卡式电表主要技术的现状及其发展

作者：铜川供电局　姚卫东　郗晓勇

［摘 要］目前，卡式电表均采用预付费模式，解决了收费难的问题，受到供电部门欢迎；方便了用户，为大多数用户接受。卡式电表欠费的断电方式主要有三种：立即断电；告警断电；柔性断电。立即断电、告警断电显得比较生硬，常常使用户措手不及，并给用户带来损失。柔性断电方案，给用户一定的缓冲，方便了用户，是人性化断电方式。应用卡式电表一定要确保卡交易的安全性。因此，建议各应用部门应尽快放弃使用 DES 算法的 CPU 卡，改用国密委推荐的使用 SSF33 算法（该算法不公开，且可抗 DPA 攻击）的 CPU 卡。

［关键词］卡式电表；预付费；后付费；卡交易安全；柔性断电

卡式电表作为一种技术比较先进、用户及供电部门操作比较简便、有利于在没有集中抄表网络条件下无需抄表即可收费和预收费的电表，得到了供电部门的青睐。二十世纪末二十一世纪初，北京、天津、南京地区大面积的安装和使用，全国其他地区也有大面积应用的趋势；但由于当时一些地区卡式电表出现抗攻击问题、数据交换安全问题、以及电力法的相关规定，除北京地区外，全国各地卡式电表纷纷下马或停止安装。近年来，随着上述问题得到逐步解决，除北京地区继续大面积使用卡式电表外，安徽、新疆、重庆、湖北、河北、云南、山西、陕西、宁夏等地也开始大规模使用卡式电表。本文研讨卡式电表一些主要技术的现状及发展方向，对卡式电表的技术应用具有一定的参考作用。

一、卡式电表的应用模式

目前，卡式电表均采用预付费模式，解决了收费难的问题，受到供电部门欢迎；方便了用户，为大多数用户接受。

1、 预付费模式

预付费方式的卡式电表，主要有如下几种：

（1） 单费率电度预付费（单费率计量，全部时间内均减单一电度）。

（2） 单费率金额预付费（单费率计量，全部时间内均每消耗一单位电量则减单一固定金额）。

（3） 复费率金额预付费（复费率计量，不同时段内按时段每消耗一单位电量则减不同单价金额）。

（4） 复费率等效电度预付费（复费率计量，不同时段内按时段每消耗一单位电量则减不同等效电度值）。

2、 后付费模式

“后付费”模式的卡式电表，主要有如下几种：

（1） 电力部门预给固定电度、单费率抄表决算预付费(单费率计量，任一时段内均减单一电度，抄表决算补回电度)。

（2） 电力部门预给固定电度、复费率抄表决算预付费(复费率计量，尖峰平谷任一时段内均减单一电度，抄表决算补回电度。

（3） 电力部门预给固定等效电度、复费率抄表决算预付费（复费率计量，尖峰平谷时段内按尖峰平谷减值减等效电度，抄表决算补回等效电度）。

（4） 电力部门预给固定金额、单费率抄表决算预付费（单费率计量，任一时段内按单价值减金额，抄表决算补回金额）。

（5） 电力部门预给固定金额、复费率抄表决算预付费（复费率计量，尖峰平谷时段内按尖峰平谷单价值减金额，抄表决算补回金额）。

3、抄表决算

卡表也可用于抄表决算模式，主要有如下两种：

（1） 单费率抄表决算（单费率计量，电表显示表底数）

（2） 复费率抄表决算（复费率计量，电表显示尖峰平谷时段、循显尖峰平谷电量）

此两种模式电表到月决算日后提示“请插卡抄表”，插卡显示上月已用尖峰平谷电量，插卡成功后显示“请到银行交款”。用户到银行（供电营业部门）交款结算后再将卡插入电表，显示消失；如果到下一结算日仍未结算，电表停止供电。

