目 录

第1章 读卡模块编程手册

1.1 通信协议数据帧结构

读卡模块与控制器的通信采用数据帧方式。

数据帧格式分为两种：控制器（主机）数据帧，模块（从机）应答数据帧。

● **控制器发送命令数据帧结构**

帧头			数据区	校验值
LEN	ID	FC	DATA	CHECK
数据长度	模块地址	命令代码	命令后的数据	校验字（累加和取反）
0-32	1-256	0x11-0xFF	0xXX ……	累加和取反

● **模块返回数据帧结构**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK
数据长度	模块地址	命令代码	返回操作状态	模块返回的数据	校验字（累加和取反）
0-32	1-256	0x11-0xFF	0x00	0xXX ……	累加和取反

注意：DesFire 卡读卡模块操作错误时数据区会返回 CPU 卡内部的操作状态，操作状态为一字节数据，例如：0xAE 表示密钥验证失败，权限不足。

● **帧数据含义**

LEN 整个数据帧的长度，包含 LEN 本身及帧最后的校验值

ID 读卡模块的地址，485 通信会校验此地址，地址错误模块不响应命令

FC 命令代码，具体含义参考命令列表

DATA 命令代码的参数 或者是读卡模块返回的数据，数据发送顺序为低字节先发

CHECK 除了 CHECK 以外的所有数据累加和取反后取最低字节

SW 模块执行命令后返回的操作状态 0x00-操作成功 其他值为错误代码

● **数据帧实例**

例：（Mifare 卡读卡模块）读卡片第 0 块数据发送的命令：

第 1 步：查看读数据的命令说明，确认需要输入参数：数据块和密钥值

第 2 步：确认数据区数据长度，数据块参数长 1 字节 密钥值参数长 6 字节

第 3 步：计算数据帧长度 LEN 本身 1 字节+模块地址 1 字节+命令代码 1 字节+数据块参数 1 字节+密钥值参数 6 字节+校验码 1 字节，因此 LEN=11 字节=0x0B

组合后的数据值为：0b 01 21 00 ff ff ff ff ff ff

第 4 部：计算校验值，校验值=校验值前面的所有数据依次累加后取最低字节的值再取反。

累加和 = 0b+01+21+00+ff+ff+ff+ff+ff+ff = 0x0627

最低字节值 = 0x27 校验值 = 0x27 取反 = 0xd8

● **数据发送方式**

数据发送方式全部采用先发低字节后发高字节的顺序。例如：卡片 UID=0x11223344，模块读到卡片的 UID 返回 UID 数据时发送数据顺序为 0x44，0x33，0x22，0x11。

1.2 命令列表

命令字节长度为 1 字节，高半字节表示命令类型，低半字节表示命令编号。

命令字	命令类型	命令含义	备注
0x11	保留		
0x12	保留		

0x13	保留	设置波特率（不支持）波特率固定 19200	0=9600，1=19200，2=28880，3=38400，4=57600
0x14	通用命令	控制 LED 闪烁	通过 INT 引脚可以输出控制信号
0x15	通用命令	读取模块信息	返回模块版本 ASCII 码信息
0x16	通用命令	A 型卡激活	此命令可以读取 A 型卡卡号-
0x17	通用命令-RC523	B 型卡激活	此命令可以读取 B 型卡卡号（**仅 CUT-200 系列读卡模块支持**）
0x18	通用命令	激活卡片到 ISO1443-4	后续可以进行 APDU 命令操作
0x19	通用命令	CPU 卡数据透传 APDU	数据透传命令，支持自定义开发 CPU 卡
命令字	**命令类型**	**命令含义**	**备注**
0xB0	DesFire EV1 操作命令	格式化卡片	通过验证根密钥重建卡片文件结构
0xB1	DesFire EV1 操作命令	写数据（高级命令）	验证对应的密钥读取应用文件数据
0xB2	DesFire EV1 操作命令	读数据（高级命令）	验证对应的密钥改写应用文件数据
0xB3	DesFire EV1 操作命令	更改密钥	更改控制密钥的值
0xB4	DesFire EV1 操作命令	增加应用	验证根目录主控密钥后增加一个新应用目录，且在目录中创建一个数据文件
0xB5	DesFire EV1 操作命令	写应用目录下的文件数据	发送此命令即可写数据
0xB6	DesFire EV1 操作命令	读应用目录下的文件数据	发送此命令即可读数据
0xB7	DesFire EV1 操作命令	修改指定应用目录下指定密钥 ID 的密钥值	发送此命令即可修改指定应用目录指定密钥 ID 的密钥值
0xB8	DesFire EV1 操作命令	获取卡片应用目录信息	获取卡片内部所有应用目录的数量和应用目录 ID 的信息
0xB9	DesFire EV1 操作命令	选择应用目录	单步指令-选择应用目录
0xBA	DesFire EV1 操作命令	验证密钥	单步指令-密钥验证
0xBB	DesFire EV1 操作命令	读数据（基本命令）	单步指令-读指定的文件数据
0xBC	DesFire EV1 操作命令	写数据（基本命令）	单步指令-写指定的文件数据
……			

