CPU卡在智能电表中的应用

肖 丽
(四川省电力公司眉山公司,四川 眉山 620010)

摘 要: 主要对智能电表用CPU卡的物理结构、数据交换、指令系统等基础知识进行了整理,结合大量的实践应用,对卡口防攻击电路进行了分析描述,对软件部分关键的认证流程和表内购电流程进行了深入的论述。侧重于理论与实践应用相结合,从硬件及软件两方面论述CPU卡在智能电表中的应用。

关键词: CPU卡; ESAM芯片; 智能电表; 认证流程; 购电流程

Abstract: The basic knowledge of CPU card for smart meter such as physical structure, data exchange, instruction system, etc are sorted out. Based on a large number of practical applications, the anti-attack circuit for card slot is described and analyzed. Some key parts of certification process and the electricity procurement process in this software are discussed. The focus is on the combination of theory and practical application, and the application of CPU card to smart meter is discussed from two aspects of hardware and software.

Key words: CPU card; ESAM chip; smart meter; certification process; electricity procurement process

中图分类号: TM930.9 **文献标志码:** B **文章编号:** 1003-6954(2012)04-0073-03

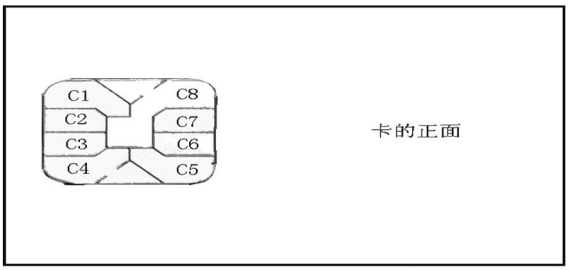
0 前言

CPU卡又称智能卡,指具有微处理器(CPU)和操作系统(COS)的IC卡,目前常用的加密算法有3DES及SM1。由于具有更高的数据安全性,CPU卡智能电能表已经开始大量使用。CPU卡分为接触式IC卡、非接触式IC卡、两种接口方式合一的双界面IC卡。接触式IC卡主要遵循的国际标准为ISO 7816系列标准,非接触卡主要遵循的国际标准为ISO 14443系列标准。智能电表为了保证数据安全交换及可靠认证,表内置ESAM芯片(也属于CPU卡),用于存贮剩余电费、费率参数等关键数据,此类数据只有通过与卡或主站加密机的双向认证才能修改,从而保证了数据的安全性。由于CPU卡和ESAM的认证过程中引入了分散因子及随机数,使用CPU卡的智能电表可实现一卡一密、一次一密,极大提高了智能电表的数据交换及电费、电价数据安全性,目前已经在国家电网大量使用。

1 CPU卡的硬件

1.1 CPU卡的物理结构

CPU卡的物理结构如图1所示,芯片有8个信号接口。



注: C1为V_{cc}(数字电源); C2为RST(复位); C3为CLK(时钟); C4为NC(空); C5为NC(空); C6为I/O(输入/输出); C7为NC(空); C8为GND(地)

图1 CPU卡的物理结构

1.2 ESAM芯片的物理结构

ESAM芯片的物理结构如图2所示,芯片有8个信号接口。

注: 1为GND(地); 2为NC(空); 3为I/O(输入/输出); 4为NC(空); 5为NC(空); 6为CLK(时钟); 7为RST(复位); 8为Vcc(数字电源)

图2 ESAM芯片的物理结构

2 CPU卡的数据交换

2.1 通信时间单位ETU

CPU卡是通过异步通信的方式进行数据交换，I/O口线上所用的数位宽度被确定为基本时间单位ETU，计算公式为 ETU = 372/f，其中 f 为时钟频率，一般在1～5 MHz范围之间选择，一般当时钟频率为3.579 MHz时，数据传输的速率为9 600 b/s。

