M1 卡在一卡多用系统中可行性分析

邹方卫，宋财华

(江西三川水表股份有限公司 技术中心研发部,江西 鹰潭 邮政编码 335000)

摘　要: 本文通过研究分析 M1 卡的数据结构及密码机制以及目前民用计量计费领域的一卡多用需求分析给出了使用 M1 卡作为一卡多用系统 IC 卡的可行性分析。并且从数据承载方式以及数据安全等方面做出了分析和介绍；提出了一种可行的解决方案，具有实际应用参考价值。

关键词: M1 卡；一卡多用；非接触式 IC 卡

0 引言

随着智能计量计费仪表在民用生活领域中的大量使用，各类 IC 计费卡越来越多的出现在人民的生活领域。在水、电、去、气甚至供暖等各个领域都采用智能 IC 卡计量计费后居民手中出现了各类 IC 卡片。IC 卡的数量增加给居民的生活带来了诸多麻烦，管理和收纳使用等都不方便；从而出现了一卡多用系统。即使用一张卡片来进行各类计费工作，但是卡片的计量数据关系到用户和企业的切身利益，数据安全性显得尤为重要，下面我们就以 M1 卡为例来讨论一卡多用系统的使用在数据存储及数据安全等方面的可行性进行分析探讨。

1 M1 卡结构

M1 卡全程为 Mifare 1 IC 智能(射频)卡，它的核心是 Philips 公司的 Mifare 1 IC 的核心是 S50 系列微模块微晶片。M1 卡采用先进的芯片制造工艺制作内建有高速的 CMOS EEPROM、MCU 等。卡片上除了 IC 微晶片及高效率天线外无任何其他元件。卡片能量由天线感应供给，卡片读写器天线发送无线电载波信号耦合到卡片上天线而产生电能一般可达 2V 以上供卡片上 IC 工作。工作频率 为 13.56MHz。射频卡标准操作距离最大可达到 100mm，与卡片读写器的通信速率高达 106Kbit/s。M1 卡具有先进的数据通信加密并双向验证密码系统；且具有防重叠功能。在同一时间处理重叠在卡片读写器天线的有效工作距离内的多张重叠的卡片。片上内建 8Kbit EEPROM 存储容量，并划分为 16 个扇区。每个扇区划分为 4 个数据存储块，每个扇区可由多种方式的密码管理。片上的数据读写可超过 10 万次以上。数据保存期可达 10 年以上；且卡片抗静电保护能力达 2KV 以上。该卡非常适合使用在一卡多用系统中。

1.1 M1卡功能组成

M1 卡内部电路分为数字电路部分和 RF 结构电路两部分。其功能组成如图 1 所示。

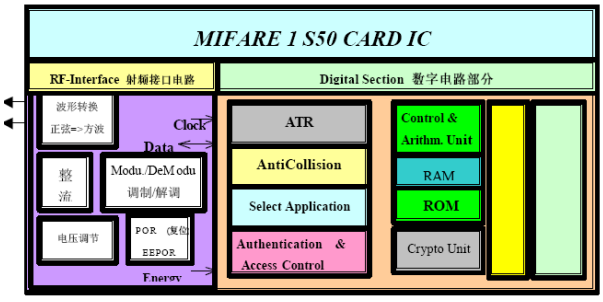

图 1 M1 卡功能组成框图

射频接口电路主要包括波形转换模块、调制/解调模块、电压调节模块以及POR模块。波形转换模块将13.56MHz信号送到调制/解调模块中提取数据以及送到电压调节模块提取能量供卡片使用。POR模块负责卡片上电后的初始化操作。

数字电路模块包括8个部分，分别为请求应答模块、防重叠模块、卡片选择模块、认证存取模块、控制及算术运算单元、RAM/ROM 单元、Crypto Unit 数据加密单元和EEPROM INTERFACE/EEPROM MEMORY EEPROM存储器及其接口路。请求应答模块负责和读写器建立基本链接；防重叠模块用来识别多张卡片在可读范围内数据传递工作；卡片选择模块用来选取特定卡片进行通信；认证存取模块是一卡多用的核心部分，可以将卡片16个扇区的内容分别加密存取操作。该模块使得一卡多用成为可能，在后一中将详细分析；控制及算术运算单元属于MCU类处理单元；RAM/ROM 单元负责协助控制处理单元操作，Crypto Unit 数据加密单元和EEPROM INTERFACE/EEPROM MEMORY EEPROM存储器负责加密和存储数据信息。

