CPU 卡流量计功能要求及实现

Functional Requirements and Implementation of the CPU Card Flow Meter

何　垚
（湘潭新奥燃气有限公司，湖南 湘潭　411100）

摘　要：随着城市燃气用户的快速发展及应用，CPU 卡流量计因功能强大、安全性能强的优点在城市燃气应用中越来越广泛，它取代了传统的上门抄表工作，为燃气公司节省了大量的人力、物力。根据 CPU 卡以及城市燃气的特点，设计了用于城市燃气的 CPU 卡文件结构以及密钥管理体系，实现了 CPU 卡流量计的计量及预付费功能。

关键词：CPU 卡　密钥管理　流量计量　安全　模块
中图分类号：TH814　　**文献标志码**：A

Abstract：Along with the rapid development of gas users in cities and applications of gases, CPU card flow meter has been used wider and wider in civic applications because of its advantages of powerful functions and high security. It replaces traditional door-to-door manual meter reading job, so saves a lot of manpower and material resources for gas companies. According to the characteristics of CPU card and civic gas, the file structure and dongle management architecture of the CPU card are designed, and the CPU card metering and pre-payment functions are achieved.

Keywords：CPU card　Dongle management　Flow measurement　Safety　Module

0　引言

IC 卡是一种半导体卡，其采用微电子技术进行信息的存储、处理。自 1970 年诞生第一张 IC 卡以来，IC 卡经历了一般存储卡、加密存储卡、CPU 卡和超级智能卡 4 个时代。IC 卡是多学科技术综合发展的结果，它的应用已成为一个国家科技发展水平的标志之一[1]。

IC 卡在城市燃气流量计量上的应用越来越广泛。在 CPU 卡流量计之前，大量使用的是逻辑加密卡。由于逻辑加密卡的技术所限，产品供应商的密钥不能向应用方（燃气公司）公开，因此应用方无法掌握核心安全，系统安全取决于产品供应商，并且不同型号的逻辑加密卡互不兼容，导致不同厂商的芯片数据存储方案也不兼容，应用方在使用多家卡表时会带来多种密钥和密钥算法管理上的复杂化[2-3]。

CPU 卡又称智能卡，卡片内自带 CPU，程序容量和数据容量大，且带加、解密算法协处理器，运算速度快[4]。采用 CPU 卡，并且制定一种统一的技术规范，燃气公司能完全掌握 CPU 卡流量计的技术核心及密钥算法，保证燃气准确计量、实现先购气再用气、防止用户偷气。由此可见，CPU 卡工业流量计成功应用的关键是设计完善的 CPU 卡密钥系统[5]。

修改稿收到日期：2010－12－15。

作者何垚，男，1971 年生，2009 年毕业于湘潭大学生产过程自动化专业，获硕士学位，工程师；主要从事计量仪表方面的研究。

1　CPU 卡流量计的功能要求

目前，新型的 CPU 卡流量计是集计量基表、电子表头和控制阀于一体的流量计。此前，CPU 卡流量计通常是集成商将流量计和 IC 卡控制阀通过电气连接而成，流量计在计量一定的量（通常为 1 m^3）时输出一个脉冲给 IC 卡控制阀，IC 卡控制阀进行扣减，当扣减超过允许透支量时，控制阀关闭。对于这种方式，电气连接的可靠性是关键，经常出现的情况是扣减不同步，流量计运行的量与 IC 卡控制阀扣减的量不尽相同，造成计量纠纷。所以，从 CPU 卡流量计功能上讲，一体化流量计是发展的趋势。燃气贸易中，用户通过 CPU 卡购气后充值到流量计中，燃气公司通过 CPU 卡达到管理用户用气的目的，CPU 卡起着联系用户和燃气公司的关键作用。另外，当上游气价浮动时，燃气公司能及时通过 CPU 卡或其他方式调整气价。

综上所述，CPU 卡应至少保存如下信息：用户信息、燃气公司标志、购气量和购气次数，以及为安全需要而设计的密钥组、不同功能卡的卡标志。为避免异常操作造成卡内数据丢失，还可以在卡文件中记录主要操作过程，异常操作后再次插卡能恢复继续进行正常的操作。