2.2 数据发送时序

CPU卡的数据传送是以字节为单位的，字节传送的时序如图3所示。

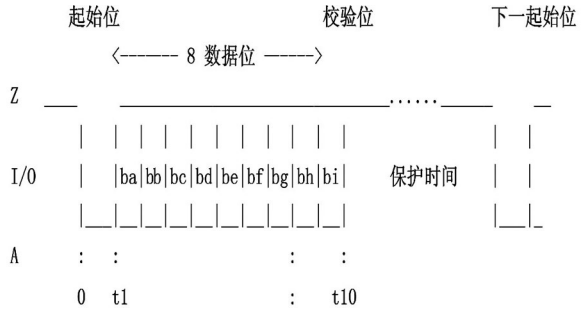


图3 CPU卡字节传送的时序

字符传送前，I/O端应被置为1，如图3所示，一个字符包括10个连续的ETU。第一个时刻 t_1 被置于状态0，这个时刻称为起始时刻；t_2 ～t_9 传送1个字节；最后一个时刻 t_{10} 传送奇偶校验位，当奇偶校验出错时，接收方在10.5 ±0.2 etu时间发送一个状态为0，最少为1 etu，最大为2 etu的出错信号，然后将等待对有争议的字节重发。

2.3 CPU卡指令

CPU卡的指令格式如图4。

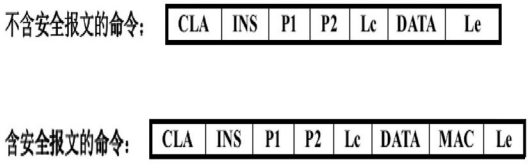


图4 CPU卡指令格式

1) CLA为命令类别，不含安全报文(命令中没有MAC校验)时，为00、0×80，含安全报文命令时为04、0×84；

2) INS为指令，用于规定数据交换作用，如0×82外部认证、0×84取随机数、0×88内部认证、0×30扣款、0×32存款、0×b0读二进制文件、0×d6写二进制文件等；

3) P1、P2为命令参数；

4) Lc为发出的命令数据长度，Le为响应数据的长度；

5) DATA为传输的数据。

6) MAC为含安全报文时的4字节校验数据。

3 CPU卡电能表卡口防攻击设计

接触式CPU卡智能电表由于数据传输速度快、可靠性高而被广泛应用。但接触式卡口由于内部直接与数字电路相连接，容易受到攻击而导致智能电表数字部分损坏失效。为此，智能电表的防攻击卡口设计对智能电表的可靠性提升很关键。通过实验及大量应用，CPU卡电能表防攻击卡口电路可参考图5。

ON_0FF_CARD信号用于控制卡口电源，平时置低电平，CPU卡插卡前不供电，MCU检测插卡信号KEY_CARD电平由高到低后，ON_0FF_CARD置高电平，给CPU卡供电。同时给CPU卡提供时钟信号，时钟信号可使用MCU的时钟输出功能，如NEC、TI等单片机都有主晶振2、4分频后输出口。300 Ω电阻R8、R9、R10、R11串在卡口与MCU通信的数据线上，用于卡口防静电，当对卡口静电攻击时，对MCU及表内数字电路起到保护作用。RT1是封装了热敏电阻及TVS管的专用卡口防攻击模块，可有效防止表外的高压、静电、短路等攻击。

4 软件设计

4.1 CPU卡与表内ESAM模块的认证过程

CPU卡智能电表的数据安全性主要是通过CPU卡与ESAM芯片的双向认证来实现的，表内MCU起数据搬运及流程控制作用。以用户卡为例，当MCU判到插卡后，先做内部认证，通过后认为用户卡与ESAM芯片是同一个系统，可进行读操作；然后CPU卡对ESAM进行外部认证，认证通过后CPU卡开放写权限，可以把ESAM芯片里的数据写入CPU卡内；最后ESAM芯片对CPU卡进行外部认证，认证通过后ESAM芯片开放写权限，可以把CPU卡的数据写入ESAM芯片卡内。具体的认证流程如下。

