MF1PLUSx0y1 器件

快速易用的主流非接触式智能 IC 卡

产品简介

Rev.3.0

广州周立功单片机发展有限公司

地址：广州市天河北路 689 号光大银行大厦 12 楼 F4

网址：http://www.zlgmcu.com

技术支持

如果您对文档有所疑问，您可以在办公时间（星期一至星期五上午 8:30~11:50；下午 1:30~5:30；星期六上午 8:30~11:50）拨打技术支持电话或 E-mail 联系。

网　　址：www.zlgmcu.com
联系电话：+86 (020) 22644358 22644359 22644360 22644361
E-mail：zlgmcu.support@zlgmcu.com

销售与服务网络

广州周立功单片机发展有限公司

地址：广州市天河北路 689 号光大银行大厦 12 楼 F4 邮编：510630
电话：(020)38730972 38730976 38730916 38730917 38730977
传真：(020)38730925
网址：http://www.zlgmcu.com

广州专卖店

地址：广州市天河区新赛格电子城 203-204 室
电话：(020)87578634 87569917
传真：(020)87578842

南京周立功

地址：南京市珠江路 280 号珠江大厦 2006 室
电话：(025)83613221 83613271 83603500
传真：(025)83613271

北京周立功

地址：北京市海淀区知春路 113 号银网中心 A 座 1207-1208 室（中发电子市场斜对面）
电话：(010)62536178 62536179 82628073
传真：(010)82614433

重庆周立功

地址：重庆市石桥铺科园一路二号大西洋国际大厦（赛格电子市场）1611 室
电话：(023)68796438 68796439
传真：(023)68796439

杭州周立功

地址：杭州市天目山路 217 号江南电子大厦 502 室
电话：(0571)28139611 28139612 28139613
28139615 28139616 28139618
传真：(0571)28139621

成都周立功

地址：成都市一环路南二段 1 号数码同人港 401 室（磨子桥立交西北角）
电话：(028) 85439836 85437446
传真：(028) 85437896

深圳周立功

地址：深圳市深南中路 2070 号电子科技大厦 A 座 24 楼 2403 室
电话：(0755)83781788（5 线）
传真：(0755)83793285

武汉周立功

地址：武汉市洪山区广埠屯珞瑜路 158 号 12128 室（华中电脑数码市场）
电话：(027)87168497 87168297 87168397
传真：(027)87163755

上海周立功

地址：上海市北京东路 668 号科技京城东座 7E 室
电话：(021)53083452 53083453 53083496
传真：(021)53083491

西安办事处

地址：西安市长安北路 54 号太平洋大厦 1201 室
电话：(029)87881296 83063000 87881295
传真：(029)87880865

目录

1. 概述

MIFARE Plus 在当前主流非接触式智能卡应用的基础上提供更高的安全性，并且可轻易升级现有卡片的安全级别。在升级到新的安全级别之前，MIFARE Plus 是唯一兼容 MIFARE 4K(MF1ICS70)，MIFARE 1K(MF1ICS50)和 MIFARE Mini(MF1ICS20)的主流智能卡。安全性升级后，MIFARE Plus 使用 AES（高级加密标准）进行认证，数据完整性和数据加密操作。MIFARE Plus 的空中接口和加密方式是基于安全级别最高的全球开放式标准，。

MIFARE Plus 有可用两个版本：MIFARE Plus S(MF1SPLUSx0y1)和 MIFARE Plus X(MF1PLUSx0y1，本文献中描述)。MIFARE Plus S 是 MIFARE Classic 系统直接向前兼容的标准版本。其配置可以提供更高的数据集成度。MIFARE Plus X 可以更灵活地优化指令流的速度和保密性。它提供丰富的特性，包括应对中断攻击的中继攻击检查。