注意：B4-BC 为扩展命令，基本操作 B0-B3 即可满足使用要求

1.3 模块返回状态码定义

0x00 // 命令执行成功
0x01 // RS485 地址错误
0x02 // 命令参数错误
0x03 // 激活卡片失败或者没有卡片存在
0x04 // Mifare 卡验证密码失败
0x05 // Mifare 卡读数据失败
0x06 // Mifare 卡写数据失败
0x07 // CPU 卡执行 RATS 失败
0x08 // 读取 CPU 卡文件失败
0x09 // 写 CPU 卡文件失败
0x0A // 初始化 CPU 卡文件系统失败

0x0B // 卡片回收失败
0x0C // 修改密钥失败
0xFE // CPU 卡操作失败
0xFF // 不支持的命令

1.4 CPU卡错误代码

0x00 // 成功的操作
0x0C // 备份文件不改变，不需要 CommitTransaction 和 AbortTransaction
0x0E // 完成命令所需的 NV 存储器不足
0x1C // 不支持的命令代码
0x1E // CRC 或 MAC 与数据不匹配，填充字节无效
0x40 // 指定的密钥无效
0x7E // 命令串长度无效
0x9D // 当前的配置/状态拒绝执行所请求的命令
0x9E // 参数值无效
0xA0 // 请求的 AID 不存在
0xA1 // 应用中不可恢复的错误，应用将被禁止*
0xAE // 当前验证状态不允许执行请求的命令。
0xAF // 期待发送额外的数据帧。
0xBE // 试图读取/写入的数据超出文件/记录的边界。
0xC1 // PICC 内不可恢复的错误，PICC 将被禁止。
0xCD // PICC 因为一个不可恢复的错误而被禁止。
0xCE // 的数目限制为 28，CreateApplication 不再可用
0xDE // 因为已经存在相同编号的文件/应用，因此文件/应用的创建失败。
0xEE // 电源故障而无法完成 NV 写操作，启动内部备份/恢复机制。
0xF0 // 指定的文件名不存在。
0xF1 // 文件中不可恢复的错误，文件将被禁止。

1.5 命令响应时间

UART 接口

测试条件：波特率 19200 UART 接口 电源电压 5V
测试卡片：NXP DesFire EV1 D21 卡片
初始化=796ms
写数据=109ms
读数据=109ms
修改密钥=156ms

1.6 命令详解

1.6.1 0x14 INT脚LED灯控制信号

● 主机发送

帧头			数据区	校验值
LEN	ID	FC	DATA	CHECK
数据长度	模块地址	命令代码	命令参数	校验字（累加和取反）
0x07	0x01	0x14	0x02 0x14 0x14	0XB9

命令功能：控制 LED 闪烁（也可以控制蜂鸣器或者作为其他驱动信号来使用）
参数说明：[0] 闪烁的次数 亮灭的交替次数
[1] 亮的时间 10ms 为基准单位 例如 0x14 = 20*10ms 亮 200ms
[2] 灭的时间 10ms 为基准单位 例如 0x14 = 20*10ms 灭 200ms
注意：亮的时间和灭的时间值 加起来不能大于 250
数据说明：亮 80ms，灭 20ms 交替闪烁 2 次