此种方式可大面积解决抄表问题，能防止用户欠费，又不改变供电局现有工作流程，也是卡表的较好的一种应用模式。

二、卡交易安全及卡相关问题

1、卡交易安全

电表使用的卡，最早为存贮卡（也称电钥匙），后为逻辑加密卡，但这两种卡前一种无安全措施，后一种极易破译（明文传递密钥），这两类卡除逻辑加密卡在物业小区范围内仍在使用外，已基本处于淘汰之中；在较大区域或较大城市使用的电表卡，目前均为 CPU 卡，CPU 卡使用 SAM 对机制，使用内部认证、外部认证来实现相互认证，使用 MAC 来保证数据传递的不被修改，确保了交易的安全性。

但是，随着加密/解密技术的发展，我们以前认为绝对安全的加密手段，现在变得不安全了。1996 年开始有公开发表的基于物理特征的密码分析技术学术论文(Cambridge 大学的 Anderson 等人发表了基于不同电压的密码分析方法，美国人 Butch 发表了基于时间和基于差分电压分析的密码分析技术)。从 1999 年起发达国家的政府组织力量研究基于物理特征的密码分析技术， 美国 NSA 投入了九千万美元从事该领域的研究。法国政府也投入了三千万美元从事该领域的研究。世界上最大的智能卡公司 GEMPLUS 在 1999 年投入了六百万美元开展该攻击上的防御技术。2000 年，我国政府和相关研究机构也开始了基于物理特征的密码分析技术的研究。

目前，基于物理特征的密码分析技术特别是 DPA 攻击技术已经普及，它是一种对密码实现系统的有效攻击方法，与穷举计算和差分密码分析的原理不同，它使用少量的普通仪器和简单的分析软件可以在几分钟内破译 512 位的 RSA 和 192 位的 3DES。

DES 是迄今为止世界上最广泛使用和流行的一种分组密码算法，于 1977 年 7 月 15 日生效作为美国联邦加密标准，因为它已经被破译，美国已决定 1998 年 12 月以后将不在使用 DES。而我们目前使用的各种 CPU 卡，均是基于 DES 和 3DES 算法的，据我们掌握的情况，国内已有众多的技术人员可以轻易地破译各厂家 CPU 卡的所有密钥。

另外，目前绝大多数电表公司使用的 CPU 卡交易流程，不符合中总行规定的银行卡交易要求，使用这些卡交易流程的 CPU 卡电表，甚至不需破译密钥，也可实现任意增加电量。

因此，建议各应用部门应尽快放弃使用 DES 算法的 CPU 卡，改用国密委推荐的使用 SSF33 算法（该算法不公开，且可抗 DPA 攻击）的 CPU 卡。

但由于使用 SSF33 算法的 CPU 卡成本昂贵，如果暂时还需要使用 DES 算法的 CPU 卡，建议使用电表-卡交易流程，与老的 CPU 卡表规范兼容，但又堵住了主要的安全漏洞。

2、卡交换信息的时间

卡表的大规模使用的经验证明：卡表故障率的 60%以上为插卡故障。因此，为保证大幅度减少插卡故障，要求用户卡工作过程分段进行，卡工作过程中完成一段，作段完成标记，各段未完成的，结果不生效，下次插入后均可从中断处进行；对于写入新增电量、写入新密钥组、写入新时段费率表/新电价等操作建议以 PBOC 方式进行，数据成组传入 ESAM，事后由电表完成，以实现快速数据交换；返写数据可分多段进行，次要返写数据不全，应不影响银行交易。另外，应严格禁止卡外（除 ESAM 卡、用户卡外）的 MCU 进行加密运算及安全处理，以保证卡交易时间和交易安全。实际运用证实：要求用户卡插卡完成交易时间小于 0.5 秒，方可大幅度降低插卡故障率。