2　密钥体系总体设计

本密钥体系设计采用三级分散四级密钥方式，从根密钥逐级分散，到最终的应用卡片密钥，如图 1 所示。

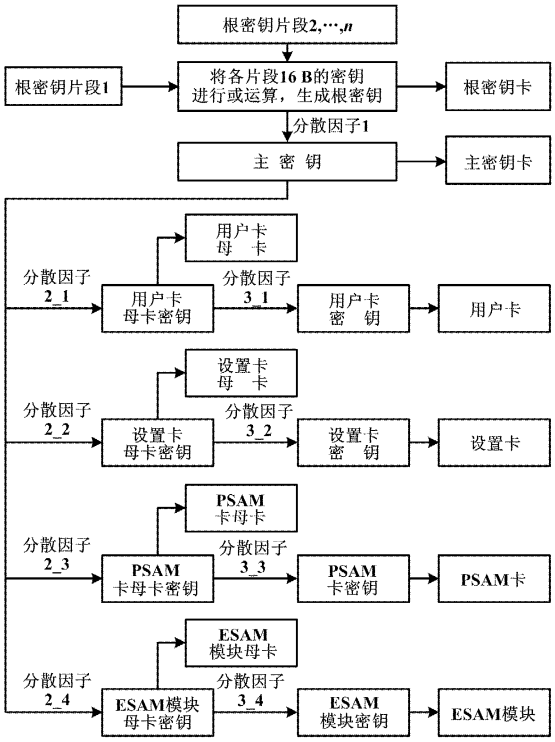

图 1　密钥体系图

Fig. 1　Dongle architecture

2.1　密钥的管理

由图 1 可见，在密钥体系中，各应用卡处在体系的最底层，其密钥是根据上一级母卡和分散因子进行密钥分散得到的。因此，必须加强对母卡的管理。为防止各级母卡在应用中不可预料的物理性损坏，必须对各级母卡进行备份并根据单位需要设置管理权限。

2.2　密钥分散

在进行密码运算时，可根据密钥长度选择数据加密标准（data encryption standard，DES），或 3DES 算法。一般而言，密钥长度为 8 B 用 DES，16 B 用 3DES 算法。这两种算法的逻辑框图如图 2 所示。

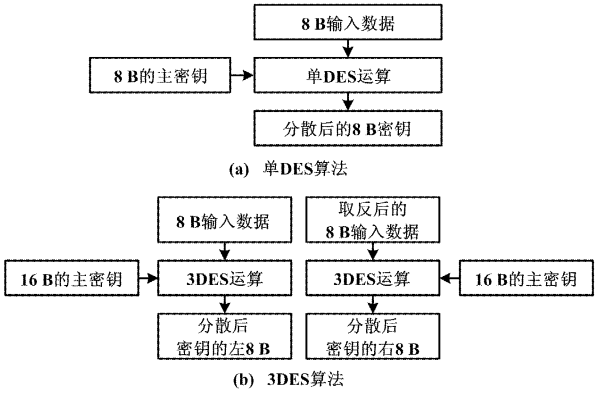

图 2　运算逻辑框图

Fig. 2　Block diagram of the operational logic

2.3　DES 算法

DES 算法为一种对称密码体制，它是 IBM 公司于 1975 年研究成功并公开发表的，开创了公开全部算法的先例。DES 算法的基本技巧是把每一位明文的影响尽可能迅速地作用到较多位输出密文中去；同时把每一位密钥的影响尽可能扩散到较多位输出密文中，以隐蔽明文的统计特性。

DES 主要采用替换和移位的方法，用 56 位密钥（密钥为 64 位，其中 8 位是奇偶校验位，所以实际上密钥为 56 位）对 64 位二进制数据块进行加密。每次加密可对 64 位的输入数据进行 16 轮编码，经一系列替换和移位后，输入的 64 位输入数据被转换成完全不同的 64 位的输出数据。