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK
数据长度	模块地址	命令代码	返回操作状态	无	校验字（累加和取反）
0x05	0x01	0x14	0x00	无	0xE5

参数说明：返回操作成功状态字 0x00，非 0 值为错误代码

● **通信实例**

主机发送：07 01 14 02 14 14 B9 // 控制 LED 闪烁 2 次 亮 200ms 灭 200ms
模块返回：05 01 14 00 E5 // 命令执行成功

1.6.2 0x15 读取模块信息

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	CHECK
数据长度	模块地址	命令代码	无	校验字（累加和取反）
0x04	0x01	0x15	-	0xE5

命令功能：读取模块的型号、版本等信息
参数说明：无

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK
数据长度	模块地址	命令代码	返回操作状态	模块返回的数据	校验字（累加和取反）
0xXX	0x01	0x15	0x00	0xXX……	0xXX

参数说明：[0] 命令执行成功的状态码 0x00
[1-n] 后续 n 个数据为模块信息 数据位 ASCII 码

● **通信实例**

主机发送：04 01 15 E5 // 读取模块型号、版本号等信息
模块返回：21 01 15 00 43 55 54 31 30 30 2D 50 42 4F 43 20 56 31 2E 30 20 32 30 31 33 2D 30 35 2D 33 30 17 // 返回模块信息转换成 ASCII 码 = CUT100-PBOC V1.0 2013-05-30

1.6.3 0x16 A型卡激活

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	CHECK
数据长度	模块地址	命令代码	无	校验字（累加和取反）
0x04	0x01	0x16	-	0xE4

命令功能：激活 A 型卡，返回卡片 UID

参数说明：无参数

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK
数据长度	模块地址	命令代码	返回操作状态	UID	校验字（累加和取反）
0xXX	0x01	0x16	0x00	卡号数据	0xXX

参数说明：返回操作成功状态字 0x00，非 0 值为错误代码
数据区返回卡片的 UID 数据

● **通信实例**

主机发送：04 01 16 E4 // 激活 A 型卡片
模块返回：09 01 16 00 **F6 65 34 49** 07 // 激活成功，返回卡片 UID **F6 65 34 49**
// UID 为小端模式 16 进制应为 **0x493465F6**

1.6.4 0xB0 格式化卡片

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	CHECK
数据长度	模块地址	命令代码	旧根密钥 新根密钥	校验字（累加和取反）
0x24	0x01	0xB0	00……00 FF……FF	0x3A

命令功能：验证卡片原根密钥后格式化卡片，重新创建文件结构，并将根密钥修改成用户指定的密钥值。
参数说明：低位 16 字节为旧根密钥（空白卡默认为 00）高位 16 字节为用户指定新根密钥

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK
数据长度	模块地址	命令代码	返回操作状态	CPU 卡操作结果	校验字（累加和取反）
0x05	0x01	0xB0	0x00	0x00	0x49

参数说明：返回操作成功状态字 0x00，非 0 值为错误代码

● **通信实例**

主机发送：24 01 B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF 3A // 验证跟密钥格式化卡片
模块返回：05 01 B0 00 49 // 操作成功
06 01 B0 0A AE 90 // 0A 格式化失败 AE 密钥错误

1.6.5 0xB1 写应用文件数据

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	CHECK
数据长度	模块地址	命令代码	文件 ID1 字节 地址偏移 密钥 16 字节 数据 32 字节	校验字（累加和取反）
0xXX	0x01	0xB1	01 00 00……00 AA……AA	0xXX

命令功能：对指定文件写入数据 数据长度固定 32 字节（1 块）
参数说明：01 文件 ID 00 块地址密钥值需要与制定文件的读写密钥相对应

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK
数据长度	模块地址	命令代码	返回操作状态	无	校验字（累加和取反）
0x05	0x01	0xB1	0x00	-	0x69
参数说明：00 CPU 卡操作成功 其他值操作失败 并且后面会跟随 1 字节 CPU 卡错误代码					

