MH1721

国密产品 COS 指令手册

MEGAHUNT

北京兆讯恒达技术有限公司

修订记录

日期	修订版本	描述	作者
2021-12-22	1.00	初稿完成	MEGAHUNT

目录

1 概述

国密产品方案采用 32 位高性能安全 CPU，支持密钥存储及加解密功能。通过 UART/SPI/I2C 对外提供密钥读写、安全算法等接口，可作为国密认证安全模块。

1.1 芯片安全组件

- 高速硬件非对称算法引擎,支持 RSA512~RSA2048、ECC、SM2 算法运算
- DES/AES 算法单元
- SM3/SM4/SM7/SM9 国密算法单元
- SHA 算法单元:支持 SHA1/SHA224/SHA256/SHA384/SHA512;
- 真随机数发生器
- CRC 校验单元
- 安全检测与防护单元
- 存储器加密机制
- 唯一芯片序列号：每颗芯片都具有 128bit 唯一序列号

1.2 主要特性

- 外围器件少，节省 PCBA 空间和生产费用
- 电压范围广，支持 2.0V~5.5V
- 通信方式多，支持串口、SPI 、预留 USB、I2C
- SPI 接口速率最高支持 8Mbps，串口默认为 115200

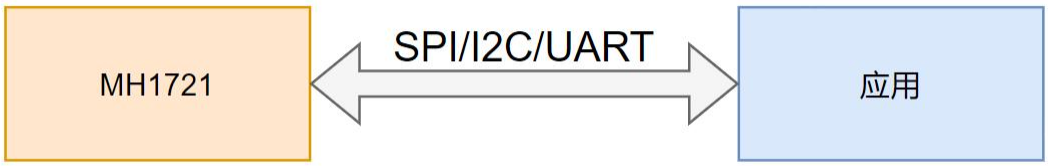
1.3 证书

国密证书二级

2　技术实现方案

2.1 系统框图

系统框图如下所示：



国 2-1

2.2 硬件连接

2.2.1　SOP8

2.2.1.1 引脚定义和解释

引脚	定义	备注
VCC	供电电源	电压范围：2.0V-5.5V
GND	地	
GPIO0	串口RX	MH17xx 串口接收
GPIO1	串口 TX	MH17xx 串口发送
GPIO4	SPI CLK	MH17xx 做从机，由AP提供时钟
GPIO5	SPI CS	
GPIO6	SPI MOSI	MH17xx 做从机，对MH71xx是输入
GPIO7	SPI MISO	MH17xx 做从机，对MH71xx是输出

2.2.1.2　硬件参考图

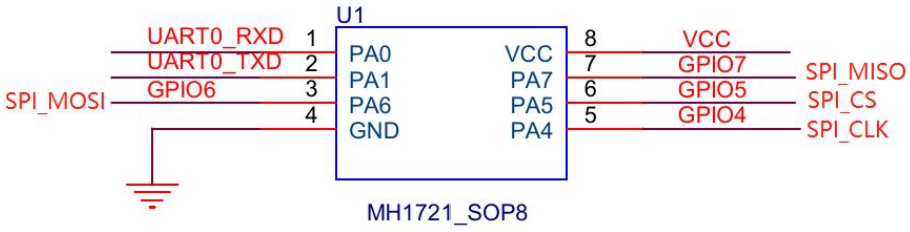


图 2-2

2.2.2 QFN16

2.2.2.1 引脚定义和解释

引脚	定义	备注
VCC/VBAT33	供电电源	电压范围：2.0V-5.5V
GND	地	
GPIO0	串口RX	MH17xx 串口接收
GPIO1	串口 TX	MH17xx 串口发送
GPIO4	SPI CLK	MH17xx 做从机，由AP提供时钟
GPIO5	SPI CS	
GPIO6	SPI MOSI	MH17xx 做从机，对MH71xx是输入
GPIO3	SPI MISO	MH17xx 做从机，对MH71xx是输出