3、接触卡与非接触卡

目前使用的 IC 卡从信息传递模式来分有两类：接触卡与非接触卡，非接触卡也称 RF 卡。非接触卡一般有四种：存贮型 RF 卡，一般用作电子标签；逻辑加密型 RF 卡；CPU 型 RF 卡；双界面型 CPU 卡。若使用非接触卡制作预付费电表，从安全要求来说，只能使用 CPU 型 RF 卡、双界面型 CPU 卡两种。接触型 CPU 卡表卡部份由 ESAM 卡（一般带芯片插座）、卡座（一般还要加上抗攻击电路）、用户卡组成；非接触型 CPU 卡表卡部份由 ESAM 卡（一般带芯片插座）、RF 读写器、双或单介面用户卡组成。使用非接触 CPU 卡，能大大提高电表的工作可靠性，减少供电部门工作人员的劳动量，提高卡信息通信的速率（卡通讯速率为 107Kbps），是当前卡式电表的发展方向。

三、复费率与实时时钟

1、复费率

目前各地区使用的卡式电表基本上都是单费率电度预付费方式，但随着居民用电在电力供应中所占比例的提高，新增电力供应赶不上电力需求的增长，国家电力政策的指向，都需要我们考虑大面积使用复费率计量方式。若使用复费率 CPU 卡式电表，普通居民无论单/复费率计量均可使用相同的电表，便于管理和收费，两种用户可方便地进行转换。复费率 CPU 卡式电表可以设置成单费率 CPU 卡式电表，需要转换为复费率 CPU 卡式电表时，仅需在银行改写用户卡相关文件即可，反之则需更换电表，造成较大浪费。目前，国内已有辽宁、安徽、江苏、上海、浙江、福建、重庆、湖北等多个省市开始或大规模将居民用表改为复费率表，其中上海至 2004 年年底已超过 400 万户，这样，作为卡式电表的设计和制造者必须考虑将其设计成复费率计量方式。据安徽、上海、江苏、浙江等省市大批量装表的经验和教训，复费率最少要设置峰、平、谷三种费率，时段数要大于等于 8，时段表数应大于等于 2。

2、实时时钟的走时与调校

推行复费率表最关键的是要保证时钟的可靠性及全温范围内的时钟精度，根据安徽、上海、江苏、浙江等省市大批量装表的经验，必须要求电表时钟部份使用硬件时钟、实施时钟温度自动补偿，时钟精度在全温范围内年误差在 120 秒之内（该要求已超过当前国标要求），达到此要求，可以确保复费率表大面积运用的成功。

（1）实施电表的时钟温度自动补偿。要求每只电表出厂前检测秒时钟相对不同温度的误差（绝对差和温飘差）并作相关记录并转为修正参数存入本只表中，当工作时，电表自动进行温度测量，依据测量结果挑选合适的参数修正秒脉冲，使时间值在全温范围内年误差控制在某一范围内（例如 120 秒/年），此方法能确保减小电表运行期间的走时误差。

（2）时钟调校方法存问题。某些公司使用部份电表的修正值平均数组来代替每只表的修正值，无法实现每只电表的完全补偿，从而无法达到应有时钟精度；但经过出厂前修正过的带温度补偿的时钟芯片可以达到上述要求（例如美信的 DS3231）。

第一，安全性。A、 目前时钟调校是使用红外抄表器发送时间/日期数据给电表；发送者可以修改抄表器时间/日期，导致修改电表时间/日期。B、传送数据只含一组固定明文密

钥，极易破译或截获，造成非法伪造日期/时间。C、使用广播校时不含密钥，虽有校时范围限制，仍可使用多次广播校时方法实现非法修改时间/日期。D、单片机+外围电路构成多功能电表方案中的问题未得到解决，反而加剧了。例如，当单片机死机时，多功能电表仅计量不能正常进行，当 RTC 加入 IC 后，加上许多专用 IC 有时钟调校功能，用户不能保证专用 IC 的 CPU 死机后，RTC 能正常工作。

第二，准确性。一般抄表器时间绝对误差为±20ppm，温度误差可为±100ppm，再加上人工对抄表器校时的误差，输出的时间经常会误差到几分钟级别，再加上电表时钟走时误差，导致电表时间误差很大，这样将无法保证正确的复费率计量。