● **通信实例**

主机发送：36 01 B1 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 AA AA AA AA
AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA
AA AA AA AA AA AA AA D6 // 写 01 号数据文件
模块返回：05 01 B1 00 48 // 写数据成功

1.6.6 0xB2 读指定文件数据

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	CHECK
数据长度	模块地址	命令代码	文件 ID1 字节 块地址 密钥 16 字节	校验字（累加和取反）
0x16	0x01	0xB2	01 00 00……00	0x35
命令功能：读数据文件 读取长度固定 32 字节（1 块） **参数说明**：01 文件 ID 00 块地址 密钥值需要与制定文件的读写密钥相对应				

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK
数据长度	模块地址	命令代码	返回操作状态	卡片数据	校验字（累加和取反）
0xXX	0x01	0xB2	0x00	0xXX……	0xXX
参数说明：00 CPU 卡操作成功 其他值操作失败 并且后面会跟随 1 字节 CPU 卡错误代码					

● **通信实例**

主机发送：16 01 B2 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 35
// 读 01 文件数据 密钥 16 字节 00
模块返回：25 01 B2 00 AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA
AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA E7
// 读数据成功 数据为 16 字节 AA

1.6.7 0xB3 修改应用目录指定编号的密钥值

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	CHECK
数据长度	模块地址	命令代码	密钥编号 旧密钥 新密钥	校验字（累加和取反）
0x25	0x01	0xB3	01 00……00 FF……FF	0x35
命令功能：对应用目录下指定编号的密钥验证旧密钥后将旧密钥的更改为新密钥				

参数说明：

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK
数据长度	模块地址	命令代码	返回操作状态	无	校验字（累加和取反）
0x05	0x01	0xB3	0x00	-	0x46

参数说明： 00 CPU 卡操作成功
其他值操作失败 并且后面会跟随 1 字节 CPU 卡错误代码

通信实例

主机发送：25 01 B3 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff 35 // 修改密钥

模块返回：05 01 B3 00 46 // 修改密钥成功

1.6.8 0xB4 增加应用

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	CHECK
数据长度	模块地址	命令代码	主控密钥 应用目录 文件大小	校验字（累加和取反）
0x18	0x01	0xB4	00……00 F1 AD 00 04	0x8C

命令功能： 验证主控密钥后增加一个应用目录，应用目录中增加一个文件 ID 为 0x01 的二进制数据文件，文件大小自定义，读密钥 ID=0x01 写密钥 ID=0x02

参数说明：

DATA[00-15]:16 字节主控密钥

DATA[16-17]:2 字节应用目录 ID，低字节在前，例如：FA AD 表示应用目录 0xADF1

DATA[18-19]:2 字节文件大小，低字节在前，例如：00 04 表示文件大小 0x0400=1024 字节

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK
数据长度	模块地址	命令代码	返回操作状态	无	校验字（累加和取反）
0x05	0x01	0xB4	0x00	-	0x45

参数说明： 00 CPU 卡操作成功
其他值操作失败 并且后面会跟随 1 字节 CPU 卡错误代码

通信实例

主机发送：18 01 B4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F1 AD 00 04 90

模块返回：05 01 B4 00 45

1.6.9 0xB5 写应用目录下的文件数据

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	CHECK
数据长度	模块地址	命令代码	应用 ID 文件 ID 密钥编号 密钥偏移地址 写数据长度 数据	校验字（累加和取反）
0x2A	0x01	0xB5	F1 AD 01 02 00……00 00 10	0xCB

			11 22 ……FF AA	

命令功能：写应用目录下的文件数据

参数说明：

DATA[00-01]:应用目录 ID 低字节在前

DATA[02-02]:文件 ID

DATA[03-03]:写文件密钥 ID

DATA[04-19]:密钥值

DATA[20-21]:偏移地址 低字节在前

DATA[22-22]:写数据长度

DATA[23-38]:16 字节待写入数据

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK
数据长度	模块地址	命令代码	返回操作状态	无	模块地址
0x05	0x01	0xB5	0x00	-	0x44