2. 特性

- 2 或 4KB EEPROM；
- 简单的固定储存器结构，与 MIFARE Mini，MIFARE 1K，MIFARE 4K 兼容；
- 存储器结构与 MIFARE 4K 相同（扇区，块）；
- 可随意配置访问条件；
- 支持 ISO/IEC 14443-A 唯一序列号（4 或 7 字节），支持任意随机 ID；
- 多扇区认证，多块读和写；
- AES 用于认证、加密和验证数据完整性；
- 防撕裂保护；
- 密钥可存储为 MIFARE CRYPTO1 密钥（2×48 位/扇区）或 AES 密钥（2×128 位/扇区）；
- 完全虚拟卡概念；
- 中继攻击检查；
- 通信速率可达 848 Kbit/s；
- 单独写操作次数：通常为 200,000；
- 通过 CC EAL4＋。

3. 应用

- 公共传输；
- 访问管理；
- 电子收费系统；
- 停车场；
- 学校及校园卡；
- 员工卡；
- 网吧；

4. 功能描述

4.1 存储器结构

4KB EEPROM 存储器（MF1PLUS80）由 32 个扇区（每个扇区 4 个块），或 8 个扇区（每

个扇区 16 个块）组成。2KB EEPROM 存储器（MF1PLUS60）由 32 个扇区（4 个块）组成。每块包含 16 个字节。

扇区	块	块内的字节数 0	1	2	3	4	5 (1)	6	7	8	9	10	11	12	13	14	15	描述
39	15	CRYPTO1密钥A							访问字节			CRYPTO1密钥B或数据						扇区尾39
	14																	Data
	13																	Data
	...																	...
	...																	...
	2																	Data
	1																	Data
	0																	Data
	...																	...
	...																	...
	...																	...
32	15	CRYPTO1密钥A							访问字节			CRYPTO1密钥B或数据						扇区尾32
	14																	Data
	13																	Data
	...																	...
	...																	...
	2																	Data
	1																	Data
	0																	Data
31	3	CRYPTO1密钥A							访问字节			CRYPTO1密钥B或数据						扇区尾31
	2																	Data
	1																	Data
	0																	Data
	...																	...
	...																	...
	...																	...
0	3	CRYPTO1密钥A							访问字节			CRYPTO1密钥B或数据						扇区尾0
	2																	Data
	1																	Data
	0																	Manufacturer data

（1）CRYPTO1密钥A安全级别0，1，2
纯文本访问字节安全级别3（见图6）

图 1 存储器结构

4.1.1 厂商块

厂商块是第一个扇区（扇区 0）的第一个数据块（块 0）。它包含厂商的信息。由于安全性和系统要求，这一块由厂商对其编程后，就被写保护。

4.1.2 数据块

扇区 0 到 31 各包含 3 个块，扇区 32 到 39 各包含 15 个块，用于数据存储。

数据块可以被访问控制位配置为：

- 读/写块，用于存储二进制数据；
- 值块（如计数器，提供直接控制存储值的填充指令，如增值及减值指令）。

在执行任何数据操作前都必须先执行认证指令。

1. 访问条件

由 3 个位定义各数据块和扇区尾的访问条件，以取反和不取反格式存储在当前扇区的扇区尾。

访问控制位控制使用密钥 A 和 B 访问存储器的权限。假如知道相关密钥，且当前访问条件允许这样做，则可以改变访问条件。

注：各存储器访问条件的格式由内部逻辑确认。如果检测到格式不符，则整个扇区就被锁定。
注：下面叙述中，访问位是以不取反形式显示。

内部逻辑确保只在认证后执行指令。

表 1 扇区 0－31 的访问条件

访问控制位	有效指令	块	描述
$C1_3C2_3C3_3$	读，写	3	扇区尾
$C1_2C2_2C3_2$	读，写，增值，减值，传送，恢复	2	数据块
$C1_1C2_1C3_1$	读，写，增值，减值，传送，恢复	1	数据块
$C1_0C2_0C3_0$	读，写，增值，减值，传送，恢复	0	数据块