3DES 是在 DES 的基础上采用三重 DES，即用两个 56 位的密钥 K_1、K_2 进行加密与解密。发送方用 K_1 加密、K_2 解密，再使用 K_1 加密；接收方使用 K_1 解密、K_2 加密，再使用 K_1 解密，其效果相当于密钥长度加倍。[6]

3　CPU 卡密钥类型及应用

所有 CPU 卡的密钥类型如下。在实际应用中，可以根据系统要求适当删减。

DES 加密密钥，用于进行 DES 加密运算的密钥，在内部认证操作时使用。

DES 解密密钥，用于进行 DES 解密运算的密钥，在内部认证操作时使用。

DES&MAC 密钥，用于进行报文鉴别代码（message authentication code，MAC）运算的密钥，在内部认证操作时使用。

内部密钥，用于产生消费、取现和圈存交易中使用的交易验证码（transaction authentication code，TAC），涉及圈存、圈提、消费/取现、修改透支限额操作命令。

维护密钥，用于在以安全报文方式访问文件时，产生安全报文的密钥。它涉及读/写文件/记录、存款、扣款、卡片锁定、应用锁定和应用解锁操作命令。

主控密钥，用于在以安全报文装载或更改密钥时，产生报文的密钥。它涉及外部认证、增加或修改密钥操作命令。

口令解锁密钥，用于在以安全报文访问口令时，产生安全报文的密钥。它涉及口令解锁、验证并修改口令操作命令。

口令重装密钥，用于产生重装 PIN 命令的 MAC。涉及重装/修改口令密钥，适用于标志为 00、长度为 2～6 B的口令密钥。

外部认证密钥，用于外部认证过程中认证鉴别数

据,如被锁死将无法被解锁。涉及外部认证命令操作。

修改透支限额密钥,用于产生修改透支限额交易中使用的过程密钥,在修改过程中计算 MAC 和 TAC。

圈提密钥,用于产生圈提交易中使用的过程密钥,在圈提交易中计算 MAC,涉及圈提操作。

消费密钥,用于产生消费/取现交易中使用的过程密钥,在操作过程中计算 MAC 和 TAC。

圈存密钥,用于产生圈存交易中使用的过程密钥,在操作过程中计算 MAC 和 TAC。

口令密钥 PIN,用于实现对卡片持有者的鉴别,长度为 2 ~ 8 B(中国人民银行应用为 2 ~ 6 B)。每次核对失败时错误计数器自动减 1,当错误数达到 0 时,口令密钥被锁死,须用相关命令解锁。

解锁口令密钥,用于解锁被锁定的 8 B 口令密钥。

4　密钥在 CPU 卡内储存方式及卡文件结构

4.1　CPU 卡的文件类型

用户数据以文件形式存储[7]。在 CPU 卡中,文件系统由主文件(master file,MF)、专用文件(definition file,DF)和基本文件(elementary file,EF)组成。CPU 卡中的文件组织树结构如图 4 所示。

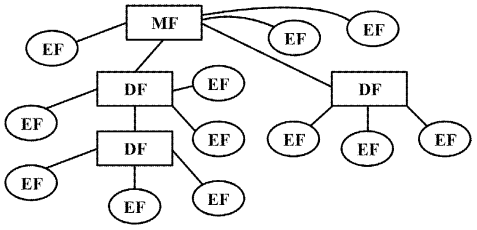

图 3　CPU 卡中的文件组织树结构

Fig. 3　The tree structure of file in CPU-card

4.1.1　专用文件 DF

专用文件好比 DOS 系统的目录或文件夹,在根处的 DF 称 MF,它是必备的。DF 下可支持多级目录,受存储空间限制,不同片内操作系统(chip operating system,COS)支持级数不同。如 TimeCOS 系统支持 3 级,即 MF-DF-DF 形式。

4.1.2　基本文件 EF

基本文件包括工作基本文件和内部基本文件。工作基本文件用于存储不由卡所解释的数据(即用户数据),包括钱包文件等。内部基本文件用于存储由卡所解释的数据,是指为了管理和控制目的由卡分析和使用的数据,如密钥文件。

