

基于商用密码技术的校园卡安全保障系统 技术白皮书



华翔腾数码 华翔腾数码科技有限公司

地址：长沙麓谷高新区麓龙路 199 号标志麓谷坐标 15 楼

邮编：410205

电话：(86) 731-88239608

传真：(86) 731-88239600

1 问题的提出

日前，工信部发布了《关于做好应对部分 IC 卡出现严重安全漏洞工作的通知》，要求各地各机关和部门开展对 IC 卡使用情况的调查及安全应对工作。工信部的这则通知的背景是什么呢？据了解：主要应用于 IC 卡系统的 Mifare 芯片的安全算法已遭到破解！目前应用此技术的 IC 卡也都将面临巨大的安全隐患。

与此同时，教育部也通知各级教育管理机构，要求各部门对 IC 卡的使用情况进行清查，并及时做好安全应对工作。

事实上，早在几个月之前，国家密码管理局就已经发出通知，要求各级密码管理部门对辖区 IC 卡的使用情况进行摸底，并责成使用单位提供安全保障体系说明，必要时还需要对安全保障体系进行升级。

1.1 什么是 IC 卡

IC 卡即集成电路卡，是一种内藏大规模集成电路的塑料卡片。IC 卡通常可分为存储卡、逻辑加密卡 and 智能卡三类。存储卡是可以直接对其进行读、写操作的存储器；逻辑加密卡是在存储卡的基础上增加了读、写加密功能，对逻辑加密卡进行操作时，必须首先核对卡中的密码，密码正确才能进行正常操作；智能卡则带有微处理器(CPU)，同时也称作 CPU 卡。

尽管存储卡、逻辑加密卡和智能卡三类 IC 卡的安全性依次提高，但成本也依次提高，所以综合考虑安全性和成本等因素，目前市面上用得最广泛的是逻辑加密卡。目前各类学校使用最普遍的校园卡也是逻辑加密卡，其中既保存有不频繁修改的管理信息，如学籍登记信息等，也保存有频繁改动的电子钱包信息。

1.2 逻辑加密卡的存储结构

Mifare 技术是一种 13.56 MHz 非接触式 IC 卡技术，目前市面上的逻辑加密卡基本上都采用了 Mifare 技术。

采用了 Mifare 技术的 IC 卡，通常分成若干个扇区，每个扇区包含若干块，块是 IC 卡的最小操作单位，块包括数据块和控制块。

其中数据块可作两种应用：

1. 用作一般的数据保存，可以进行读写操作；
2. 用作数据值，可以进行初始化、加值、减值、读值操作；这种应用模式通常称之为“值块”。

控制块包括了密码 A、密码 B 和存取控制位。通过存取控制位的组合，可以确定访问某个数据块是否需要验证密码，以及需要验证密码 A 还是验证密码 B，或者两个密码都需要验证。

1.3 卡信息不再安全

IC 卡卡信息的加密与解密永远都是一枚硬币的两面，每天在世界的各个地方，都有无数的科学家、学者和黑客们不停地在研究着各种加密和解密的技术与技巧，成功与失败也在不断地上演着。2008 年，德国研究员亨里克·普洛茨和美国弗吉尼亚大学在读博士卡尔斯滕·诺尔就享受到了成功的喜悦：他们最先利用电脑成功破解了 Mifare 芯片的安全算法。而他们所破解的 Mifare 芯片的安全算法，正是目前全世界应用最广泛的非接触 IC 卡的安全算法！

对于使用 Mifare 技术的 IC 卡来说，卡信息是明文存放的，但只有通过卡片与读卡器的相互认证才有权对卡信息进行读写。换言之，卡信息的安全完全是依靠存取控制来保障的。这就好像我们家里没有保险柜，没有上锁的抽屉，甚至银行帐户也没有密码，家庭财产的安全完全依赖于大门的安全。而 Mifare 芯片安全算法破解技术，就类似于开锁技术。一旦小偷掌握了任意打开我们门锁的技术，我们家庭财产的安全性也就可想而知了。

可以想象，如果不法分子也掌握了这一 Mifare 芯片安全算法的破解技术，那么使用 Mifare 芯片的 IC 卡，如在校学生普遍使用的校园卡，将面临巨大的安全威胁。不法分子可以随意修改卡内的信息，比如原来电子钱包中剩余 10 元，不法分子就可以随意改成 1000 元或者 10000 元，甚至更多。这对持卡人、学校和整个消费系统来说，无疑是一个极大的安全隐患。

