文章编号:1001-5132（2009）01-0017-06

低功耗无磁水表中射频卡读写器的设计

祝向辉[1]，王让定[1*]，姚　灵[2]，孙广清[1]，陈昌根[1]

（1.宁波大学 信息科学与工程学院，浙江 宁波 315211; 2.宁波水表股份有限公司，浙江 宁波 315000）

摘要：为了加强数据的安全性且方便用户进行刷卡操作，选择在无磁水表中加入射频读卡器. 读卡器的硬件上采用 MSP430 单片机与射频读写芯片 RC522 相结合的方式，具有较低的功耗；软件上根据 Mifare 1 S50 射频卡及多扇区多密码的特点，采用一次一密的动态加密方式，较好地保护了卡内数据的安全性，同时对于用户恶意补卡现象也做了相应防备措施.

关键词：RC522; MSP430 单片机; Mifare 1 S50 卡；射频读卡器

中图分类号：TP391　　文献标识码：A

随着我国金卡工程的实施和发展，智能卡的应用已逐步融入人们的生活，水表中智能卡的应用也是趋势发展的必然结果. 射频卡以其良好的可靠性、方便的操作及其本身非接触等特点，成为卡式水表中智能 IC 卡的首选.

RC522 是 philips 公司继 MF RC500、RC531 及 RC632 等一系列典型产品后推出的一款针对智能仪表领域的低电压、低功耗、低成本的完全符合 ISO1443A 协议的非接触读卡芯片，采用统一的 3.3 V 供电电压，且具有灵活高速串行接口(I^2C、SPI、UART). 但它的操作难度主要在于如何通过单片机来设置其内部寄存器，以及传送特有格式的指令来向射频卡发送、接收有效数据，从而达到读、写卡的目的.

本设计硬件上采用 MSP430 单片机与 RC522 结合，供电电压完全一致，读卡器与 Mifare 1 S50 卡(以下简称 M1 卡)间以典型值 106 Kbps 的速率通信，软件上采用动态的加密方式，并在单片机中留部分 Flash 空间用以记录使用过的 M1 卡的序列号，以防止人为的恶意换卡.

1　系统硬件设计

1.1　系统总体设计

设计采用 TI 公司 MSP430FW427 单片机为主控芯片，它与外围扩展的无磁传感器、电源管理、存储模块、LCD 显示、保护装置、电磁阀门驱动、读写卡器共 7 个模块共同构成了整个水表系统的主体，其系统框图如图 1 所示.

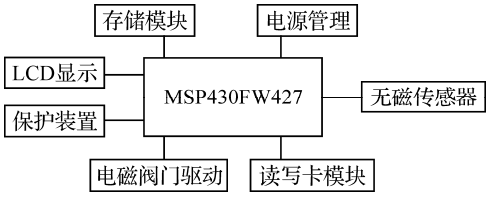

图 1　系统框图

图 1 中的无磁传感器采用 2 个 LC 振荡器，用于检测叶轮转动速度和转动方向；电源管理模块

收稿日期：2008-04-03.　　宁波大学学报（理工版）网址: http://3xb.nbu.edu.cn
基金项目：浙江省科技厅计划项目（2007C21G2070004）；宁波市科技局工业攻关项目（2006B100067）.
第一作者：祝向辉（1987－），男，江西鹰潭人，在读硕士研究生，主要研究方向：射频通信及嵌入式应用. E-mail: zxh19870127@163.com
*通讯作者：王让定（1962－），男，甘肃天水人，博士/教授，主要研究方向：数字水印及语音识别. E-mail: wangrangding@nbu.edu.cn

可检测电池电量以及完成必要的电压转换功能; 而存储模块主要用于记录用户用水量的历史数据; LCD 显示模块作为人机交互接口, 方便用户查询用水信息或自来水公司查询水表工作状态; 保护装置主要用于防止用户恶意拆卸、破坏水表, 并保障水表即使在非正常工作的状态下也不发生错误计量; 用户的供水由电磁阀门控制, 当用水量余额不足或电池电量不足时, 阀门关闭; 用户还可通过读写卡模块向水表充值, 实现用水金额的预付.

