 访问控制条件

控制位(块号X=0~2)			控制条件(对块0、1、2)			
C1X	C2X	C3X	Read(读)	Write(写)	Increment(增值)	Decrement(减值),Transfer(转存),Restore(恢复)
0	0	0	Key A | B	Key A |B	Key A | B	Key A | B
0	1	0	Key A | B	Never	Never	Never
1	0	0	Key A | B	Key B	Never	Never
1	1	0	Key A | B	Key B	Key B	Key A | B
0	0	1	Key A | B	Never	Never	Key A | B
0	1	1	Key B	Key B	Never	Never
1	0	1	Key B	Never	Never	Never

统后，由管理员授权后可以进入工作模式。

(2)工作模式阶段：工作模式阶段可由解锁该系统的智能卡 ID 号确定，此时任何未经注册的 IC 卡和无法通过 UID+SID 哈希码组合验证的 IC 卡都无效，作为不合法 IC 卡不具有有效性。只有系统认定合法的用户才能正常识别，通过智能识别系统。如果用户不慎将卡丢失，为防止意外事故，需及时通知管理员注销。

(3)注销模式阶段：进入注销模式后，用户可以手动输入用户的 SID(十进制)进行注销。系统将通过用户提供的 SID 号对应生成 Jotta 哈希码检索并删除此卡所有相关信息，被注销卡的所有信息(包括 UID 和 SID)将会从 EEPROM 存储单元删除。

如上所述，此时丢失的卡即使被非法分子得到，且被得知 IC 卡的 ID 号也无妨，因为仍需破解密钥 A 或密钥 B 才能访问到用户卡的数据信息，而密钥 A 和密钥 B 又是结合用户 SID 生成的，卡里只存储了用户 SID 对应的哈希码，鉴于哈希码的不可逆性，所以非法分子无法获取真正的密钥，也就无法获得卡内存储的信息，密钥无法被泄露，这大大增加了破解和伪造用户卡的难度。另一种情况，若原卡被非法复制，只要失主及时在读写器端注销此卡，使用这张复制的卡同样无法通过验证，因为系统数据库中已经把原卡的 SID 和 UID 信息全部删除，复制的卡会被识别为不合法，也就无法通过读卡器端的验证。这就意味着用户的安全级别更高，小区安全或者家庭财产安全也更有保障。

3.2 哈希码

哈希码是一种算法，它不是唯一确定的一串字符。通过散列算法将任意长度的输入变换成固定长度的输出。不同的输入可能有相同的输出，但不可能从散列值来唯一的确定输入值。不同的哈希算法得出的哈希码差别迥异。

常用的哈希算法有 MD4、MD5 和 SHA-1 等。Joaat hash 全称为 Jenkin's "One at a time"hash，是一种简单高性能的字符串映射加密算法。其加密过程高效，加密后的密文具有不可逆和低字节的特点，适合于在代码容量较小的系统及实时系统中使用。对于 RFID 用户验证的应用满足这两个特点，故选用此加密方式。

4 系统组成

本智能识别系统由完整且功能完备的硬件和软件构成。由模块化思想设计的硬件结构大大降低了后期维护的成本，同时软件部分也采用模块化设计，易于开发者后期维护。系统总体组成如图 1 所示。

4.1 硬件系统

硬件部分主要由 STC89C52RC 单片机、MFRC522 射频模块、AT24C256 存储模块、人机交互按键模块、外围控制电路以及报警模块等部分组成。

(1)单片机控制部分

系统主控部分采用 STC89C52 单片机。STC89C52 MCU

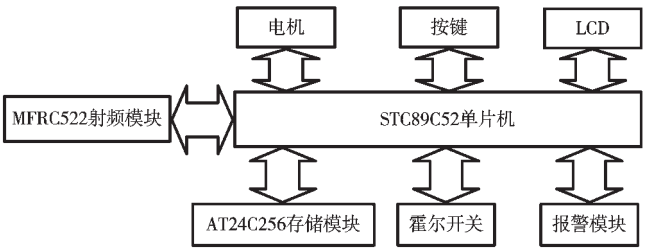


图 1 系统结构图

采用 MCS-51 核心，其抗干扰能力强、运行速度快、性能高、功耗低。其内置8 KB 的闪存 ROM、512 B RAM 和 2 KB 的 EEPROM、3 个 16 位定时器/计数器、32 个普通 I/O 口，满足此系统工作条件。此外，STC89C52 单片机还具有价格低廉的特点。因此，选用 STC89C52 作为主控芯片，能够降低系统成本。