2 问题应对措施

2.1 校园卡现状

目前，我国各级各类学校普遍使用的校园卡，主要包括电子支付和身份识别两大功能。教师、学生手持校园卡在校园内可以方便快捷地完成就餐、超市购物等各种校内消费，还可以实现图书借阅、上机、医疗、出入门禁、用水用电管理、自助洗衣、自助复印、考试管理、学籍注册、学费缴纳等，大大提高了学校教学、管理、服务和生活的整体水平。此外，校园卡系统还可以通过圈存机与银行后台对接，使持卡人可以直接将银行卡中的钱圈存到校园卡，从而使学校的信息管理更加人性化。

通常的校园卡都包含以下几类信息：

1. 卡片基本信息：卡芯片制造商在芯片出厂时写入的芯片相关信息。此信息不可修改，同时也不会对系统安全造成影响。
2. 卡应用基本信息：校园卡持有者在校园卡应用系统中的基本信息，由应用系统写入。这部分信息可能包含有效证件类型、证件号码、姓名、籍贯等，在应用有效期间很少修改。
3. 卡应用扩展信息：校园卡持有者在校园卡应用系统中的扩展信息，由应用系统写入，可能包括学籍登记信息、借书证、学习成绩等信息。这类信息在不同的应用系统中会有不同具体内容，可以被学校管理部门进行修改，但修改的频率很低。
4. 电子钱包：校园卡在校内消费交易系统中主要被访问的区域。校内消费应用的场合很多，包括每天的餐饮、开水、洗浴、上机、杂物购买等，所有消费行为都需要使用到电子钱包。

为了便于管理，各学校一般都采用了“预付费”方式进行卡内电子钱包的充值。由于技术和经费的原因，消费点的终端设备并不实时与学校的后台数据库连接，因此不能实时核对卡内金额是否被异常修改，也无法校验所用卡片的合法性。非实时联网带来的另外一个问题就是黑名单和白名单更新的滞后，这也使得某些不法行为有了操作的时间。

2.2 校园卡安全隐患

目前校园卡最主要的安全问题就在于对电子钱包的有效保护，因为这个问题直接威胁到了整个校内交易系统的安全性和学校的合法权益。

常见的针对校园卡的卡信息恶意修改主要包括以下两种方式：

1. 根据破解的信息格式，重新改写 IC 卡内电子钱包的金额，甚至直接产生一张新的 IC 卡。这种数据修改方式，可以称之为“异卡复制”。
2. 未能准确获取、破解卡内信息，而是通过获得本卡的电子钱包的信息拷贝，在消费后重置卡内的电子钱包。这种数据修改方式，可以称之为“本卡复制”。

异卡复制是非常严重的情况，它意味着不法分子可以无限制的大量制造无法识别的假校园卡，伪造卡虽然不能在学籍等管理系统中使用，但可以在校园卡的消费系统中使用，从而实现非法牟利并导致消费系统紊乱。

本卡复制由于只能复制到本卡，使用的可能性比较小。即使少数不法分子做了本卡复制，学校也可以通过技术手段很快定位嫌疑人。本卡复制问题目前还没有很好的技术解决方案，只能通过管理手段尽量避免这种情况的发生。

2.3 校园卡安全升级

为了有效防范 Mifare 算法破解所带来的安全隐患，我们认为最根本解决方案是彻底改造现有校园卡系统，将逻辑加密卡替换为 CPU 卡。相比逻辑加密卡，虽然 CPU 卡出现的时间较晚，成本较高，但因为 CPU 卡拥有独立的 CPU 处理器和芯片操作系统，可以更灵活的支持各种不同的应用需求，交易也更安全。CPU 卡的优势主要体现在数据安全性更高、应用更加灵活。目前，欧洲各国的银行卡普遍是采用 CPU 卡，至今未出现被破解和攻击等恶性事件，充分说明了 CPU 卡的安全性优势。

