IC 卡及其应用

邵建新　杨晓冬　张新峰
(石河子大学师范学院物理系,新疆　832002)　(新疆兵团农 7 师中学　833200)

当今世界信息技术的发展日新月异,一个以采集、开发、利用信息资源为特征的信息技术革命正席卷全球,信息技术已广泛地渗透到社会生活的各个领域:从电话卡到工资卡;从借书卡到售饭卡;从汽车加油卡到健康卡;从 ATM 机到电子商务……无处不见 IC 卡的身影。什么是 IC 卡?它工作的基本原理是什么?安全性如何?有哪些具体应用?本文拟对此作些介绍。

一、IC 卡及其分类

1. 什么是 IC 卡

IC 卡即集成电路卡(integrated circuit card)。它是将一个集成电路芯片镶嵌于塑料基片中,封装成卡片的形式。IC 卡芯片具有写入数据和存储数据的功能,其存储器中的内容根据需要可以有条件地供外部读取,或供内部信息处理和判断之用。

2. IC 卡的分类

(1) 根据卡中所镶嵌的集成电路的不同可以分成 3 类:

a. 存储器卡。卡中的集成电路为 EEPROM(可用电擦除的可编程只读存储器)也写作 E^2PROM;

b. 逻辑加密卡。卡中的集成电路具有加密逻辑和 EEPROM;

c. CPU 卡。卡中的集成电路包括中央处理器 CPU、随机存储器 RAM 以及固化在只读存储器 ROM 中的片内操作系统 COS(chip operating system)。

(2) 根据应用领域来分,有金融卡和非金融卡两种。金融卡又有信用卡(credit card)和现金卡(debit card)等。信用卡主要由银行发行和管理,持卡人可用它作为消费时的支付工具。现金卡又称储蓄卡,可以作为电子存折和电子钱包。另外还有一些预付费卡如公交系统中的交通卡、电表上的 IC 卡等。非金融卡往往出现在各种事务管理、安全管理场所,如身份证明、健康记录和职工考勤等。

(3) 根据卡与外界数据传送的形式来分,有接触式 IC 卡和非接触式 IC 卡两种。接触式 IC 卡使用最为广泛,其芯片有 8 个触点可与外界接触。非接触式 IC 卡的集成电路不向外引出触点,它除了含有 EEPROM、CPU 卡及加密逻辑电路外,还带有射频收发电路及其相关电路。

二、IC 卡的硬件

IC 卡的硬件主要包括两部分:微处理器和存储器。逻辑结构如图 1 所示。在这两部分之间通常还有一些连接电路及控制电路。微处理器接收从接口设备发送过来的指令,对其进行分析后,根据需要控制对存储器的访问。访问时,微处理器向存储器提供要访问的数据单元地址或数据,然后由存储器根据返回对应的数据给微处理器,由微处理器再对这些数据进行进一步处理。另外,IC 卡所需要的运算(如加密运算等)也是由微处理器完成的。在上述诸过程中,如何控制及实现这些过程则是由 IC 卡的操作系统 COS 来完成的。

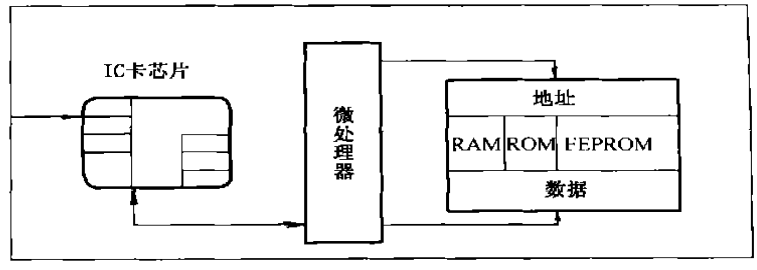

图　1

三、IC 卡的操作系统——COS

COS 是根据各种 IC 卡的具体特点及其应用范围而设计开发的针对外部命令进行处理、响应的专用系统。它的主要功能是控制 IC 卡和外界的信息交换,管理 IC 卡内的存储器并在卡内部完成各种命令的处理。其命令处理的过程如图 2 所示。