2.2.2.2 硬件参考图

示意图如下：

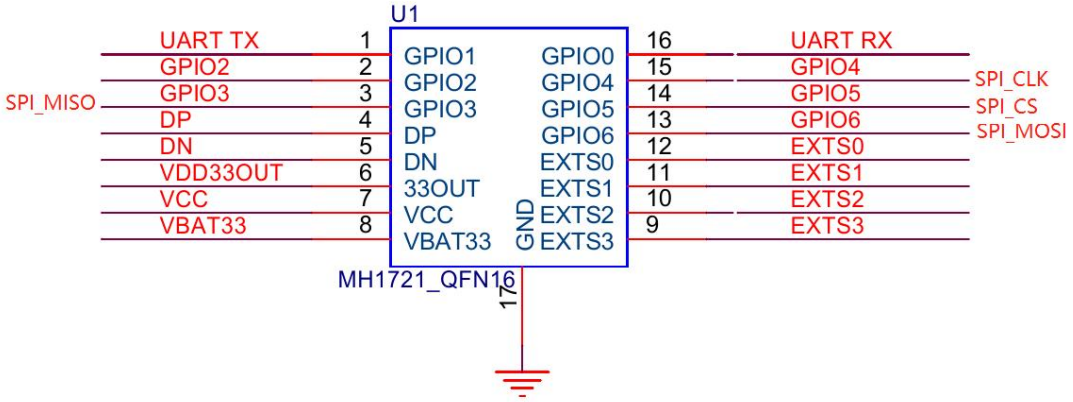


图 2-3

2.3 硬件设计要点

- ✧ QFN16 VBAT33 和 VCC 都需要供电，供电电压为(2~5.5V)
- ✧ 芯片不支持 JLINK 下载，下载方式为：串口 UART0 (GPIO0、 GPIO1)，QFN16 还支持 SPI(GPIO4、GPIO5、GPIO6、GPIO3)
- ✧ Tamper 管脚,保证内部上下拉电阻默认打开,外部 tamper 管脚可以悬空
- ✧ 如不使用 USB,将 DP、DN 悬空即可。
- ✧ 通信方式建议使用 SPI

2.4 SPI通信接口说明

SPI 接口使用模式 1 进行通信，时钟极性（CPOL）=0，时钟相位（CPHA）=1，该模式下

串行同步时钟的空闲状态为低电平，芯片将在串行同步时钟的第二个跳变沿（下降沿）采样。

2.5 串口通信接口说明

串口配置	值
波特率	115200 bps
数据位	8
停止位	1
奇偶校验位	N
流控	N

2.6 密钥管理方案

2.6.1 密钥类型编号

密钥类型	编号
SM2	0x02
SM3	0x03
SM4	0x04
AES	0x05
RSA1024	0x011
RSA2048	0x12
SHA256	0x13

2.6.2 密钥存储

每种密钥最多存储 8 组，ID 号为 1-8. 可以由外部注入和内部生成，只支持生成和替换，不支持删除。

3 通信协议指令说明

多字节数据域(参数类型)采用大端传输；

3.1 上位机发送指令格式定义

```
typedef struct _STRRecData
{
   uint8_t cSTX;                    //包头
   uint8_t cFrame;                  //包序号
   uint8_t cTotleLen[2];            //包长度
   uint8_t cType;                   //指令类型
   uint8_t cCMD;                    //指令命令
   uint8_t cLen[2];                 //指令数据长度
   uint8_t cBuf[cLen];              //指令数据值
   uint8_t cLrc;                    //包 BCC(异或)校验值
   uint8_t cETX;                    //包结束
}STRRecData;
```

3.2 模块响应指令格式定义

```
typedef struct _STRSendData
{
   uint8_t cSTX;                    //包头
   uint8_t cFrame;                  //包序号
   uint8_t cTotleLen[2];            //包长度
   uint8_t cType;                   //指令类型
   uint8_t cCMD;                    //指令命令
   uint8_t cSTACode;                //响应状态码
   uint8_t cLen[2];                 //响应数据长度
   uint8_t cBuf[cLen];              //响应数据
   uint8_t cLrc;                    //包 BCC(异或)校验值
   uint8_t cETX;                    //包结束
}STRSendData;
```

3.3 指令数据说明

数据域	值(HEX)
cSTX	0x02
cFrame	从 0x00 开始每次加 1
cTotleLen	等于 cType + cCMD +[cSTACode] + 2 + cLen
cType	详见下面指令类型说明
cCMD	详见下面指令命令说明
cSTACode	SA 返回的指令执行状态，0x00 表示成功

cLen	指令的数据长度
cBuf	指令的数据值
cLrc	等于 cFrame 到 cBuf 的 BCC(异或)码
cETX	0x40

[cSTACode]表示该数据元只在模块返回数据的指令中才存在。

3.4 返回码(STA)