(2)按键和 LCD 模块

本系统具有 3 种工作模式，因此必须具备模式切换的功能。另外本系统具有注销功能，需要在用户注销时输入 SID。本系统设置按键模块，使用按键扫描的方式确定系统的工作模式。因此，系统采用 4×4 矩阵键盘，设有数字键(0~9)、确认键、退格键、清空键，以及功能键 A、B、C。

(3)外围控制电路

外围控制电路包括了电机以及电机控制电路、霍尔感应开关和报警模块，用来控制锁的开启和关闭以及防止非法开锁。

(4)存储部分

本系统存在注册模式，注册模式时，用户的注册信息存储在 EEPROM 中。考虑到该系统将应用到类似小区的中型门禁管理系统，因此，本系统选取 ATMEL 公司生产的 AT24C256 可编程只读存取器，它具有 256 Kbit 的位存储单元、32 KB 存储单元，而用户 SID 对应的哈希码和 IC 的 UID(Unique ID)只需要 8 B 的存储空间，其详细的数据存储记录格式见表 2 所示。因此本系统最多支持 4 096 个 IC 卡，可应用于中型门禁系统。

表 2 EEPROM 数据记录格式

EEPROM 地址	数据记录	说明
0x00	哈希码	哈希码第 1 字节
0x01	哈希码	哈希码第 2 字节
0x02	哈希码	哈希码第 3 字节
0x03	哈希码	哈希码第 4 字节
0x01	UID	UID 最高字节
0x02	UID	UID 次高字节
0x03	UID	UID 次低字节
0x04	UID	UID 最低字节
……	……	……

4.2 软件系统

基于硬件电路的设计，本文开发出相应的软件来配

合响应硬件电路以实现整体识别功能。软件程序的质量直接决定着整个系统的成败。使用可移植性高的 C 语言编写，在 Real View MDK 编译环境中运行，使用 STC-ISP 软件与单片机交互，这给程序的修改和调试带来很大的方便。图 2 展示了系统的软件结构设计流程图。

系统的关键 API 函数主要有：

```
InitializeSystem( );                    //初始化系统
PcdReset();                             //读写器复位
PcdAntennaOff();                        //关闭天线
PcdAntennaOn();                         //开启天线
PcdRequest();                           //复位
PcdAnticoll();                          //防碰撞
PcdSelect();                            //选择卡片
PcdAuthState();                         //卡片认证
PcdWrite();                             //向某块写数据
PcdRead();                              //从某块读数据
StrCmp();                               //数据比对
HashJotta();                            //哈希码转换
```

4.3 系统测试

识别部分是该系统的关键部分，需要进行大量实验以测试验证系统的可靠性。为便于观察，需通过多机通讯的方式验证识别系统是否可靠。图 3 所示为搭建的系统实验测试方案，其主要由 RFID-RC522 射频模块和终端处理组成，射频模块用于 IC 卡感应识别，终端处理器负责完成对数据的读写控制操作。首先进行 IC 卡的注册，如图 4 所示，用户进入注册模式需要输入管理员密码，之后将卡贴近读卡器，读卡器识别到 UID 为 B4EEF8E2 的卡后，将卡序列号转换为哈希码作为 SID 并显示在屏幕上。该 SID 由用户保管。

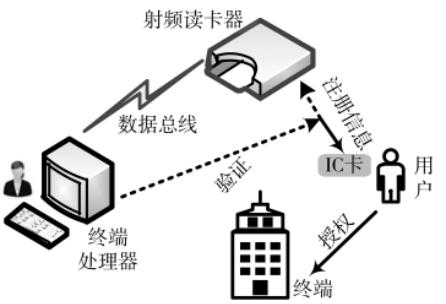


图 3 系统结构实验测试图

然后，进入到工作模式。如图 5 所示，屏幕显示 UID 为 B4EEF8E2 的卡通过了 ID 验证及块认证，UID 为 56AC2312 的卡因未注册所以没有通过 ID 验证，更无法进行下一步的块认证。而 UID 为 CABB9A10 的通过了 ID 认证但没有通过块认证，结果同样是验证失败。