参数说明：00 CPU 卡操作成功

其他值操作失败 并且后面会跟随 1 字节 CPU 卡错误代码

● **通信实例**

主机发送：2B 01 B5 F1 AD 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF AA CB

模块返回：05 01 B5 00 44

1.6.10 0xB6 读应用目录下的文件数据

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	应用 ID 文件 ID 密钥编号 密钥 偏移地址 读数据长度	校验字（累加和取反）
0x1B	0x01	0xB6	F1 AD 01 01 00……00 00 10	0x7D

命令功能：读应用目录下的文件数据

参数说明：

DATA[00-01]:应用目录 ID 低字节在前

DATA[02-02]:文件 ID

DATA[03-03]:读文件密钥 ID

DATA[04-19]:密钥值

DATA[20-21]:偏移地址 低字节在前

DATA[22-22]:读数据长度

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK
数据长度	模块地址	命令代码	返回操作状态	数据	模块地址
0xXX	0x01	0xB6	0x00	0xXX….0xXX	0xXX

参数说明：

SW：00 CPU 卡操作成功，其他值操作失败 并且后面跟随 1 字节 CPU 卡错误代码
DATA[00-XX]:返回的卡片数据

● **通信实例**

主机发送：1B 01 B6 F1 AD 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 7D
模块返回：15 01 B6 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF AA 91

1.6.11 0xB7 修改指定目录下指定密钥编号的密钥值

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	应用目录 密钥 ID 旧密钥 新密钥	校验字（累加和取反）
0x27	0x01	0xB7	F1 AD 01 00……00 FF……FF	0x91

命令功能：修改指定目录下指定密钥编号的密钥值

参数说明：

DATA[00-01]:应用目录 ID 低字节在前
DATA[02-02]:密钥 ID
DATA[03-18]:旧密钥
DATA[19-34]:新密钥

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK
数据长度	模块地址	命令代码	返回操作状态	无	模块地址
0x05	0x01	0xB7	0x00	-	0x42

参数说明：

SW：00 CPU 卡操作成功，其他值操作失败 并且后面跟随 1 字节 CPU 卡错误代码

● **通信实例**

主机发送：27 01 B7 F1 AD 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 91
模块返回：05 01 B7 00 42

1.6.12 0xB8 获取卡片内所有应用目录的数量和应用目录ID

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	验证方式 主控密钥	校验字（累加和取反）
0x15	0x01	0xB8	01 00……00	0x30

命令功能：获取卡片内所有应用目录的数量和应用目录 ID

参数说明：

DATA[00-00]:获取应用目录时的验证方式 00=不验证主控密钥 01=验证主控密钥
DATA[01-16]:主控密钥值

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK

数据长度	模块地址	命令代码	返回操作状态	应用数量 应用目录 ID 数据	模块地址
0x0C	0x01	0xB8	0x00	02 00 10 01 00 AD F1	0x89

参数说明：

SW：00 CPU 卡操作成功，其他值操作失败 并且后面跟随 1 字节 CPU 卡错误代码

DATA[00-00]:应用目录数量

DATA[01-XX]:应用目录 ID 数据，低字节在前

注意：Desfire 卡中的目录 ID 长度为 3 字节，因此每 3 个字节的数据为一个应用目录 ID

● **通信实例**

主机发送：15 01 B8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30

模块返回：0C 01 B8 00 02 01 10 00 F1 AD 00 89 有 2 个应用目录 0x001001 和 0x00ADF1

1.6.13 0xB9 选择应用目录

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	应用目录 ID	校验字（累加和取反）
0x07	0x01	0xB9	F1 AD 00	0xA0

命令功能：根据应用目录 ID 选择应用目录

参数说明：

DATA[00-02]:应用目录 ID，长度 3 字节，低字节在前

注意：此命令为单步操作，使用此命令前先发送 04 01 18 E2 命令激活卡片才能正常操作

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK
数据长度	模块地址	命令代码	返回操作状态	无	模块地址
0x05	0x01	0xB9	0x00	-	0x40