4.1.1 内部认证流程

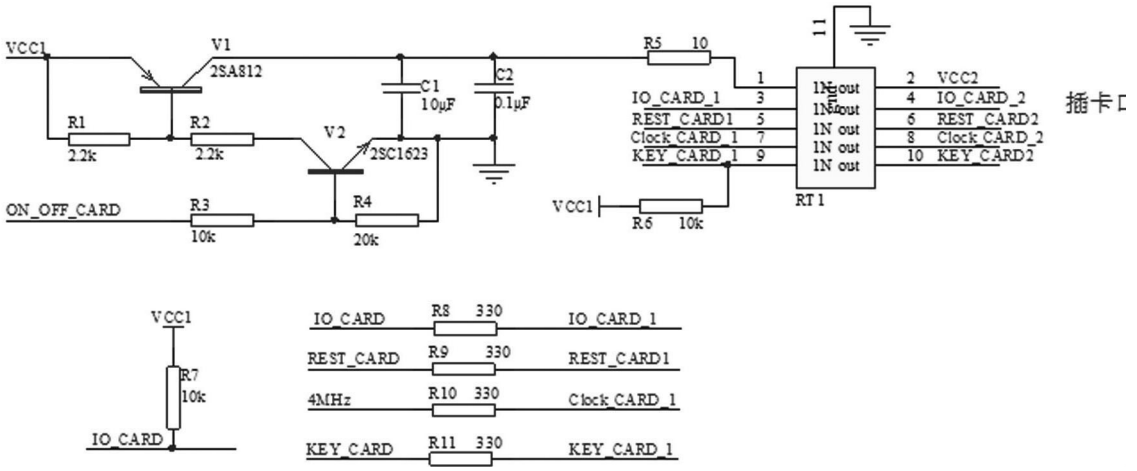


图 5　防攻击卡口电路

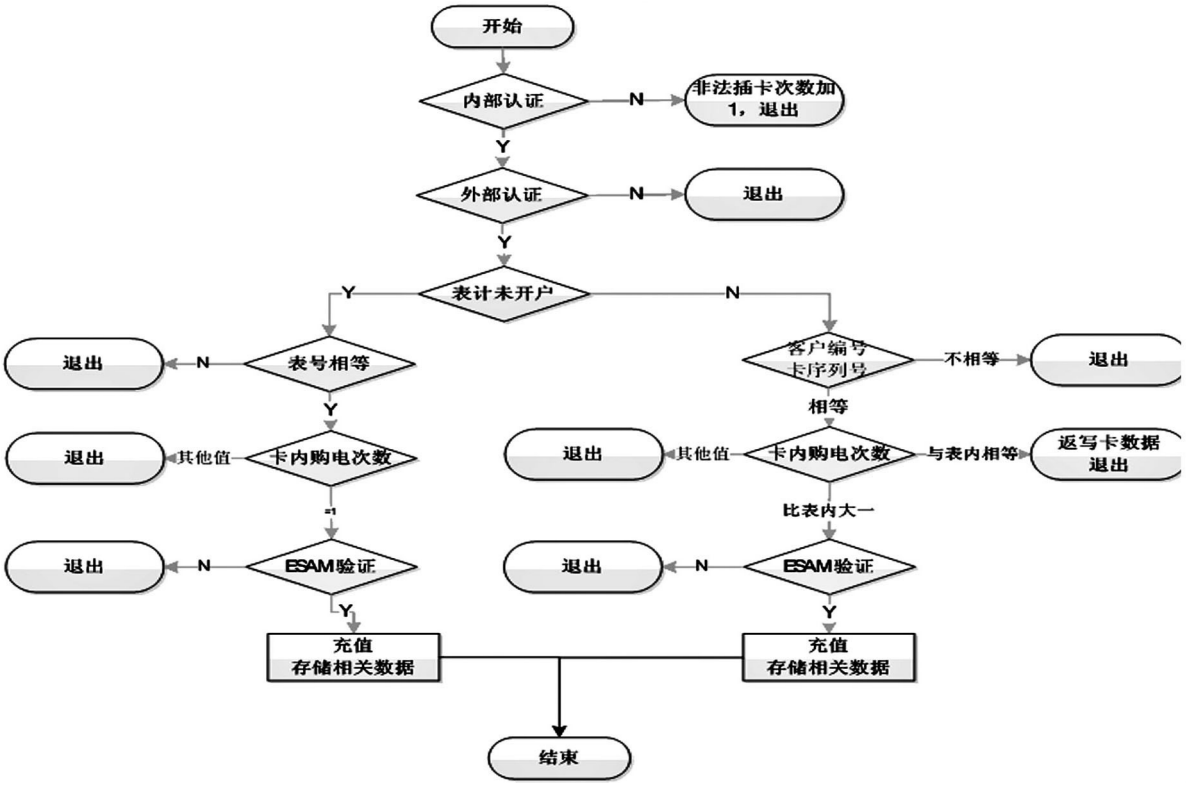


图 6　用户卡购电流程

适用于各种卡片与 ESAM 之间的认证。

1) ESAM 或电能表产生随机数;

2) 卡片对随机数加密获得密文;

3) ESAM 根据卡片卡号产生过程密钥;

4) ESAM 利用过程密钥加密随机数获得密文;