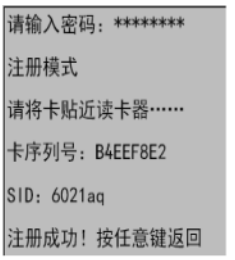


图 4 注册模式

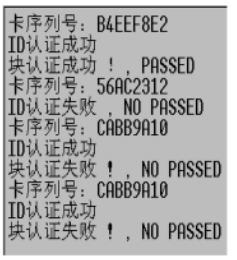


图 5 工作模式

假设 UID 为 B4EEF8E2 卡的主人将卡遗失，被非法分子捡到。该卡的主人及时进行了注销，如图 6 所示，进

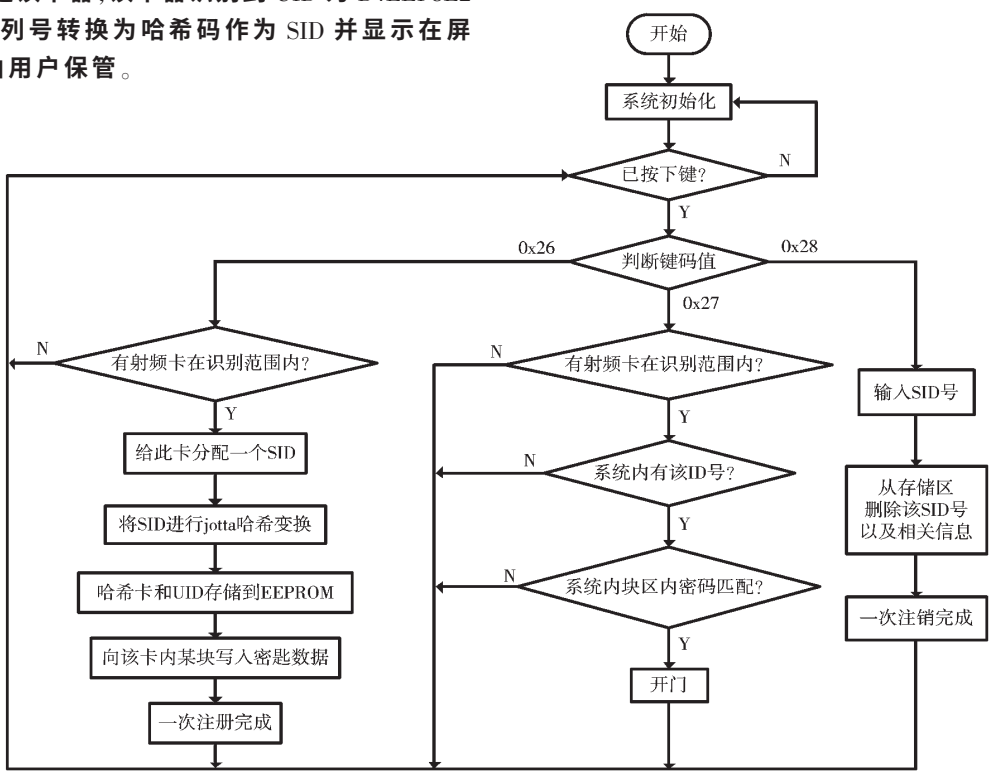


图 2 系统软件流程图

入注销模式，输入 SID 号后，系统将该卡的所有相关验证信息删除。如图 7 所示，非法分子使用 IC 卡复制工具将 UID 为 B4EEF8E2 的卡复制到“Chinese Magic Card”上，企图使用复制的卡通过系统验证，但复制卡只通过了 ID 认证，没有通过块认证，结果如图 8 所示。

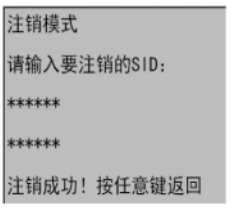
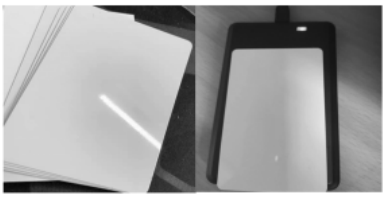


