Mifare 安全性与对策

南湘浩　中国军事科学院

摘　要：最近，灵巧卡 mifare 的被破解，以及仿真破译机 ghost 的出现，可以随心所欲地生产合法的灵巧卡，给射频卡生产厂家和使用单位带来极大压力。本文探讨了 mifare 在 cipher01 的设计上存在问题的原因，并针对问题深入分析了应对策略，认为目前唯一可行的方法是 RFID 技术与 CPK 鉴别技术的结合。

关键词：mifare，CPK，RFID，安全，识别

The Security Issue for Mifare and Solution

Na Xianghao

Abstract: Recently, smart cards mifare have been cracking, as well as simulation of the emergence of ghost deciphering machine, you can produce a legitimate smart card as long as you want to, those have given tremendous pressure to manufacturers and exert on the use of units. This paper discusses the problem of mifare, and analysis that the only feasible way to solve this problem is the combination of identification techniques of RFID technology and CPK.

Key words:mifare,CPK,RFID,safety, identification techniques

1 技术背景

近年来除无线射频卡(RFID)又发展出无线灵巧卡(smart card) mifare。RFID 广泛适用于物流管理、出入控制等领域；灵巧卡除存储功能外，还有简单的计算功能，适用于公交卡、电子钱包等数据变动的场合。

无论是存储卡或是灵巧卡，其安全性要求是相同的，即：一是防复制性；二是防仿冒性。对于复制性，只能靠物理特性解决，逻辑方法是无能为力的；对于仿冒性，只能靠逻辑特性解决，物理方法是无能为力的。因此全世界一直在寻求一种物理的和逻辑的相结合的出路。

RFID 的首要特性是标识的唯一性(UID)，一张卡一个号。因为 ID 号是该卡的唯一标识，保证这个标识的真实性成为主要问题。

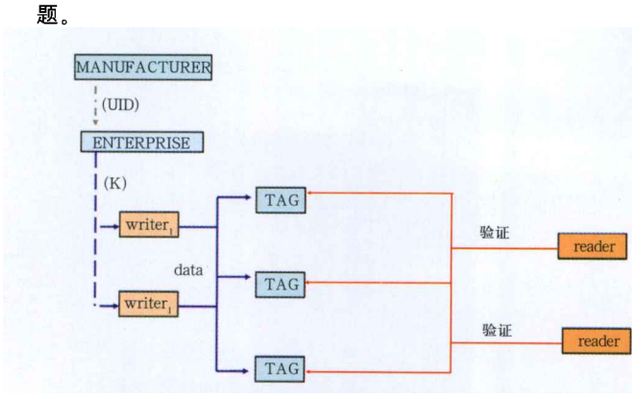

图 1　写入仪和读写器认证

mifare 的设计特点反映了鉴别关系的不同理解。在写入仪(writer)、TAG、读卡器(reader)三者之间，mifare 则突出了读卡器和 TAG 之间的互相鉴别。由此不得不给予 TAG 一定的"智能化"功能，于是在 TAG 中设置了密码器和随机数发生器等简单的动态器件，勉强与读卡器交互鉴别。这种交互鉴别不可能是对等的，因为读卡器是有源的智能器件，而 TAG 是无源的记忆器件，由此产生了不可克服的致命漏洞。

(1) 随机数发生器是一个 16 级线性反馈移存器，其初值为开机时间。开机时间是可知的，因此整个序列可以说是"明"序列。

(2) 密码器 cipher01 是一个 48 级的线性反馈移位寄存器。

生成多项式：

f(x)=(48,43,39,38,36,34,33,31,29,24,23,21,19,13,9,7,6,5,0)

连接多项式：

f(x)=(0,5,9,10,12,13,15,17,19,2425,27,29,35,39,41,42,43,48)

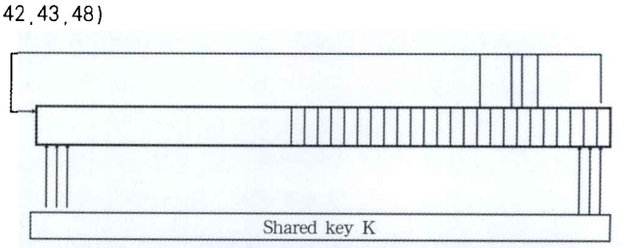

图 2　cipher01

(3) 在鉴别协议踪迹分析中可发现，在TAG和读卡器的密码器的密同步过程不可能以隐蔽方式进行。

Step	sender	Hex	abstraction
01	Reader	29	req type A
02	Tag	04 00	it's 1k
03	Reader	93 20	your UID?
04	Tag	c2 a8 2d f4 b3	UID bcc
05	Reader	93 70 c2 a8 2d f4 b3 ba a3	want to talk to (UID)
06	Tag	08 b6 dd	that's ok
07	Reader	60 30 76 4a	auth(block30)
08	Tag	42 97 c0 a4	n_T
09	Reader	7d db 9b 83 67 eb 5d 83	$n_R \oplus ks_1, a_R \oplus ks_2$
10	Tag	8b d4 10 08	$a_T \oplus ks_3$