5) 电能表对比卡片和 ESAM 对随机数加密的结果,一致则合法,否则非法。

4.1.2　外部认证流程

情况 1: 用户卡认证 ESAM

1) 用户卡取随机数;

2) ESAM 根据用户卡卡号产生过程密钥;

3) ESAM 利用过程密钥加密随机数获得密文;

4) 用户卡利用以上密文完成外部认证过程,获得相应的写权限。

情况 2: ESAM 认证用户卡

1) ESAM 取随机数;

2) 用户卡加密随机数获得密文;

3) ESAM 利用以上密文完成外部认证过程,获得相应的写权限。

(下转第 86 页)

可承受压强，kPa，因为发电机基坑可承受压力较大，取值为4.8 KPa；X 为泄压孔面积，mm^2。

$$X = 239 \times 672 / 4.8^{0.5} = 73\ 307.19\ mm^2$$

4) 主喷放管路以及延时喷放管路管径选择

$$Q = M/T$$

$$D = (1.41 \sim 3.78)\sqrt{Q}$$

式中，D 为管路直径，mm；Q 为平均主管管路中的流量，kg/min；T 为喷放时间，1 min。

由上式，可计算出主喷放管路与延时喷放管路主管管径均可选用DN50。

5) 管路材质及壁厚选择

管路材质一般根据主、合同要求。合同没有要求的，可以使用不锈钢管、焊接钢管，若使用焊接钢管要内外镀锌，个别项目业主要求不能内镀锌，但可以涂防锈油漆，根据合同要求执行。管路安装完毕后需要进行打压试验，一般钢管均可承受，若合同已经规定的管路腐蚀厚度，应根据管路壁厚计算公式计算，然后选择钢管厚度。公式如下。

$$S = \frac{pd}{2\sigma} + c + \nabla S$$

式中，S 为管路壁厚，mm；P 为管路设计压力，MPa；d 为管路公称直径，mm；σ 为设计工作温度下材料许用应力，MPa；c 为腐蚀厚度，mm；：∇S 为制造偏差，取15%管路壁厚，mm。

6) 灭火后气体抽离系统

发电机灭火后，需要从发电机机坑内将 CO_2 抽离，并且排出室外。

3 结 语

从水电站设立值班人员数量看，中国值班人员较多，国外水电站多按照无人值班设计，尤其是欧洲电站。在中国水电站，发电机水喷雾灭火发生误报警误动作时，若灭火采用自动方式，则水喷雾会使线圈损坏，导致水电站损失较大，所以中国发电机水喷雾灭火一般采用手动方式。当有报警发生后，值班人员去现场确认，确认发生火灾后，手动启动灭火装置，给发电机灭火。这时，发电机灭火快慢取决于值班人员的动作快慢。无人值班水电站一般采用发电机 CO_2 灭火，发生火灾后灭火系统动作迅速，即使误动作，抽离 CO_2 后，不影响机组继续使用。随着社会和科技的发展，中国水电站会逐步实现无人值班，发电机灭火也会由水喷雾灭火为主，逐步改变为 CO_2 灭火。

参考文献

[1] NFPA 12－28，Standard on Carbon Dioxide Extinguishing System [S].

作者简介：

王 伟(1983)，男，学士，主要从事火电调试工作；

曹 静(1986)，女，硕士，主要从事水电站机电设计工作。

(收稿日期：2012－04－06)

(上接第75页)

4.2 购电流程

用户卡购电流程复杂，也是CPU卡操作流程中最关键的部分，需要多次认证及判断，最后才能把购电卡里的电费充值到表内ESAM钱包文件里。图6是结合国内主流售电系统流程的用户卡表内购电流程图。

5 结束语

CPU卡是继存贮器卡、逻辑加密卡后的第三代IC卡，CPU卡及ESAM芯片在智能电表上的应用为智能电表本地安全数据交换、远程加密数据通信提供了重要技术支撑，为未来智能电表的双向信息互动提供了很好的技术平台。CPU卡智能电表会因其快捷的充值操作、安全的数据传递而受到供电局及用户的青睐。

参考文献

[1] ISO/IEC 7816，卡片基本规范及数据交换命令 [S].

[2] Q/GDW_365－2009，智能电能表信息交换安全认证技术规范 [S].

[3] 北京握奇有限公司，TimeCOS/PBOC通用技术参考手册.

[4] 北京融通高科有限公司，ARTCOS ESAM通用手册.

(收稿日期：2012－05－29)