1.2 读写卡器硬件设计

射频读卡器的主要硬件电路包括 RC522 与单片机的接口电路以及外围天线的设计. 其中读写卡芯片 RC522 与单片机通过 I^2C 总线连接, 其接口方式如图 2 所示.

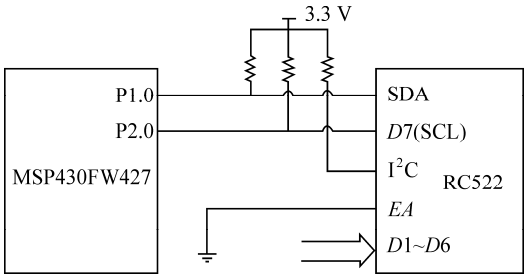

图 2 单片机与 RC522 连接方式

由于二者连接采用 I^2C 总线协议, 因此 RC522 的 I^2C 口应接高电平, *EA* 与 *D*1~*D*6 共同确定 RC522 作为 I^2C 协议中从设备的地址(7 bit). 当 *EA*=1, RC522 地址的 6 bit 数据由 *D*1~*D*6 来决定(这里特别要注意的是 *D*1~*D*6 的值不要与 I^2C 协议中规定的一些特殊地址冲突), 剩下 1 bit 一般为 0; 若 *EA*=0, 则 RC522 的地址的高四位为 0101, 低位由 *D*1~*D*3 确定[1].

除了与单片机的连接, RC522 还需要外接天线及其匹配、滤波和接收电路, 如图 3 所示.

在图 3 的电路中, 由 C_{mid}、R_1、C_{rx}、R_2 组成的接收电路与由 L_0 及 C_0 组成的滤波电路其元件参数值是固定的, 而天线匹配电路中 C_1、C_2 与 R_a 的值由设计的天线确定. 由于 M1 卡工作所需的电压由读卡器天线产生的磁通供给, 其能量的传输类似于变压器原理, 因此卡获得的能量随着卡和天线

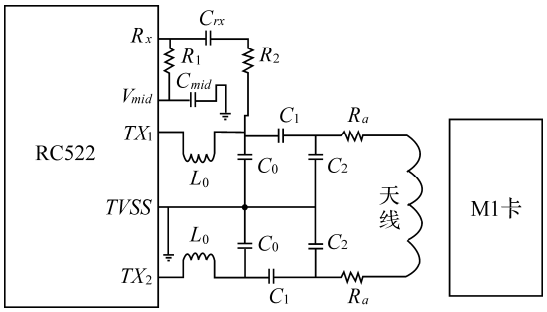

图 3 RC522 外围天线电路

间的距离不同而变化, 为获得良好性能, 相关参数值的选取还须经过天线的调谐过程[2].

2 系统软件设计

系统软件设计是整个系统设计的核心与难点, 主要完成射频卡和读卡器之间的信息交互.

2.1 标准 M1 卡的内部存储结构[3]

M1 卡内部有 1 个容量为 8 K 的 EEPROM, 分为 16 个扇区, 每个扇区为 4 块, 每块 16 Byte, 其结构如图 4 所示.

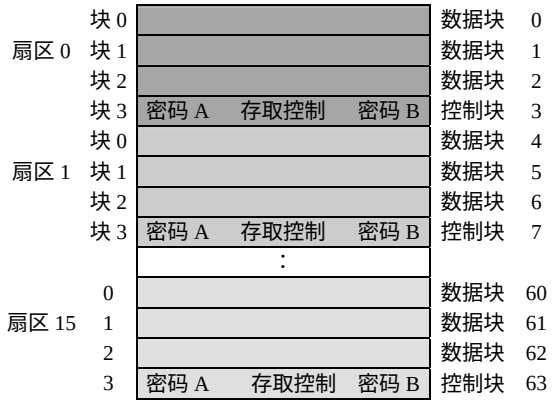

图 4 M1 S50 卡内部存储结构

其中每个扇区的块 0、1、2 为数据块, 用于存储 16 Byte 数据. 数据块可分为 2 种: 普通的数据块和特殊数据块, 二者的区别在于数据的存储格式不同, 普通数据块可存任意 16 Byte 数据, 而特殊数据块内数据存储格式如图 5 所示, 其中有效数据为 4 Byte, 块号为 1 Byte, 只有这种存储格式的数据块才可执行卡的增/减指令. 另外, 每个扇区的块 3 为控制块, 其中包括了密码 A、存取控制和密码 B,

具体结构如图 6 所示. 每个扇区的密码和存取控制都是独立的，默认存取控制(FF 07 80 69)表明该扇区使用密码 A 验证，而密码 B 无效. 需要注意的是：第 0 扇区的块 0 用于存放厂商代码，已经固化，永远不可更改.