STA	说明
0x01	执行成功
0x0A	执行失败
0x11	模块打开失败
0x12	模块关闭失败
0x13	模块操作错误
0x21	读操作失败
0x22	写操作失败
0x61	指令数据错误
0x62	指令参数错误
0x63	数据域长度错误
0x64	指令类型错误
0x64	Flash 数据错误
0x65	终端已被攻击
0x71	密钥错误
0x72	加解密错误
0x73	签名验签错误
0x91	处理超时
0xE1	包长度错误
0xE2	包校验错误
0xE3	包结束错误

4　基础功能模块指令详解(11)

4.1 获取芯片SN(11 01)

4.1.1　命令格式

数据域	值(HEX)
TYPE	0x11
CMD	0x01
Len[2]	高字节在前，低字节在后

4.1.2　响应数据

序号	长度	说明
1	16	获取芯片 SN，每颗芯片的 SN 都不同

4.1.3　状态码

STA	说明
0x01	获取成功

4.1.4　示例

指令：02 01 00 04 11 01 00 00 15 40
回复：02 01 00 15 11 01 01 00 10 31 37 32 31 51 31 36 40 00 00 00 00 00 00 10 03 15 40

4.2 获取随机数(11 02)

4.2.1　命令格式

数据域	值(HEX)
TYPE	0x11
CMD	0x02
cLen 长度，2 字节	需要获取随机数的字节数，最大 512

4.2.2　响应数据

序号	长度	说明
1	-	随机数数据，最大 512 字节

4.2.3　状态码

STA	说明

0x01	获取成功

4.2.4 示例

获取 8 字节随机数指令：02 02 00 06 11 02 00 02 00 08 1D 40
回复：02 02 00 0D 11 02 01 00 08 7F B6 97 6B F0 28 34 B9 75 40

4.3 读版本号(11 03)

4.3.1 命令格式

数据域	值(HEX)
TYPE	0x11
CMD	0x03
cLen 长度，2 字节	00 00

4.3.2 响应数据

序号	长度	说明
1	4	版本号信息

4.3.3 状态码

STA	说明
0x01	获取成功

4.3.4 示例

指令：02 03 00 04 11 03 00 00 15 40
回复：02 03 00 09 11 03 01 00 04 00 02 01 04 1A 40
固件更新，版本号会有变化。

4.4 设置模块当前电源状态(11 13)

4.4.1 命令格式

数据域	值(HEX)
TYPE	0x11
CMD	0x13
cLen 长度，2 字节	数据长度
电源类型，1 字节	模块进入休眠：1； 模块关机：2； 模块重启：3；

4.4.2 响应数据

序号	长度	说明
-	0	-

4.4.3 状态码

STA	说明
0x62	指令错误
0x01	执行成功

4.4.4 示例

模块关机指令：02 07 00 05 11 13 00 01 01 00 40(设置休眠)
回复：02 07 00 05 11 13 01 00 00 01 40

4.5 设置模块唤醒方式(11 14)

4.5.1 命令格式

数据域	值(HEX)
TYPE	0x11
CMD	0x14
cLen 长度，2 字节	数据长度
唤醒方式，2 字节	第一字节：使能对应的 IO 作为 IO 唤醒源： 0x00-0x07：对应 Pin0-7 第二字节：唤醒方式：预留

4.5.2 响应数据

序号	长度	说明
-	0	-

4.5.3 状态码

STA	说明
0x62	指令错误
0x01	执行成功

4.5.4 示例

模块关机指令：02 08 00 06 11 14 00 02 14 01 1C 40(使能 PB4 作为 IO 唤醒源)
回复：02 08 00 05 11 14 01 00 00 09 40

4.6 设置GPIO输出电平(11 20)

4.6.1 命令格式

数据域	值(HEX)
TYPE	0x11
CMD	0x20
cLen 长度，2 字节	数据长度
配置方式，2 字节	第一字节：IO 选择： 0x02-0x07：对应 Pin2-7 第二字节，输出电平选择： 0x00：输出低电平 0x01：输出高电平

4.6.2 响应数据

序号	长度	说明
-	0	-

4.6.3 状态码

STA	说明
0x62	指令错误
0x01	执行成功

4.6.4 示例

GPIO4 输出高电平指令：02 09 00 06 11 20 00 02 04 01 39 40
回复：02 09 00 05 11 20 01 00 00 3C 40

GPIO4 输出低电平指令：02 09 00 06 11 20 00 02 04 00 38 40
回复：02 09 00 05 11 20 01 00 00 3C 40

5 算法模块指令详解(41)

5.1 密钥写入(41 01)