1. 传送管理器(transmission manager)功能是根

据 IC 卡所使用的信息传输协议, 对由读写设备发出的命令进行接收; 同时把对命令的响应按照协议的格式发送出去。

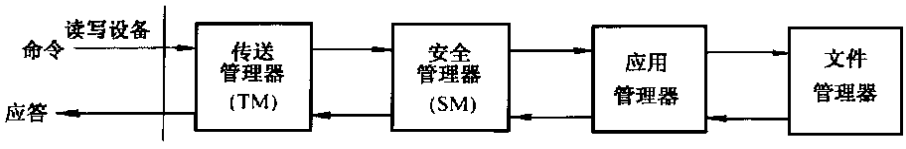

图 2

2. 安全管理(security manager) 包括安全状态、安全属性和安全机制。安全状态是指 IC 卡在处理完某命令之后所处的状态, 通常用 IC 卡在当前已经满足的条件的集合来表示。安全属性则是指定义了某个命令所需要的一些条件, 只有 IC 卡满足了这些条件, 该命令才是可执行的。这样, 如果将 IC 卡当前所处的安全状态与某个操作的安全属性相比较, 根据比较的结果可以很容易地判断出一个命令在当前状态下是否允许执行, 从而达到安全控制的目的。安全机制是安全状态实现转移所采用的转移方法和手段即通行字鉴别、密码鉴别、数据鉴别及数据加密。一种安全状态经过这些程序后就可以转移到另一种状态, 把这个状态与某个安全属性相比较, 如果一致, 则表明能够执行该属性对应的命令。这就是安全管理器的基本工作原理。

3. 应用管理器(application manager) 主要任务是对 IC 卡接收的命令的可执行性进行判断。

4. 文件管理器(file manager) 是对各类文件进行管理。这里文件的含义是指关于数据单元或卡中记录的由组织的集合。COS 通过给每种应用建立一个对应文件的方法来实现它对各个应用的存储及管理。

四、**IC** 卡的安全性

为了保证 IC 卡的安全应用, 芯片制造商和卡的发行商有各自明确的职责。制造商考虑在设计制造芯片时的安全问题: 例如对卡中的 RAM、ROM 和 EEPROM 分成若干个存储区, 根据安全需要对各分区进行读保护, 即在一定条件下, 某些分区不允许读出; 或可以读出但不能送到卡的触点上, 以防不正当窃取; 对 EEPROM 的各个分区还可以分别进行写入/擦除保护; 封闭制造环境和流程, 不准无关人员进入制造区; 各个工序之间保持独立等。发行商则考虑对持卡人、卡和接口设备的合法性进行相互检验; 重要数据进行加密传送; 设置安全区, 其中含有逻辑电路或外部不可读的存储区, 任何有害的不合规范的操作将自动禁止进一步的操作; 设置止付名单(黑名单) 等等。上述一系列安全防范措施, 极大地提高了 IC 卡应用的可靠性与安全性。

五、**IC** 卡应用扫描

1. IC 卡食堂收费系统。该系统包括发卡管理系统和凭卡支付餐费系统两部分组成。前者完成卡的发行管理、成本核算、金额统计、报表打印等; 后者对卡的合法性进行核对, 并显示卡上的金额, 对超过卡上金额的消费予以拒绝。

2. IC 卡考勤管理系统。该系统可对职工的出勤进行考核, 实现自动化管理。独立工作的考勤机平时不需要与微机相连接, 数据存储在考勤机内, 仅当微机要求数据或考勤机存储器不够用时才向微机传送信息。从 IC 卡上读得的考勤数据(姓名、时间等) 可实时向微机传送, 微机可以根据每个人的出勤情况和管理人员制定的考勤规则进行统计处理。

3. IC 卡门锁。这是用 IC 卡来开启门锁的装置, 有门锁和写卡机两部分组成。写卡机用于向 IC 卡内写入密码, 门锁部分用于读取 IC 卡上的密码, 并与存放在门锁内的密码比较, 如相等, 则向电控门锁发出开门命令。

4. 电话卡计费系统。常用的方式是按位计数方式, 如逻辑加密卡用作电话卡时, 是将用户数据区划分成两个区: 其中一个是大额区, 另一个是小额区。用户购买的卡中的 EEPROM 用户数据区全部置成了“1”, 每个“1”代表一个计数单位, 代表一定金额。例如小额区的一个“1”可代表一次市内通话的最低费用, 大额区的一个“1”代表小额区的总和。如果小额区有 1024 位, 则可打 1024 个市内电话或相应金额的长途电话。每打一次电话, 将小额区的一个“1”或若干个“1”置成“0”; 当小额区的“1”全为“0”时, 自动将大额区的一个“1”置成“0”, 并将小额区全部擦除, 并重新全部置成“1”, ……, 直到大小、金额区全为“0”时, 便不能继续使用。

5. 指纹卡身份验证系统。该系统是一种集计算机、网络 IC 卡、光电技术、图像处理、模糊识别、数据库技术于一体的综合管理系统。指纹卡上存有持卡人的指纹图像等有关信息, 并用指纹代替密码。使用指纹卡时, 持卡人只要根据指纹卡身份验证系统的提示, 把手指在取指纹窗上轻按一(下转 57 页)