有效数据	有效数据	有效数据	块号	块号	块号	块号

图 5　特殊数据块存储格式

密码 A (6 Byte)	存取控制 (4 Byte)	密码 B (6 Byte)

图 6　各扇区控制块结构

2.2　卡的基本功能的实现

卡的基本功能包括卡的增、减、读、写操作，它需要借助于许多不同指令来实现，RC522 与 M1 卡都有各自的指令(分别称之为 Command 指令和 M1 指令)[4]，因此如何通过 Command 指令来完成 M1 指令从而达到读写卡的目的是整个软件设计的主要内容.

在一般情况基本的卡操作中，并不是所有指令都要用到，常用的几个 Command 指令有空闲指令(IDLE)，它可使读卡器进入空闲模式；CalcCRC 用于 CRC 校验计算；Transceive 指令是 Command 指令中最常用的一个，主要用于数据的发送与接收；而 MFAuthent 密码认证指令用于 M1 卡中的密码验证.

常用的 M1 指令主要有询卡指令(Request)，包括 Request All 和 Request Idle 2 种模式，用于搜索一定范围内是否存在 M1 卡；防冲突指令(Anticollision)和选卡指令(Select)成功执行后，可从多张卡中选取 1 张有效 M1 卡; Authentication 指令是进行密码认证；其他的还有 Read、Write、Decrement、Increment 指令分别用于对卡的读、写、增值与减值; Halt 指令可使卡进入空闲状态.

M1 卡与读卡器之间的典型通讯过程如下：将待发送数据(包括标准 M1 卡指令)按一定格式写入 RC522 的 FIFOData 寄存器后，再写 Command 指令到 Command 寄存器，以此触发通信的开始(有些指令还需对一些寄存器操作后才开始通信)，卡若接收到数据，先读取数据中的 M1 卡指令，再将余下数据作为 M1 指令的操作对象进行相应的操作，并将结果返回 RC522 的 FIFOData 寄存器. 卡内部操作是自发，一般只将 Command 指令写入 Command 寄存器中，一定时间后通过读取 FIFOData 寄存器中卡的返回值来确定 M1 卡是否成功地完成了预定的操作. 显然, Command 指令在 RC522 内识别，标准 M1 卡指令在读卡器内相当于一些普通数据，它的识别过程在 M1 卡内进行. M1 指令的执行过程是卡基本功能的具体实现过程，流程如图 7 所示.

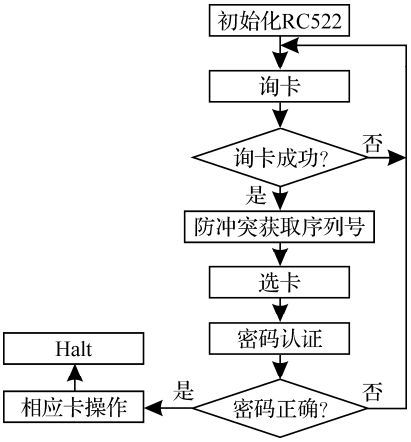

图 7　M1 卡操作流程

要对 M1 卡进行读写，必须先经过询卡、防冲突、选卡、密码认证等环节[5]. 询卡主要用于搜寻一定范围内是否存在 M1 卡，询卡成功后，则进入防冲突获取序列号过程，这是整个流程中较为复杂的环节，它的主要功能是在若干个 M1 卡中按一定的算法获取其中 1 张 M1 卡的序列号，为选卡做准备.