1.2 M1卡数据结构

M1卡片的存储容量为1Kx8位字长.采用EEPROM作为存储介质,整个结构划分为16个扇区。每个扇区有4 个块Block 16个字节。一个扇区共有64Byte存储空间。其结构如图2所示。

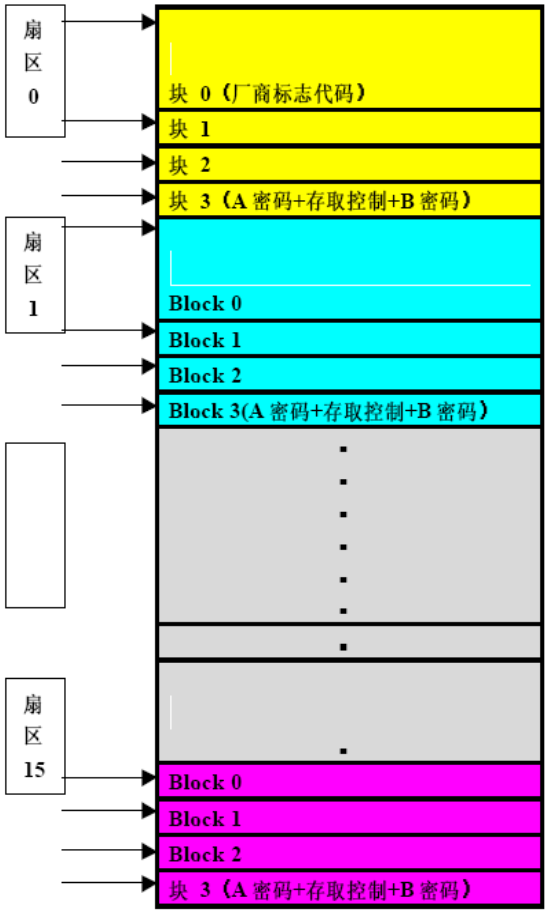

图 2 M1 卡数据结构图

每个扇区的块 3 包含了 6 个字节的扇区密码、4 个字节的存取控制以及 6 个字节的密码。其他三个块存储普通数

据，可以对数据进行普通操作，也可以进行加值减值操作。其中扇区 0 块 0 数据位厂商定义数据，不可更改。

2 一卡多用可行性分析

在上一节中介绍了 M1 卡的基本结构和数据结构功能，下面介绍将 M1 卡应用到一卡多用系统（一卡通）在数据容量和数据安全两方面的可行性进行分析。

2.1 数据容量

M1 卡有 16 个扇区共计 8192Bit 可以供规划使用。而在非接触式 IC 卡的智能仪表中 T5557 卡应用还是比较广泛的，T5557 卡容量为 330Bit，很多应用系统中都是用该卡片来做计量卡。M1 卡的容量是 T5557 卡容量的二十多倍，所以从容量上看，即使规划成为 8 个系统，每个系统使用 2 个扇区还是有足够的容量来做系统计量计费，并且还剩下足够的容量来做扩展功能使用。例如在水表领域的多阶水价计费，我们有足够的容量来设计 10 阶以上的阶梯价格计费，在用户数据带回水司方面也可以做到带回系统错误，历史价格，甚至每个月历史数据供分析使用。

2.2 数据安全

数据安全是一个重要课题对于计量领域来说。在这里 M1 卡将存储结构分为 16 个扇区，每个扇区有单独的验证传输机制为实现一卡多用提供了现实可能。M1 的读写操作都需要对已经设子的卡片扇区密码进行匹配，认证成功才允许进行读写操作，否则卡片系统拒绝操作请求。而且 M1 卡对每个扇区实行单独的密码机制，它们之间互不干涉。这一点为一卡多用提供了便利，也就是说，企业可以协商各自使用的扇区进行规划分配。然后各自的用户信息数据单独操作又不互相影响。