[1]扇区 0 的块 0 通常为只读。

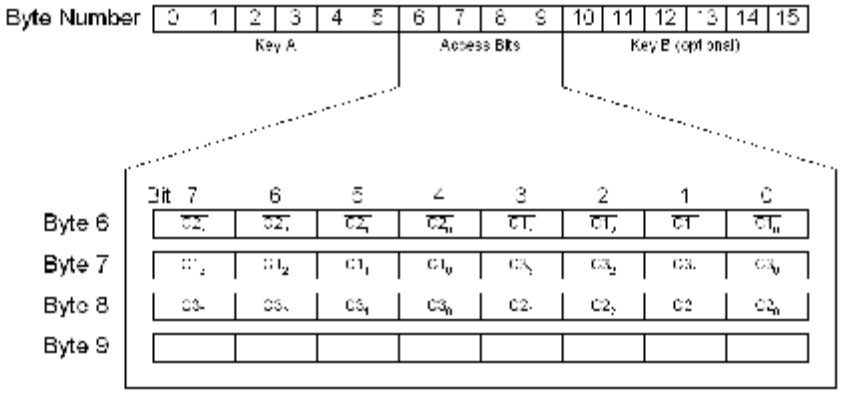

图 2 安全级别 1 和 2 的访问条件

2. 数据块的访问条件

根据数据块（块 0…2 或块 0…14，取决于扇区，见图 1）的访问控制位，可将读/写访问指定为“从不”，“密钥 A”，“密钥 B”或“密钥 A|B”（密钥 A 或密钥 B）。相关访问位的设置定义了应用及相应的可用指令。

- 读/写块：允许读、写操作；
- 值块：允许附加值操作，如增值，减值，传送及恢复。在一种情况下（“001”），只能对不可写的卡可进行只读及减值操作。另一种情况（“110”）下，使用密钥 B 可再写；
- 厂商块：不管怎样设置访问控制位，该块都是只读；
- 密钥管理：在传输配置中，密钥 A 必须用于认证。

表 2 数据块的访问条件

访问控制位			访问条件				应用
C1	C2	C3	读	写	增值	减值，传送，恢复	

续上表

访问控制位			访问条件				应用
0	0	0	密钥 A|B[1]	密钥 A|B[1]	密钥 A|B[1]	密钥 A|B[1]	传送配置
0	1	0	密钥 A|B[1]	从不	从不	从不	读/写块
1	0	0	密钥 A|B[1]	密钥 B[1]	从不	从不	读/写块
1	1	0	密钥 A|B[1]	密钥 B[1]	密钥 B[1]	密钥 A|B[1]	值块
0	0	1	密钥 A|B[1]	从不	从不	密钥 A|B[1]	值块
0	1	1	密钥 B[1]	密钥 B[1]	从不	从不	读/写块
1	0	1	密钥 B[1]	从不	从不	从不	读/写块
1	1	1	从不	从不	从不	从不	读/写块

[1]如果在相应扇区尾可读密钥 B，则它不能用于认证（表中灰色区域）。总结：如果读写器试图在灰色区域标注的条件下，使用密钥 B 对扇区的任一块进行认证，则在认证后，卡将拒绝后面所有的存储器访问。

3. 值块

值块可实现计数功能（如电子钱包，有效指令：读，写，增值，减值，恢复，转移）。值块有固定的数据格式，可以进行差错检测、纠错和备份管理。值块必须符合下列格式才能执行相应的值操作：

- 值：表示一个有符号的 4 字节值。其中值的最低有效字节存储在最低地址字节内。取反的字节以标准 2 的补码格式保存。为了保证数据的完整性和安全性，值要保存 3 次，其中 2 次不取反，1 次取反；
- 地址（Adr）：表示一个 1 字节地址，可用于保存一个块的存储地址。地址字节要保存 4 次，其中 2 次取反，2 次不取反。在增值，减值，恢复操作期间，地址（块地址）保持不变。如果指令在执行增值/减值/恢复的另一个块完成，则传送指令内的地址字节可变。