的事实或现象。此种预言应有极高的精确性，正是在这种意义上数学理论无疑是自然科学的工具，也是自然科学定量化、精确化和严密化的必然需要，是自然科学的灵魂。也就是说没有一定的数学理论的支持物理理论是不可能产生的。自然科学的预测就是采用一定的科学理论和初始条件或边界条件相结合依据演绎数学方法推得特殊结论，正是这些结论才存在与经验资料是否符合的问题。正是在这个意义上物理理论才是一个严格的假说 —演绎系统或公理—演绎系统，离开了数学理论的支持，一切物理理论都将成为不可能的。

3. 对已有科学理论的批判

物理理论产生的另一重要原因就是对已有物理理论的批判与考察。物理理论本身要求其具有广泛的适应性和普遍性，也就是说追求科学的统一性和最大的思维经济性。然而迄今为止科学的发展既呈现出不断分化又不断综合的趋势。科学史向我们表明任何科学理论只能适应于特定的范围和领域，某一科学理论适应有效的特定范围和领域又是通过其他科学理论的产生才得到确定和界定的。爱因斯坦又在对狭义相对论进行批判的基础上提出了广义相对论。在广义相对论中惯性系的优越地位消失，正是通过狭义和广义相对论使我们对时间和空间又有了全新的理解和认识。正是通过狭义和广义相对论又把我们的认识推进到了宇观和高能的领域。由此可见，通过对已有物理理论的批判表现出新物理理论的产生又具有一定的自主性和内在的规律性。

现代意义上的科学理论与以前理论体系的重要差别就是科学理论不再是一种纯思辨的体系。作为科学理论的产生是主体智力劳动的结果，具有主观性；科学理论作为指导科学实践的工具要求其具有客观性的特征。因此科学理论的产生、发展和完善是一个历史的过程，是一个由主观向客观转化的过程。

据上面的讨论可知科学理论的产生是一个极其复杂而又艰辛的过程。作为产生科学理论的归纳法和演绎法都是片面的，仅仅反映了其产生过程一个侧面的特征。科学理论产生的复杂性致使许多科学哲学家把科学发现的逻辑排除在研究领域之外。从伽利略开始就把科学理论和实验有机地联系起来进行了卓有成效的研究。正是伽利略开创了现代自然科学研究的一般方法。我们已经表明不仅经验资料渗透着科学理论，科学理论中也渗透着经验资料的信息，二者之间既相互独立、相互依赖又相互作用。正是物理理论与经验资料之间的互动作用促使新的物理理论产生并不断地把经验资料纳入新的物理理论的逻辑体系。我们也应该明白这样一个基本的事实，没有一定构造和创造性的语词即基本语言系统的存在，经验资料的表述也就不可能，也不可能把其从纯粹经验之中分离出来。物理理论的构造即与采用归纳法、演绎法、类比法、理想化和抽象化的方法等有关。也与适当概念的产生、数学理论、较系统的经验资料的取得和对已有物理理论的批判有关。在科学理论的构造过程中想象力具有极为重要的作用。正如爱因斯坦所言：“想象力比知识更重要，因为知识是有限的，而想象力概括着世界上的一切，推动着进步，并且是知识进化的源泉。严格说来，想象力是科学研究中的实在因素。”也就是说，若没有极其丰富的想象力，物理理论也就不可能产生。物理理论的产生是一种主体理智的构造和发明活动，此种活动又是以当时获取的经验资料、科学理论水平、科学实践的水平和文化传统为素材并受其制约的。

只有通过不断地科学实践，获取新的经验资料，开发新的研究领域，经验资料就有可能与现有的物理理论发生矛盾，也就预示着需要新的物理理论。正是科学实践的需要推动着新的物理理论产生，反过来新的物理理论又指导科学实践，促使新的物理理论发展和完善。

(上接 32 页)下，该系统就能识别持卡人的身份。即使指纹卡丢失，拾到的人也无法使用，因为世界上没有两个完全相同的指纹。

6. 电度表 IC 卡预收费系统。由 IC 卡发行系统和电度表 IC 卡使用系统两部分组成。用户到 IC 卡发行部门或代理银行预交费(售电)，发行部门在 IC 卡内写入允许用电的数量及用户标识码，该标识码与装在用户处的电表是一一对应的。同时，将用户的用电情况记录在本系统微机的数据中，以备日后查询。用户将 IC 卡插入电表中即可用电。

像 IC 卡交通收费系统、汽车加油系统、汽车停车收费系统、市民健康卡等都是 IC 卡的应用。随着我国经济的发展及 IC 卡技术的不断完善，IC 卡应用的范围会越来越广泛。