4.2　密钥存储方式

一个密钥文件中包含多种密钥,每种密钥可以有多个。在 TimeCOS/PBOC 中,密钥文件采用变长记录格式,数据项定义如表 1 所示。

表 1　密钥文件记录格式

Tab. 1　Record format of KEY file

数据元	长度
T	1
L	1
密钥头值	5
密钥值	不同的密钥类型长度不同

由表 1 可知,每条记录长度 = 1 B 标签(表 1 中的 *T*) +1 B 的长度(表 1 中的 *L*) +5 B 的密钥头 + 密钥值的长度。每个 DF 下只能有一个密钥文件,且它必须最先被建立,并根据密钥数量预留足够的存储空间。在任何情况下,密钥数据均无法被读出。

4.3　CPU 卡文件结构

在一般的中国人民银行应用中,通常 CPU 卡文件结构如图 4 所示。

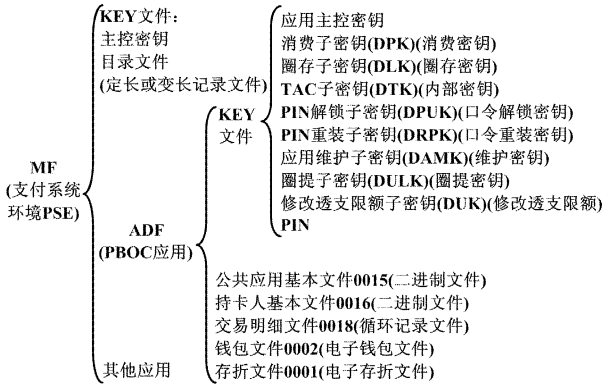

图 4　CPU 卡的卡文件结构

Fig. 4　File structure of CPU-card

5　密钥系统的实现与卡的发行

按照对图 1 各种母卡的管理方式,逐级分散卡片的发行。除密钥体系中最下层,即应用卡片(如用户卡等)外,其余密钥均采用母卡进行严格管理。

在实际应用中,为防止母卡的密钥外泄,还须规定密钥使用年限,在超过规定使用年限后,须更改密钥,同时对系统内所有发行的卡片进行密钥更新操作。

卡片发行,即对卡片进行初始化,建立卡片的文件结构。除对用户卡写入基本数据外,大部分的数据需在实际应用中写入,如流量计用户信息、流量计基本信息等。要写入数据,则需使用终端安全控制模块(pur-

(下转第 72 页)

3　应用实例

本采集器作为数据采集前端应用于某火电厂,其系统示意图如图 3 所示。

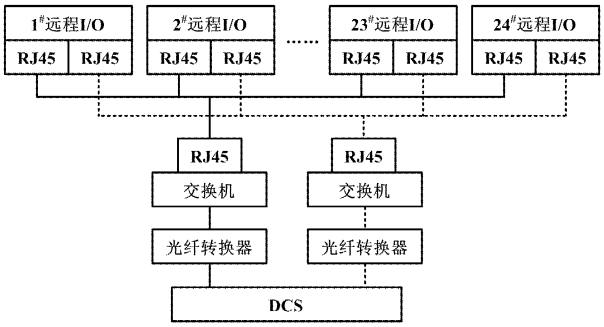

图 3　远程 I/O 数据采集器应用示意图

Fig. 3　Example of application of remote I/O data collector

由图 3 可以看出,数据采集系统使用 24 台远程 I/O数据采集器,采集器采用挂壁式就地安装在被测设备附近。采集器的以太网通信接口使用 RJ45 接口通过双绞线连到交换机上,交换机经光纤转换器通过光缆连到 DCS 系统,通信接口采用双网冗余方式。通信协议采用 Modbus TCP,远程 I/O 数据采集器 IP 地址分别设为 192.168.0.201 ~ 192.168.0.224,服务端口号都设为 502。