参数说明：

SW：00 CPU 卡操作成功，其他值操作失败 并且后面跟随 1 字节 CPU 卡错误代码

● **通信实例**

主机发送：07 01 B9 F1 AD 00 A0

模块返回：05 01 B9 00 40

1.6.14 0xBA 密钥验证

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	密钥 ID 密钥值	校验字（累加和取反）
0x15	0x01	0xBA	01 00……00	0x2E

命令功能：验证指定编号的密钥

参数说明：

DATA[00-00]:密钥 ID

DATA[01-06]:密钥值

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK
数据长度	模块地址	命令代码	返回操作状态	无	模块地址
0x05	0x01	0xBA	0x00	-	0x3F

参数说明：

SW：00 CPU 卡操作成功，其他值操作失败 并且后面跟随 1 字节 CPU 卡错误代码

● **通信实例**

主机发送：15 01 BA 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2E

模块返回：05 01 BA 00 3F

1.6.15 0xBB 写数据文件

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	文件 ID 偏移地址 写长度 数据	校验字（累加和取反）
0x18	0x01	0xBB	01 00 00 10 11……FF AA	0x78

命令功能：写指定文件 ID 的数据文件

参数说明：

DATA[00-00]:文件 ID

DATA[01-02]:偏移地址，低字节在前

DATA[03-03]:写数据长度（0-128 字节）

DATA[04-19]:待写入数据

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK
数据长度	模块地址	命令代码	返回操作状态	无	模块地址
0x05	0x01	0xBB	0x00	-	0x3E

参数说明：

SW：00 CPU 卡操作成功，其他值操作失败 并且后面跟随 1 字节 CPU 卡错误代码

● **通信实例**

主机发送：18 01 BB 01 00 00 10 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF AA 78

模块返回：05 01 BB 00 3E

1.6.16 0xBC 读数据文件

● **主机发送**

帧头			数据区	校验值
LEN	ID	FC	DATA	BCC
数据长度	模块地址	命令代码	文件 ID 偏移地址 写长度	校验字（累加和取反）
0x08	0x01	0xBC	01 00 00 10	0x29

命令功能：读指定文件 ID 的数据文件

参数说明：

DATA[00-00]:文件 ID
DATA[01-02]:偏移地址，低字节在前
DATA[03-03]:读数据长度（0-128 字节）

● **模块返回**

帧头			返回状态	数据区	校验值
LEN	ID	FC	SW	DATA	CHECK
数据长度	模块地址	命令代码	返回操作状态	数据	模块地址
0xXX	0x01	0xBC	0x00	0xXX……0xXX	0xXX

参数说明：
SW：00 CPU 卡操作成功，其他值操作失败 并且后面跟随 1 字节 CPU 卡错误代码

● **通信实例**
主机发送：08 01 BC 01 00 00 10 29
模块返回：15 01 BC 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF AA 8B

1.6.17 单步操作命令使用注意事项

- B9、BA、BB、BC 四个命令为 Desfire 卡的单步操作命令，方便用户操作一些自定义目录的卡片使用
- 使用这些命令前必须要先发送《04 01 18 E2》命令，将卡片激活到 ISO14443-4，然后才能发送 B9、BA、BB、BC 命令中的任何一个，在卡片没有拿离天线之前可以连续多次发送 B9、BA、BB、BC 命令中的任何一个而不需要重新发送《04 01 18 E2》这条命令。
- 卡片离开天线后再次重新放到天线区域时，需要重发《04 01 18 E2》激活命令后才能发送 B9、BA、BB、BC 命令中的任何一个。

1.7 DesFire EV1 卡读卡模块文件访问密钥定义

密钥编号	密钥用途	备注
0x01	文件 1 读密钥	应用目录下的应用密钥
0x02	文件 1 读写密钥	
0x03	文件 2 读密钥	
0x04	文件 2 读写密钥	
0x05	文件 3 读密钥	
0x06	文件 3 读写密钥	
0x07	文件 4 读密钥	
0x08	文件 4 读写密钥	