（3）时钟调校方法改进方案。不增加 CPU 卡式复费率电表任何硬件成本的条件下，改进方案如下：

第一， 密文校时：电表禁止原来的明文/密钥（红外或其它通讯口）较时，改为密文较时，方法为：电表和电表较时器中均装入一块 ESAM 芯片（卡表可用卡表的 ESAM 芯片），驻留一个不可读的基础较时密钥（128Bit）；较时时，电表较时器先呼唤电表，电表从 ESAM 芯片中取一随机数明文发给电表较时器，同时此随机数用基础校时密钥进行加密（DES 或 SSF33），得到本次解密密钥；电表较时器取出时间/日期值用加密密钥（本次加密密钥生成方法同电表本次解密密钥）进行加密（加密方法同电表），得到时间/日期密文发给电表，电表解密后核对格式和校验核对则接受修改本表时间/日期。此种方法每次密钥不同，无法破译，确保时间/日期传递过程无法伪造和修改。

第二， 广播较时时，主机呼唤群表，主动发随机数，群表不再发随机数，但用与随机数相对应的密钥来解密文（方法同单表密文较时），这样，每次解密密钥也不相同。

第三， GPS 提供不可更改高精度时间/日期值：新开发的电表较时器时间/日期值唯一来源于 GPS 模块，操作者不可更改和插入，确保时间/日期的高精度准确和唯一。

四、红外及其它集抄通讯

绝大多数已装的卡式电表，均未加装红外及集抄通讯接口，只是增加了“检查卡”，用于抄录电表数据和相关状态。我们认为：“检查卡”在实际使用中不如红外抄表器方便和贮存的数据容量大，而现在电表上的红外通讯口成本很低。卡式电表本身是脱网设备，若能通过其它网络联至售电系统主机，则将发挥较大的作用，因此，我们认为，卡式电表加装通讯口是必要的。

对于卡式电表，预留标准接口（建议为带光耦 TTL 电平 RS232），规定该标准接口的点位、信号规范、插接件，规定表内预留空间及相关尺寸，便于增加通讯模块与各种网络联接（RS485、载波、有线电视 HFC 网、电话或 ADSL、GPRS、SMS、IP 等），只需更换通讯模块即可组成各种集抄网。在有两个串口的情况下，红外、集抄标准串口通讯波特率应能独立设置。另外，红外、串口通讯（特别是写命令）应充分考虑信息安全，仅使用清零密钥、编程密钥、对时密钥，错误 7 次以上锁死的方式是远远不够的，必须采用密文或明文+MAC 传递，仅按 DL/T645 规约实施通讯已不能满足现实的要求。

五、欠费断电方式

1、断电方式

卡式电表欠费的断电方式，主要有三种：立即断电：电表欠费开始立即断电；告警断电：告警断电，插卡恢复供电，欠费彻底断电；柔性断电：欠费可适当透支，再不购电时彻底断电。

2、柔性断电

（1） 单费率计量、无时钟方式：欠费开始报警，透支 M 度电量断电；欠费开始报警，透支 M 元金额断电。

（2） 单费率计量，与时钟/日期相关方式：欠费开始报警，可透支 N 日用电后断电；

欠费开始报警，节假日不断电

（3） 复费率计量，不与时钟相关方式：欠费开始报警，可透支 M 度电量断电；欠费开始报警，可透支 M 度等效电度值断电；欠费开始报警，可透支 M 元金额断电。

（4） 复费率计量，与时钟/日期相关方式：欠费开始报警，可透支 N 日用电后断电；欠费开始报警，节假日不断电。

3、断电方式的应用

立即断电、告警断电显得比较生硬，当许多用户表装在表箱内且不易观察时或者不知道告警，彻底断电常常使用户措手不及，并给用户带来损失，不够人性化。

柔性断电方案，给用户一定的缓冲，方便了用户，是人性化断电方式。也可采取几种方案相综合的方式。如欠费后继续透支和欠费时断电，插入用户卡记录透支标记后开始透支等方案。

总之，随着电力系统的发展和广大电力客户观念的转变，“电是商品”已深入人心，卡式电表有望全面普及，具有广泛的应用前景。