这样就实现了远程 I/O 通过工业以太网把测量数据送到 DCS 系统的目的,由 DCS 系统做统一处理后,可作为设备参数监控的依据。

4　结束语

本文介绍了一种基于 ARM 的嵌入式多微处理器结构的远程 I/O 数据采集器,阐述了适用于 DCS 系统的远程 I/O 数据 A/D 转换模块 MCad、DNet 数据通信模块与 DCS 系统通信接口电路的设计与实现。由本方案设计实现的远程 I/O 数据采集器已实现产业化,目前已在国内外近百台 300 MW、600 MW、1 000 MW 大型火电机组中运用,达到了现场抗干扰能力强、运行稳定可靠、安装使用方便和经济实用等设计要求,是代表当今测量技术发展趋势的新型智能仪表。

参考文献

[1] 李正军. 计算机测控系统设计与应用[M]. 北京:机械工业出版社,2004.

[2] 周立功. ARM 微控制器基础与实战[M]. 北京:北京航空航天大学出版社,2003.

[3] 朱三元. 网络通信软件设计指南[M]. 北京:清华大学出版社,1994.

[4] 周明天,汪文勇. TCP/IP 网络原理与技术[M]. 北京:清华大学出版社,1993.

[5] 贾智平,张瑞华. 嵌入式系统原理与接口技术[M]. 北京:清华大学出版社,2005.

[6] 王树清,赵鹏程. 集散型计算机控制系统(DCS)[M]. 杭州:浙江大学出版社,1994.

[7] 王琳,商周,王学伟. 数据采集系统的发展与应用[J]. 电测与仪表,2004,41(8):4 - 8.

[8] 张州,陆静. PROFIBUS 现场总线技术及应用[J]. 上海电力学院学报:自然科学版,2008,24(2):157 - 160.

(上接第 68 页)

chase secure access module, PSAM)卡进行密钥认证。只有通过密钥认证,CPU 卡获得写入权限时才可以写入数据。所以在实际应用中,一般采用 PSAM 卡用于认证,如在重要的数据安全场合,则需采用专用加密机进行数据认证。

6　结束语

CPU 卡在工业流量计的应用仅是个开始,它的应用是多学科、多系统的综合。密钥体系作为应用的核心,决定了 CPU 卡应用的数据安全。用 CPU 卡实现城市燃气预收费系统,有效解决了行业收费问题,有利于事业的发展和人力、物力的节约,具有广阔的应用前景。

参考文献

[1] 李翔. 智能卡研发技术与工程实践[M]. 北京:人民邮电出版社,2003:1 - 20.

[2] 王爱英. IC 卡技术入门[M]. 北京:清华大学出版社,1998:52 - 59.

[3] 董威,杨义先,钮心忻. 基于 JavaSIM 卡的 GlobalPlatform 安全技术研究[J]. 北京邮电大学学报:工学版,2006,29(3):91 - 94.

[4] 肖银良. CPU 卡应用方案和密码管理技术[J]. A&S:安防工程商,2009(12):137 - 139.

[5] 李靖波. 基于密钥系统的 CPU 卡在预付费电能表中的应用[J]. 电力信息化,2008(12):101 - 105.

[6] 郑磊,易波. 于单片机的实时 3DES 加密算法的实现[J]. 微处理机,2000(3):40 - 42.

[7] 张向军,陈克非. 基于 PBOC 智能卡的匿名可分电子货币协议[J]. 计算机应用,2009(7):1785 - 1789.

[8] 中国金融标准化技术委员会. JR/T 0025.1-2005 中国金融集成电路(IC)卡规范第 1 部分:电子钱包/电子存折卡片规范[S]. 北京:中国金融出版社,2005.

[9] 中国金融标准化技术委员会. JR/T 0025.2-2005 中国金融集成电路(IC)卡规范第 2 部分:电子钱包/电子存折应用规范[S]. 北京:中国金融出版社,2005.

[10] 中国金融标准化技术委员会. JR/T 0025.3-2005 中国金融集成电路(IC)卡规范第 3 部分:与借记/贷记应用无关的 IC 卡与终端接口需求[S]. 北京:中国金融出版社,2005.