图3 Authentication Trace

(4) 从cipher01密码器的结构和协议的执行看，外界输入n_T(由随机数发生器产生)和UID直接暴露于外面，因此为推导出线性反馈移位寄存器(LFSR)初值K提供了依据。

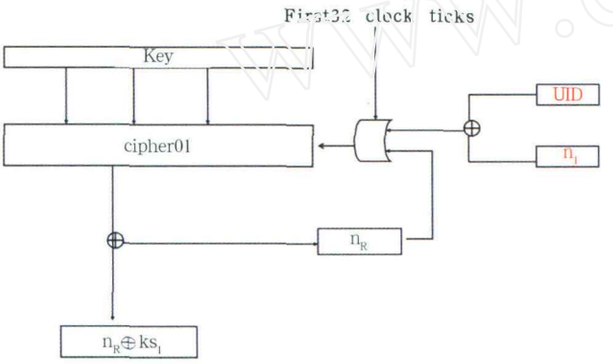

图4 Mifare Classic Attack

由此可见，mifare的鉴别和加密是不可靠的。最近，灵巧卡mifare的被破解，以及仿真破译机ghost的出现，可以随心所欲地生产合法的灵巧卡，因而在国内外引起了很大恐慌，给射频卡生产厂家和使用单位带来极大压力。

现在讨论另一种设计思想，就是在写入仪、TAG、读卡器三者之间，突出写入仪和读卡器之间的互相鉴别，TAG只是作为写入仪的代理工具，写入仪和读卡器均为有源的智能器具，互相鉴别可以是对等的。由此大大降低了对TAG的苛刻要求。

但是，要做到这一点，需要新的鉴别技术支持。值得庆幸的是，基于CPK的标识鉴别技术，能够直接应用于写入仪和读卡器的互相鉴别中，在更高的水平上实现防复制、防假冒。CPK是目前唯一能用于标识鉴别的公钥体制，提供数字签名和验证，以及数据加密和脱密的功能。北京易恒信(e-Henxen)公司已有CPK-chip、CPK-key、CPK-card等现成产品，直接可以应用。

下面就mifare鉴别系统，讨论在不改动TAG结构的情况下增加CPK鉴别功能的具体方法。TAG中的数据将分类为固态数据和动态数据。固态数据由写入仪(writer)定义，读卡器(reader)只能读，无权改动，如证件中的基本要素等；动态数据由写入仪定义，读卡器有权读、写，如公交卡中的余额等。不同类的数据存放在TAG的不同的区域。

2 芯片的鉴别

原有鉴别协议01步到10步的问答照常进行，但是对判定结论的解释则不相同。在本方案中的结论只是：如果通过了鉴别协议(数据加密之前)，读卡器则认为所用芯片为本厂的芯片，进入数据鉴别过程，否则认为假冒芯片，退出过程。

3 数据的鉴别

数据的鉴别是追加的功能，由CPK鉴别协议提供。将CPK-chip或CPK-key插入写入仪(writer)和读卡器(reader)两个智能终端，使其具有CPK鉴别功能，使TAG和读卡器之间的鉴别关系改变为读卡器和写入仪之间的鉴别关系。

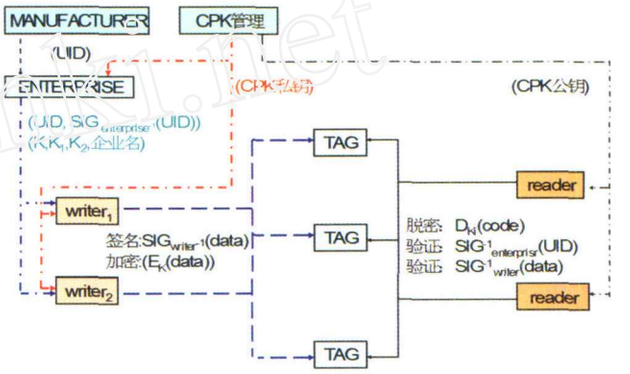

图5 写入仪和读卡器认证

将CPK-key分发给各写入仪$writer_i$和读卡器$reader_j$，也可以分发到写入仪的每一操作员($operator_j$)。另行设置两个密钥K_1和K_2，以加密的形式存放于CPK-key中，分别用于固态数据加密和动态数据加密。K_1与K_2密钥长度暂定为48bit，加密体制为AES，CPK公钥密钥长度暂定为96bit(12B)。基于CPK的Mifare鉴别协议如下：