但现有校园卡系统的改造并非一朝一夕之功，在彻底的替换方案实施以前，我们不能消极等待，而是必须寻找合理的过渡方案。

我们注意到，安全算法可以被攻破，但只要从系统层面周密考虑，合理布局，那么卡片算法破解后出现的一系列安全隐患都将得到有效遏制。我们在这里介绍

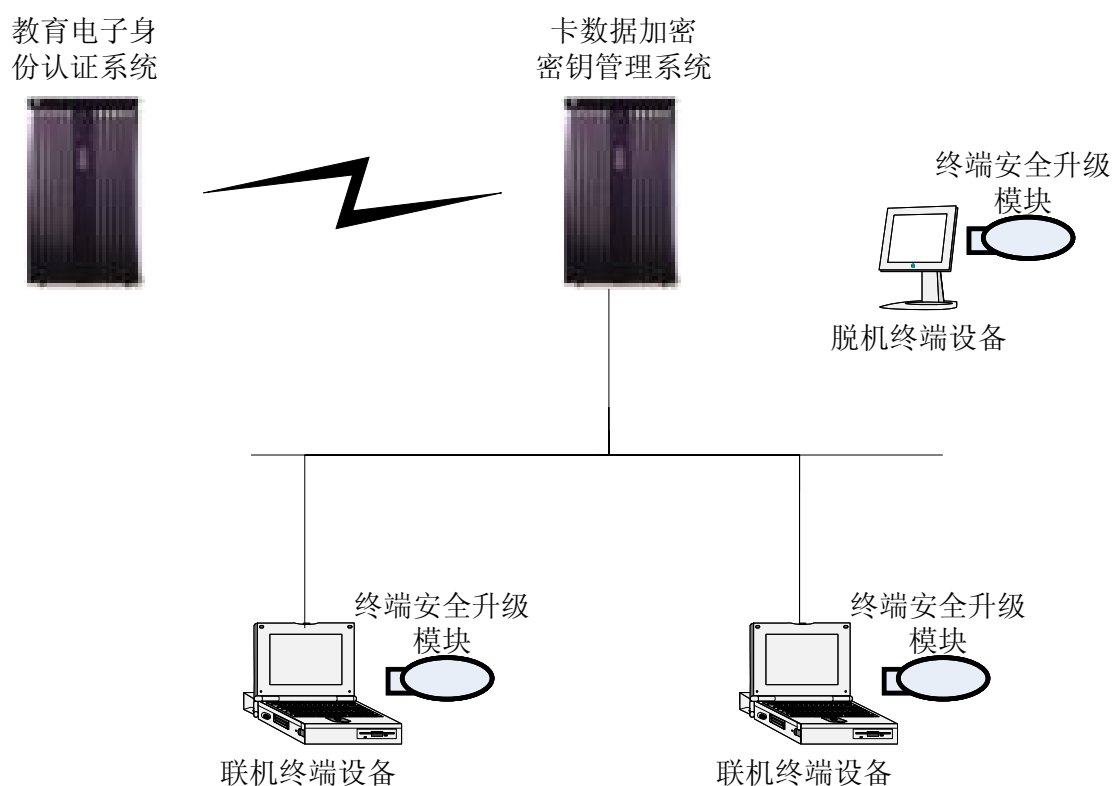
的“基于商用密码技术的校园卡安全保障系统”，是一个采用国产密码算法，使用经过国家密码主管部门批准的密码产品，对校园卡卡信息进行有效加密处理的校园卡安全升级过渡方案。

2.4 校园卡安全升级过渡方案

如前分析，本过渡方案着重处理异卡复制的问题。

本方案要求在终端机上增加终端安全升级模块，终端机在对卡片进行读写时，通过调用终端安全升级模块来实现数据的加解密操作。数据经过终端安全升级模块加密后以密文形式存入卡片，需要使用该数据时，终端机读取卡片密文数据，终端安全升级模块将密文还原成明文。这样一来，尽管 IC 卡的存取控制机制已经失效，但由于卡内信息经过加密处理，从而保证了即使数据被非法获取，非法分子也无法解析数据，更不能改变数据。

系统拓扑结构如下图所示。



由上图可见，我们将终端设备分为联机终端和脱机终端两大类，不同类型的

终端设备使用不同的终端安全升级模块。卡数据加密密钥由专门的管理系统进行管理，并通过安全途径分发到终端安全升级模块。教育电子身份认证系统为本系统提供电子认证服务。

3 系统配置

本系统由以下几部分组成：

1. 卡数据加密密钥管理系统软件：一套。
2. 教育电子证书：所需数量根据学校的规模而定，最少需要六份电子证书。
3. 终端升级安全模块：所需数量和类型根据终端设备的数量和类型而定。
4. 终端安全升级 SDK：一套。

4 系统特点

本系统具有以下显著特点：

1. 符合国家有关产业政策，能保证现有校园卡应用系统平稳过渡。
2. 符合国家密码管理政策，全部采用经过国家密码主管部门批准的密码设备。
3. 采用卡片关联的信息加密技术，卡片信息读出后无法解析，卡片信息复制会直接导致卡片信息失效，能有效防止对卡片信息结构、信息内容的破解。
4. 采用“一卡一密”进行系统设计，确保每张卡片使用不同的加密密钥，提高系统的抗风险能力。
5. 采用教育电子身份认证系统签发的教育电子证书，确保系统设备、操作人员以及系统自身的安全。
6. 采用了不同类型的安全模块，充分考虑了各种不同类型终端设备对密码运算处理能力的要求。
7. 具有良好的兼容性，系统在部署时不需要改变现有校园卡应用系统的结构。

8. 具有良好的可扩展性，能满足不同规模的校园卡应用系统的安全升级的需要。
9. 具有良好的可操作性，对现有校园卡应用系统只做了最小的改动，系统的实施不会对校园卡应用系统的正常运行造成太大影响。