在实际使用中，一般将值存储在 2 个块中。在增值/减值之前，先校验块的一致性。如果其中一个被破坏，则需要通过另一个块的值对其进行更新。如果值不同，则可决定应向 2 个块中写入更高或更低值。按下列步骤进行：

- 根据图 3 所描述格式将值保存到 2 个块中（块 A 和块 B）；
- 对块 A 增值/减值；
- 将值操作的结果保存到块 B；
- 将值从块 B 复制到块 A。

为了保证性能，安全级别 3 也将增值/减值操作与恢复/转移操作结合，见 9.7.5 节。

字节数描述	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	值				值				值				地址	$\overline{\text{地址}}$	地址	$\overline{\text{地址}}$

图 3 值块

4.1.3 扇区尾

每个扇区的最后一个块称为扇区尾。这个扇区尾位于 NV－存储器的起始 2KB（扇区 0 到扇区 31）中各扇区的块 3，在 4KB NV－存储器的上行 2KB（扇区 31 到扇区 39）中各扇区的块 15。

图 4 扇区尾

各扇区尾包括：

- 密钥 A 和 B（可选，也可以是数据）；
- 扇区的 4/ 16 个块的访问条件存储在 6…9 字节，即访问控制位。访问控制位还指定了数据块的类型（读/写或值）；
- 安全级别 3 中，字节 5 为.通信模式（明文/密文）配置字节。升级到安全级别 3 后，若修改了扇区尾的通信模式配置字节，则通信模式为该字节设定的模式，否则通信模式为 MFP 配置块设定的模式。该配置字节的值默认设置为 0Fh（所有块均明文通信，见 10.11 节），可以在安全级别 0 时更改。

在安全级别 3 时使用防撕裂机制确保安全更新扇区尾。

1. 扇区尾的访问条件

根据扇区尾（块 3 或块 15，取决于扇区，见图 1），可以将对密钥及访问控制位的读/写操作设定为“从不”，“密钥 A”，“密钥 B”或“密钥 A|B”（密钥 A 或密钥 B）。

卡片出厂时的访问条件为传输配置。该配置中密钥 B 是可读的，不能作为密钥使用，因此必须使用密钥 A 认证新卡。由于访问控制位可能被阻塞，因此在个人化卡时必须特别注意。

表 3 扇区尾的访问条件

访问控制位			访问条件						注
			密钥 A		访问控制位		密钥 B		
C1	C2	C3	读	写	读	写	读	写	
0	0	0	从不	密钥 A	密钥 A	从不	密钥 A	密钥 A	密钥 B 可读
0	1	0	从不	从不	密钥 A	从不	密钥 A	从不	密钥 B 可读
1	0	0	从不	密钥 B	密钥 A|B	从不	从不	密钥 B	
1	1	0	从不	从不	密钥 A|B	从不	从不	从不	
0	0	1	从不	密钥 A	密钥 A	密钥 A	密钥 A	密钥 A	密钥 B 可读，传送配置
0	1	1	从不	密钥 B	密钥 A|B	密钥 B	从不	密钥 B	
1	0	1	从不	从不	密钥 A|B	密钥 B	从不	从不	
1	1	1	从不	从不	密钥 A|B	从不	从不	从不	

注：灰色区域为可读密钥 B 的访问条件，其中密钥 B 可用于数据。

4.1.4 AES 密钥

AES 密钥不显示在存储器结构当中。该密钥存储在其它数据顶端，可以被更新及引用，因此称为 KEY No（见**错误！未找到引用源。**）。在安全级别 3，支持防撕裂机制以更新 AES 密钥，及更新扇区尾。在安全级别 2，只有更新 AES 密钥才支持防撕裂机制。这种在线防撕裂机制是由 PICC 自身完成的。即使在写操作期间卡片离开 RF 场区，EEPROM 仍保持确定的状态。