防冲突循环的流程如图 8 所示，其中防冲突命令(SEL+NVB)中 SEL 为防冲突指令 0x93, NVB 为 1 Byte 数据，高 4 位表示本次待发送数据的有效字节数，低 4 位为发送数据最后 1 个字节的有效位数. 成功接收到读卡器发送的防冲突指令后，有效范围内的所有卡均以其序列号响应，显然，若范围内不单有 1 张卡时，冲突必然发生，一旦发生冲突，则应读取相应寄存器的值确定冲突位；之后通过不断更新 NVB 的值与接收到的有效数据位来更新防

冲突指令传送的数据，直至再无冲突产生，若成功接收到某 1 张卡的序列号，则可发送选卡命令，成功选卡后方可进行密码认证过程.

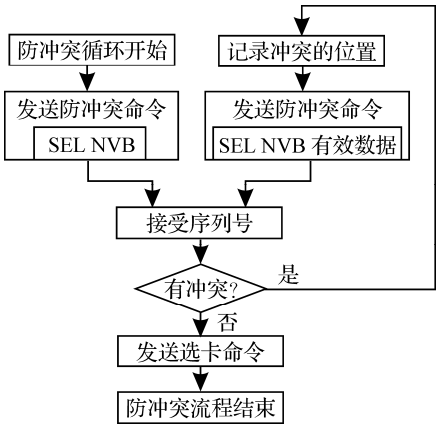

图 8　防冲突循环流程

密码认证以扇区为单位，其结果在于开启通信加密单元，成功后的数据传输都将加密. 且只有密码认证通过之后才可对卡进行读、写、增/减值等操作. 卡的读、写、增/减值等操作均以块为单位，其中增/减值过程较为复杂，其过程如下:

(1) 发送增值(0xC0)/减值(0xC1)指令+块号+CRC 校验(2 Byte)共 4 Byte 数据，若返回 4 bit 数据 1010，则可进行下一步操作;

(2) 继续发送以下数据：待增/减值(4 Byte)+CRC 校验(2 Byte)共 6 Byte，仍以返回值 1010 来判断该步操作是否成功;

(3) 最后发送数据 Transfer 指令(0xB0)+块号+CRC 校验(2 Byte)共 4 Byte，成功则返回 1010，如此则表明整个增/减值过程执行成功.

卡操作完毕后，可使卡进入 Halt 状态，此时只有 Request All 指令方可唤醒该卡.

3　动态加密方式

由于 M1 卡有多个扇区，每个扇区可以有各自不同的密码，这为一卡多表提供了可能性，同时也成为本设计中一次一密的加密方式(称之为动态加密)成功实现的前提条件.

虽然前述密码认证之后数据的传输将先被加密，但若只用单一密码且每次执行相同的卡操作(比如增值)的话，则卡与读卡器之间的数据通信存有一定规律性，有时甚至是固定的，这样攻击者可先通过图 9 所示的方式监听数据通信的过程，完全了解该过程之后，便可模拟 M1 卡与读卡器通讯(图 10)，这样即使没有射频卡也可达到增值的目的，这是我们所不想看到的.

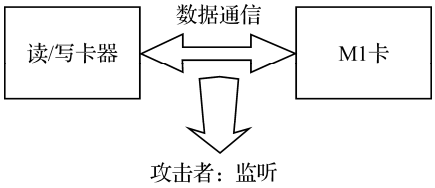

图 9　攻击者监听数据通信过程

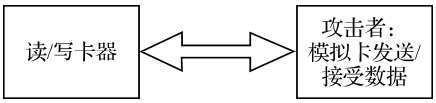

图 10　攻击者模拟卡发送数据

为此，我们可以采用动态加密方式来克服上述弊端，整个加密过程可分解为 M1 卡的初始化和具体的加密操作 2 部分. 为便于描述该过程，先假设函数 des(Data, Key, flag)为 8 Byte DES 加/解密算法，其中 Data 为待加/解密数据，Key 为密钥，flag 为加/解密模式(0 为解密，1 为加密)；另外，由于动态加密过程需要用到两个扇区，程序员可选 0~15 中的任意 2 个，这里假定为扇区 1 和扇区 2，其中扇区 1 存储与扇区 2 的密码相关的数据，扇区 2 真正记录卡内余额.