(1) 厂家(manufacturer)：定义UID，将UID写入TAG提供企业；

(2) 企业(enterprise)：对UID签名，$SIG_{enterprise}-1(UID)=sign_1$

将签名$sign_1$写入TAG中，提供各写入仪($writer_i$)，

(3) 写入仪($writer_i$)：写入仪可以是多个，应编号，各负其责。

1)对固态数据($data_1$)签名：

$SIG_{writer_i}-1(data_1)=sign_2$

2)对动态数据($data_2$)签名：

$SIG_{writer_i}-1(data_2)=sign_3$

3)对固态数据($data_1$)用专用密钥k_1加密：

E_{k1} (data1)=$code_1$

4)对动态数据($data_2$)用专用密钥k_2加密：

E_{k2} ($data_2$)=$code_2$

(4) 操作员($operator_j$)：一个写入仪可以配置多名操作员，操作员代理执行写入仪的功能，除具有写入仪的操作功能外，允许每一操作员提供数字签名服务，以明确操作责任(可选)。

1）对固态数据签名：

$SIG_{operator_i}-1(data_1)=sign_4$

2）对动态数据签名：

$SIG_{operator_i}-1(data_2)=sign_5$

（5）读卡器i（$reader_i$）：读卡器可以是多个，读卡器的主要功能是验证，但是对改动的数据签名的功能（可选），读卡器如果没有签名功能，则可不编号。

1）企业对UID签名的验证：$SIG^{-1}{}_{enterprise}(UID)=sign_1'$

2）写入仪对固态数据签名的验证：$SIG^{-1}{}_{writer_i}(data_1)=sign_2'$

3）写入仪对动态数据签名的验证：$SIG^{-1}{}_{writer_i}(data_2)=sign_3'$

4）操作员对固态数据签名的验证：$SIG^{-1}{}_{operator_i}(data_1)=sign_4'$

5）操作员对动态数据的验证：$SIG^{-1}{}_{operator_i}(data_2)=sign_5'$

6）读卡器i对动态数据的签名：$SIG_{reader_i}-1(data_2)=sign_6$

7）读卡器j对动态数据签名的验证：$SIG^{-1}{}_{reader_j}(data_2)=sign_6'$

8）对固态数据的脱密：$D_{K1}(code_1)=data_1$

9）对动态数据的脱密：$D_{K2}(code_2)=data_2$

10）对动态数据的加密：$E_{K2}(data_2)=code_2$

CPK的鉴别功能是强大的，但不是功能越多越好，而是满足需求的最简单认证结构才是最合理的认证结构，应当根据不同系统的不同需求，适当选择必要的功能是至关重要的。

4 安全性分析

（1）cipher01只作为该芯片是否本厂TAG的判别，ghost的仿真作案，只影响本判别，不造成更大危害。

（2）企业对UID的签名，保证了UID的真实性和负责性，并防止假冒的可能性。

（3）写入仪和操作员对数据的签名，保证数据的真实性和负责性。

（4）TAG中的数据均以加密的形式存放，使复制失去意义。

（5）CPK是智能卡系统，具有很强的访问控制机制和防复制、防假冒功能，足以对付ghost等仿真攻击。

总之，mifare尽管在cipher01的设计上存在一些问题，但是在工程设计上是相当成功的，仍不愧是一个很好的防伪器件。通过mifare的鉴别协议的分析和CPK鉴别协议的研究，对RFID芯片的设计、应用等，有了更深刻的理解。Mifare尽管设置了动态的密码器，但远不是智能卡，只不过是较好的灵巧卡而已。无论RFID作为存储卡还是灵巧卡，都有各自的用途，如果想要设计得好，应用得好，工程技术人员和鉴别技术人员必须相结合。从上述鉴别方案的讨论中可以看出，RFID技术与CPK鉴别技术的结合是最简捷的方法，截至到目前，是唯一可行的方法。尽管如此，在信用卡等大额支付系统中不建议使用RFID，而直接使用智能的CPK-card为好。（特约记者 苏亚娟 采稿）**RFID技术与应用**

参考文献

[1] "Dismantling MIFARE Classic", by Flavio.D. Garcia et al. http://www.sos.cs.ru.nl

[2] "组合公钥（CPK）体制标准 v2.1" 南湘浩，陈华平，陈钟 http://www.e-henxen.com

[3] "CPK密码体制与网际安全" p127-135 南缃浩，国防工业出版社，2008.12

图片快讯

胸章臂章下有RF标签

RF卷标标签