4.1.5 中继攻击检查

安全级别 3 通过精确测量请求响应交互作用时间，提供了检测中继攻击方法。详细描述见 9.7.6 节。

4.1.6 多扇区认证

在安全级别 2 和 3，可使用多扇区认证优化性能并减少认证次数。判定是否使用多扇区认证的操作如下：

1.使用密钥 M 对卡的 X 扇区进行认证。

2.读写器试图对另一个需要使用密钥 N 访问的扇区 Y 进行写/读/执行值操作。

3.如果密钥 M 与密钥 N 的值及类型（A 或 B）都相同，则不需要重新认证 Y 扇区。读写器可立即从扇区 Y 读/写数据或执行值操作。

PICC 将密钥 M 作为认证密钥，而不是将密钥 N 作为认证密钥。这样就可以在不认证密钥 N 的情况下改变密钥 N。在修改密钥 N 之后，若不使用新的密钥 N 重新认证，则不能访问该扇区。

在多扇区认证情况下，只需要密钥值和类型匹配，不要求操作扇区的次序，一个接一个地对扇区进行操作即可。

在安全级别 3，可将卡配置为只需认证一次便可访问有扇区。这也适用于安全级别 2 认证（一种是基于 AES，一种是基于 CRYPTO1）。

4.1.7 独创功能

用独创密钥做 AES 认证（如 9.7.2.1 节和 9.7.2.2 节所述）（见 10.7 节）以使能独创功能。认证应该在 ISO 14443-4 协议层执行（见 9.2.2 节）。

4.2 卡激活及通信协议

ISO/IEC 14443-3A 防冲突机制允许同时处理区域内的多张卡。防冲突算法逐次选择卡片，并确保正确执行所选择的卡片操作，避免受区域内其它卡片影响而造成数据损坏。

有三个不同版本的 PICC。前两个有编程到 NV 存储器锁定部分的 UID，这部分为厂商保留：

- 全球唯一的 7 字节序列号；
- 全球唯一的 4 字节序列号。

由于安全性和系统要求，这些字节在出厂时由 PICC 厂商编程后就被写保护了。

第三种有伪唯一 ID，符合 ISO/IEC 14443-3，使用 0xFX ID 范围。

客户订购产品时必须确定要使用的 UID 长度，订购信息参见**错误！未找到引用源。**。

4.2.1 向后兼容协议

该产品向后兼容，用于安全级别 1 和安全级别 2，必须运行在与 MIFARE 1K，4K 及

Mini 相同的协议层。协议由下列成分组成：

- 帧定义：

  根据 ISO/IEC 14443-3；

- 位编码：

  根据 ISO/IEC 14443-2；

- 错误代码处理：

  处理错误代码是半字节形式。使用的错误代码（NACK－未确认）如 10.8 节所述。

- 指令规范：

  指令是私有指令。请使用参考文献[1]，参考文献[2]，参考文献[3]中的规范及附加指令，附加指令只在 MIFARE Plus 中执行，如本数据手册所述。

- 以下安全级别可适用该协议：

  - 安全级别 0；
  - 安全级别 1；
  - 安全级别 2。

4.2.2 ISO/IEC 14443-4 协议

ISO/IEC 14443-4 协议（也称为 T＝CL）用于许多处理器卡中。对于 MIFARE Plus，该协议用于下列安全级别：

- 安全级别 0；
- 安全级别 1－只用于安全级别切换和独创校验；
- 安全级别 2－只用于更新 AES 密钥和配置块，以及安全级别切换和独创校验；
- 安全级别 3

  在个人化期间内，可将在安全级别 3 时卡片配置为支持随机 ID。用户可决定使用随机 ID 还是固定 UID，并在区域结构块中配置（见 10.9 节）。根据 ISO/IEC 14443-3，如果使用随机 ID，则第一个反冲突循环（见 MIFARE 应用笔记 ISO/IEC 14443 PICC 选择）将返回随机号标记 0x08，3 字节随机编号和 BC。