3.1　卡的初始化

要使 M1 卡能用于上述的动态加密，首先必须经过卡的初始化过程，过程如图 11 所示，其中 UID 即为 M1 卡的序列号.

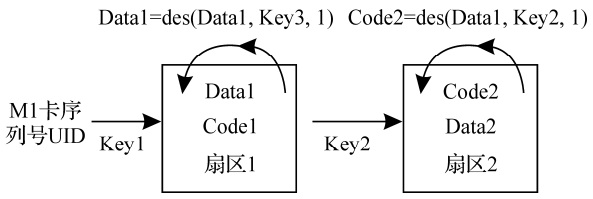

图 11　动态加密

初始化过程如下:

(1) 读取 M1 卡的序列号，并设定扇区 1 密码 Code1 与 UID 及 Key1 相关；

(2) 任意初始化扇区 1 内 8 Byte 数据 Data1，但注意最好不要初始化为全 0 或全 1 等极具规律性的数据，因为使用这些数据将会大大降低通讯的安全性；

(3) 将扇区 1 数据 Data1 用密钥 KEY2 加密后，作为扇区 2 的密码 Code2，即为: Code2=des(Data1, Key2, 1).

3.2　具体的加密操作过程

M1 卡经过初始化后，其动态加密具体执行过程如下:

(1) 表内读卡器获取卡 UID 后，用密钥 Key1 和 UID 获取扇区 1 密码并访问扇区 1 数据 Data1;

(2) 用密钥 Key2 将 Data1 加密后作为扇区 2 的密码，并访问扇区 2 数据 Data2，从而可进行相应的卡操作;

(3) 如图 11 所示，将 Data1 作为输入数据，用密钥 Key3 加密后得到的数据更新 Data1;

(4) 同理，用密钥 Key2 将更新后的 Data1 加密，再将得到的数据更新扇区 2 密码 Code2.

经过以上 4 个步骤，则 1 次动态加密过程中卡的操作便已完成. 为确保每次卡操作的成功，扇区 1 中数据 Data1 的改变与扇区 2 中密码 Code2 的更新必须同步，即每执行过 1 次步骤 3 后，一定要有 1 次步骤 4 的执行. 另外, des 算法在此并未起到加/解密的作用，只是将 2 个无规律 8 Byte 数用密钥 Key 联系起来，程序员可以用其他更简单的算法代替，以降低单片机的计算复杂度，从而减少操作时间. 整个加密过程的安全性取决于数据 Data1 与 Code2 更改的无规律性，程序员自己编写算法时须注意到此点.

4　防止用户恶意补卡

为防止用户在前 1 张卡还完好时，向自来水厂提出补卡的要求将导致用户同时拥有 2 张有效卡向水表充值(第 2 张卡免费且拥有第 1 张卡中的余额)，因此有必要在单片机中留有一定的 Flash 空间. 若发现异常情况，则记录相应卡的序列号，防止用户再使用，该过程如图 12 所示.

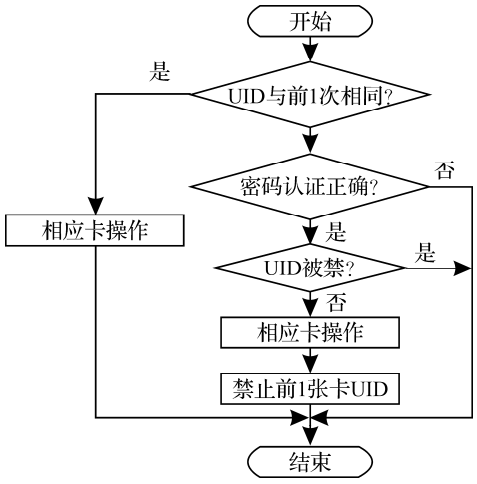

图 12　软件防止恶意补卡流程

可以在 Flash 地址 A 中存储前 1 张卡的 UID，Flash 地址 B 中存放被禁止卡的 UID，该过程中首先读取地址 A 中的数据与当前卡的 UID，若二者相同，则判断为同 1 张卡；若不同，则进行密码认证，成功认证后读取地址 B 中存放的数据(可以记录多个被禁止的 UID)逐一与当前 UID 相比，只有全不相同的情况下才确定当前卡为补卡，进行相应卡的操作后将前 1 张卡 UID 记入地址 B 中，禁止它再次被使用，同时将当前卡 UID 记入地址 A.