图 6 注销模式



(a)IC 白卡 (b)复制 IC 卡工具

图 7 IC 卡复制

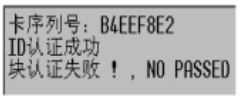


图 8 复制卡无法通过验证

综上，测试的卡分别是注册过的卡、未注册的卡和系统中已注册的卡的复制卡。经测试，系统运行稳定，未注册的卡和已注册卡的复制卡无法通过认证。同时，因为有密钥的存在，也无法轻易读取卡内信息。

对于已注销的卡，仍可以在注册模式下进行注册，但需要系统管理员提供进注册模式的密码，此时即可验证注册者的身份是否合法。

5 结论

基于 RFID 技术的二次认证加密智能识别系统便捷、有效地保障了用户信息的安全性，解决了个人信息存储于服务器带来的安全隐患与昂贵成本问题。此外，本文详细阐述了二次认证系统的 3 种工作模式以及针对各工作模式下的实验测试效果，表明其具有极高的安全性，且不易被破解和伪造，也能有效识别并阻止复制卡认证。所以此设计方法具有极大的应用价值，适用于家庭小区、办公室、学校等任何可以使用智能识别系统的场所，以提高安全等级。另外，随着 IoT 的大规模普及，RFID 技术作为一种物联网的促进剂将不断改进，安全和隐私级别会不断提高，RFID 在日常生活中的应用将更加广泛，而基于 RFID 技术的性能优异、便捷可靠的安全识别系统也会得到快速提升与推广。

参考文献

[1] 贺建飚，高建良.物联网 RFID 原理与技术[M].北京：电子工业出版社，2013.

[2] MFRC522 Contactless reader IC[Z].2009.

[3] DIMITRIOU T.Key evolving RFID systems：forward/backward privacy and ownership transfer of RFID tags[J].Ad Hoc Networks，2016，37(2)：195-208.

[4] 李诚，臧俊斌.基于 STC12C5A60S2 的室内环境监测系统设计[J].电子制作，2016(9)：32-34.

[5] DASS P，OM H.A secure authentication scheme for RFID systems[J].Procedia Computer Science，2016，78：100-106.

[6] HOON W F，SEOK Y B，MALEK M F A，et al.The design of ultra-high frequency(UHF) radio frequency identification (RFID) reader antenna[C].Advance in Intelligent Systems and Computing，2018.

[7] BRETON M L，BAILLET L，LAROSE E，et al.Outdoor UHF RFID：phase stabilization for real-world applications[J].IEEE Journal of Radio Frequency Identification，2018，1(4)：279-290.

[8] ABDELNOUR A，KADDOUR D，TEDJINI S.Transformation of barcode into RFID tag，design，and validation[J].IEEE Microwave & Wireless Components Letters，2018(99)：1-3.

[9] VOGT H.Efficient object identification with passive RFID tags[C].International Conference on Pervasive Computing，2002：98-113.

[10] SARMA S E，WEIS S A，ENGELS D W.RFID systems and security and privacy implications[C].Revised Papers from International Workshop on Cryptographic Hardware & Embedded Systems. Springer Berlin Heidelberg，2002.

[11] LEE S R，JOO S D，LEE C W.An enhanced dynamic framed slotted ALOHA algorithm for RFID tag identification[C].International Conference on Mobile & Ubiquitous Systems: Networking & Services.IEEE Computer Society，2005.

[12] FINKENZELLER K.RFID handbook(fundamentals and applications in contactless smart cards，radio frequency identification and near-field communication) || standardisation[M].2010 John & Sons，2010.

[13] Sun Peiran，Wang Bohan，Wu Fan.A new method to guard inpatient medication safety by the implementation of RFID[J].Journal of Medical Systems，2008，32(4)：327-332.

[14] 位书敏，张永华，商玉芳.轻量级移动 RFID 认证协议研究设计[J].计算机与现代化，2016(11)：74-78.

[15] Ouyang Hongzhi，Wang Xinlin，Zhu Weihua，et al.Design of auto-guard system based on RFID and network[C].International Conference on Electric Information & Control Engineering.IEEE，2011.

(收稿日期：2020-03-27)

作者简介：

臧俊斌(1987-)，男，博士，讲师，主要研究方向：MEMS 物联网类传感器件、深度学习。

白洋(1994-)，男，硕士，主要研究方向：物联网类传感器件、模式识别。

扫码下载电子文档

版权声明