  这种情况下，可使用 VC Support Last 指令获取实际 UID（如 9.7.7 节所述），或通过读出块 0 恢复实际 UID。

4.3 安全级别转换

产品有 4 个安全级别：

- 安全级别 0：

  初始配置；

- 安全级别 1：

  功能向后兼容模式（与 MIFARE 1K/4K/Mini），带有可选 AES 认证；

- 安全级别 2：

  基于 AES 的 3 重认证，随后是 MIFARE CRYPTO1 认证，MIFARE CRYPTO1 保证通信安全；

- 安全级别 3：

  基于 AES 的 3 重认证，使用 AES，通过数据加密和指令加 MAC 方法确保操作指令安全。

如果是“L3”卡，则 Commit Perso 将直接把卡升级到安全级别 3，而不是安全级别 1。对于“L3 卡”，只需要写卡配置密钥及卡主控密钥。要直接进入新的安全级别，还需要复位

及再次激活卡。

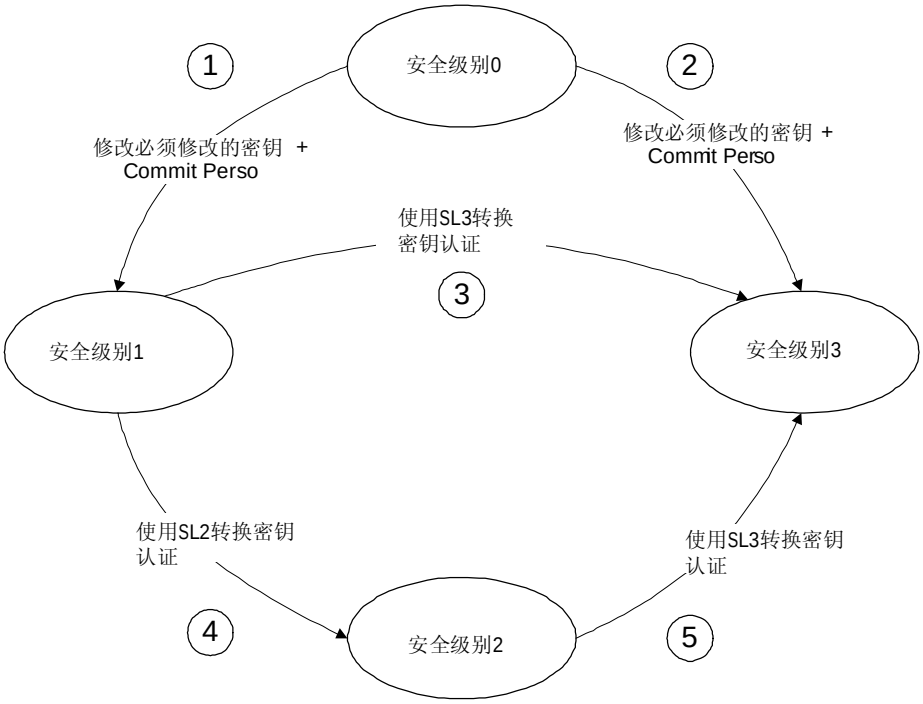

图 5 安全级别转换

图 5 所示为 MF1PLUSx0y1 的安全级别转换。产品出厂时为安全级别 0。根据指令代码不同，选择的产品可能为“L1 卡”或“L3 卡”：

1.如果是“L1 卡”，则 PICC 在修改所有必须修改的密钥，且成功执行 Commit Perso 后，转换到安全级别 1。

2. 如果是“L3 卡”，则 PICC 在修改所有必须修改的密钥，且成功执行 Commit Perso 后，转换到安全级别 3。

3.使用 L3 转换密钥认证后，处于安全级别 1 的“L1 卡”可转换到安全级别 3。

4.使用 L2 转换密钥认证后，处于安全级别 1 的“L1 卡”可转换到安全级别 2。

5.使用 L3 转换密钥认证后，处于安全级别 2 的“L1 卡”可转换到安全级别 3。

附录A 修订历史

版本号	日期	描述
Rev.3.0	2009/7/22	