需要注意的是，由前述 M1 卡初始化过程可知，水表内读取数据 Data 是通过当前卡 UID 来完成的，那么虽然不同的卡有不同的 UID，但密码存储在卡内，所以所有以上述方法初始化后的卡都可以在相同的水表上操作，这显然是不可行. 为解决此问题，可以在 Flash 地址 C 中存储第 1 张卡的 UID(这里的第 1 张卡指的是从水表被制造完成后的第 1 张与其接触的 M1 卡)，这显然是唯一的，且地址 C 中的数据永远不得改动. 以后可通过读取地址 C 中的数据来获取扇区 1 密码，从而读取数据 Data1. 因此，1 块水表对应的只有 1 个密码即可解决上述

问题. 自来水厂应记录用户第 1 张卡的序列号(用户水表中密码只与该序列号有关), 若用户需补卡, 对其初始化过程与前述过程相似, 注意初始化扇区 1 密码时 UID 为第 1 张卡序列号即可.

5 小结

介绍了无磁水表中以 MFRC522 为核心的读卡器的设计, 硬件上采用 Philips 提供的 RC522 典型外围电路, 软件上除了基本的卡操作流程外, 根据 M1 卡多扇区多密码的特点, 在数据传输的加密方面采用了一次一密的动态加密方式, 大大地提高了数据安全性, 不过由于每次读写卡时至少要访问到两个扇区, 这样增加了一些用户的操作等待时间, 但总体来讲并无大碍.

尽管基于 RC500 读写卡器的技术已十分成熟, 但以 RC522 为核心的相关系统在国内并不多见, 同样是 Philips 公司的产品, RC522 显然是 RC500 的精简版, 无论是 Command 指令, 还是内部寄存器都比 RC500 要更为简洁, 且价格更为低廉, 而总体功能上却并未削弱多少, 因此本文认为 RC522 替代 RC500 将会是一种趋势.

参考文献:

[1] Philips. MFRC522 contactless reader IC product data sheet(Rev3.2)[EB/OL]. (2007-12-11)[2006-08-15]. http://www.rfidworld.com.cn/.

[2] Philips. Design of RC500 matching circuits and antennas (Rev1.0) [EB/OL]. (2007-12-13)[2006-07-25]. http://www.rfidworld.com.cn/.

[3] Philips. Mifare standard card IC MF 1 IC S50 functional specification (Rev4.0) [EB/OL]. (2007-12-10) [2006-06-12]. http://www.rfidworld.com.cn/.

[4] Philips. MFRC500 Basical Function Library(Rev2.0) [EB/OL]. (2008-01-10) [2006-12-05]. http://www.rfidworld.com.cn/

[5] 徐丽华. 射频卡识别读写模块的设计与应用[D]. 苏州: 苏州大学, 2005.

Design of Unsupervised Reading System for Low Power Nonmagnetic Water Meter

ZHU Xiang-hui[1], WANG Rang-ding[1*], YAO Ling[2], SUN Guang-qing[1], CHENG Chang-gen[1]

(1.Faculty of Information Science and Technology, Ningbo University, Ningbo 315211, China;
2.Ningbo Water Meter Limited Corporation, Ningbo 315211, China)

Abstract: In order to increase the data security and reduce inconveniences in meter reading, a non-contact reader is designed for ultimate embedding into the nonmagnetic water meter system. The system power consumption is lowered as result of combining MSP430 singlechip and MF RC522 chip in the design. By taking advantage of multi-sector and multi-password featured in Mifare 1 S50 card, the dynamic mode of one-encrypting-at-a-time is adopted, which consequently enhances the security of data transfer. In addition, some measures are also taken to prevent users from holding more than one card when interfacing with the system.

Key words: RC522; MSP430 singlechip; Mifare 1 S50 card; contactless reader

CLC number: TP391 **Document code:** A

（责任编辑 章践立）