M1 卡的密码认证方式采用三遍认证机制。三遍认证机制令牌图如图 3 所示。

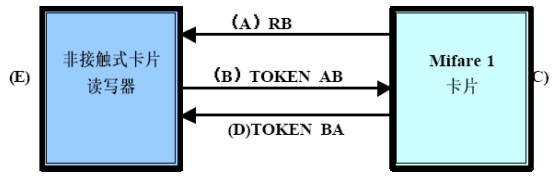

图 3 三遍认证原理框图

认证过程如下：

A 环：由 M1 卡片向读写器发送一个随机数据 RB；

B 环：由读写器收到 RB 后向 M1 卡片发送一个令牌数据 TOKEN AB，其中包含了读写器发出的一个随机数据 RA；

C 环：M1 卡片收到 TOKEN AB 后对 TOKEN AB 的加密的部分进行解密并校验第一次由 A 环中 M1 卡片 发出去的随机数 RB 是否与 B 环中接收到的 TOKEN AB 中的 RB 相一致；

D 环：如果 C 环校验是正确的则 M1 卡片向读写器 发送令牌 TOKEN BA 给读写器；

E 环：读写器收到令牌 TOKEN BA 后读写器将对令牌 TOKEN BA 中的 RB 随机数进行解密并校验第一次由 B 环中读写器发出去的随机数 RA 是否与 D 环中接收到的 TOKEN BA 中的 RA 相一致

在上述每一个环节中都为真验证才能通过，否则认证失败。验证成功后就可以对卡片进行该扇区的读写操作。但是这时候不能操作该扇区以外的其他扇区数据。其他扇区的数据必须使用这些扇区的密码进行认证。该机制相当于给了用户 16 个子卡来使用，也就是说用户可以最多使用 M1 卡做 16 个单独的系统卡片进行单独分别使用。如果遇到一个扇区存储扇区不够用的情况下可以考虑使用多个扇区来存放数据。这样规划可以根据实际情况单独来进行规划申请，同时留出预留资源供扩展使用。例如，民用领域可以将水、热、气、供热和电等 5 个不可缺少的企业用户数据整合到同一张卡片中。即使给每个企业分配两个扇区还是有 6 个扇区供扩展使用。所以说资源还是足够使用的。

密码认证过程必须保证每个环节都不出错才能通过，否则认证失败，如果使用暴力方式破解打开扇区由于密码变化和位数相当复杂，所以这种方式几乎为零。所以具有极高的安全性。但是如果某个扇区密码遗失必然导致该扇区数据永久失效，所以必须牢记密码以免数据丢失。

3 结束语

本文通过分析 M1 卡的结构数据特点得出使用该卡作为一卡多用系统方案是可行的。从数据结构以及安全方面都拥有足够的资源供用户使用，但是 M1 卡曾经被破解给用卡安全带来威胁，但是如果有每卡使用单独扇区单独秘密一般可以避免安全问题。所以实际可行性还是得进一步探讨。

参考文献:

[1] 王卓人,邓晋钧,刘宗祥. IC 卡的技术与应用 [M]. 北京: 电子工业出版社,1999.

[2] 戴蓉,王春麟,陈 祯.路桥车辆自动收费系统的研究 [M] 武汉:理工大学学报,2000.

[3] 王韧;IC 卡智能水表的设计与实现[J];仪表技术;2003 年 04 期

[4] 张松,方小马,廖科;无线预付费电表系统设计[J];电子工程师;2005 年 05 期

[5] 康叶伟;黄亚楼;孙凤池;;一种低功耗智能 IC 卡冷水表的设计与实现 [J];南开大学学报(自然科学版);2006 年 05 期

[6] 徐敏;基于 Web 的预付费售电运营系统的研究与设计[D];北京交通大学;2007 年

[7]岳蕾;基于无磁扫描技术的流量检测系统的研究与实现[D];武汉理工大学;2007 年

[8]郑芬;基于智能卡的预付费智能水表的研究与设计[D];中南大学;2007 年

[9] 程杰,陈惠明,陆荣;IC 卡预付费售电管理系统的研究与开发[J];电子工程师;2003 年 05 期

[10]李建;;校园一卡通系统在电大学习支持服务中的应用[J];中国教育信息化;2007 年 17 期

[11] 王娟玲;侯卫周;成强;;关于 C++面向对象设计方法的浅析[J];科技咨询导报;2007 年 20 期

[12] 唐金华;一卡通机房管理系统分析与设计[D];北京邮电大学;2008 年

收稿日期：2013-4-6；

作者简介：邹方卫(1985-)，男 ，江西省宜春市铜鼓县人，,硕士研究生,硬件高级工程师，主要研究领域为综合信息网络技术；宋财华(1970-)，男，江西鹰潭人，MBA，高级工程师，中国计量协会水表工作委员会兼职副秘书长，主要研究领域为光机电一体化。