写入密钥到芯片中。

5.1.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x01
名称	长度（字节）	说明
密钥类型	1	SM4：0x04 SM2 公钥：0x21(密钥长度为 64，数据为 x+y) SM2 私钥：0x22(密钥长度为 32) SM2 密钥对：0x02(密钥长度为 96，数据为私钥+公钥) RSA1024 公钥：0x23（密钥长度 4+128，e+n） RSA1024 私钥：0x24（密钥长度 128+128，n+d） RSA1024 密钥对：0x11（密钥长度 4+128+128，e+n+d） RSA2048 公钥：0x25（密钥长度 4+256，e+n） RSA2048 私钥：0x26（密钥长度 256+256,n+d） RSA2048 密钥对：0x12（密钥长度 4+256+256,e+n+d） AES：0x05
密钥 ID	1	密钥 id 号(0x01-0x08)
密钥长度	2	密钥长度（最大 1024 字节）
密钥数据	最大 1024 字节	密钥数据

5.1.2 响应数据

数据域	值(HEX)
TYPE	0x41
CMD	0x01
cSTACode	见下表
cLen（2 个字节）	00 00

5.1.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.1.4 示例

写入 SM4 密钥指令：

02 01 00 18 41 01 00 14 04 07 00 10 11 11 11 11 22 22 22 22 33 33 33 33 44 44 44 44 5E 40

回复：02 01 00 05 41 01 01 00 00 45 40

写入 SM2 公钥：

02 01 00 48 41 01 00 44 21 01 00 40 E9 4B F6 D3 3B C1 ED E3 36 DD B7 18 76 ED 30 91 80 1B 71 D5 4D 30 F2 07 A2 47 A6 DB F4 12 CE 94 2A E1 67 04 6E AF F8 CC B8 ED 32 9B 1D D8 64 4F F5 CA CE AD E9 BD DF 67 EF 1A F8 75 BC 6E C8 9D B3 40

回复：02 01 00 05 41 01 01 00 00 45 40

写入 SM2 私钥：

02 01 00 28 41 01 00 24 22 02 00 20 E5 1A 0A 43 1E C1 78 36 4C 5E 7B 6D 9E 54 D9 25 CB 3A A5 3C 62 2E 9D 2F A9 9A F7 90 3A B7 04 14 07 40

回复：02 01 00 05 41 01 01 00 00 45 40

写入 RSA2048 公钥：

02 01 01 0C 41 01 01 08 25 01 01 04 00 01 00 01 8D BE 22 62 CA 49 78 92 D0 56 A8 D2 84 2A 57 6F 75 64 F3 7A 00 55 F4 88 93 C2 A4 F6 BB 26 6E A0 BD 3E FA F1 02 69 71 52 1D 7A 53 EC 2F 46 37 C4 9A E2 FF DA 56 3B 8A 4A 61 59 F4 EA 4C C6 E6 EF FF C4 E8 36 63 AF 9A D3 95 EA E1 4D 7D BD E8 7C C9 3B 07 6C 82 67 93 05 6C 51 96 6A 33 86 69 22 B1 FC 1E 6F A2 7F F0 46 0B B4 73 7F F7 31 69 6D 35 58 3A 90 3F FE FA 23 5D DE 13 5D 2E 31 55 5F 10 38 42 86 3E F3 E0 7A AE 09 ED 5C 8C A9 BB 73 0A 09 92 47 9F 7E 67 83 09 0A 96 A6 A9 5D 11 D3 22 FB 66 FD 6F 28 62 2C 4E 2F 4B AD 57 8E 36 E1 05 F7 DB 94 D9 AD D6 1B 96 28 80 04 02 4B 32 F3 1B 9E 87 5E 9A 33 38 84 B5 E8 7C 06 2A BA 13 57 73 EE 48 84 4B 43 3E 0D D1 96 A1 3A 2A 48 51 B7 CA CD 89 7B 31 B4 74 1D EB B5 91 BD AF 20 5F 22 CB 44 12 BD 59 31 9C 68 8E AC 11 84 90 06 9A 65 A0 40

回复：02 01 00 05 41 01 01 00 00 45 40

写入 RSA2048 私钥：

02 01 02 08 41 01 02 04 26 02 02 00 8D BE 22 62 CA 49 78 92 D0 56 A8 D2 84 2A 57 6F 75 64 F3 7A 00 55 F4 88 93 C2 A4 F6 BB 26 6E A0 BD 3E FA F1 02 69 71 52 1D 7A 53 EC 2F 46 37 C4 9A E2 FF DA 56 3B 8A 4A 61 59 F4 EA 4C C6 E6 EF FF C4 E8 36 63 AF 9A D3 95 EA E1 4D 7D BD E8 7C C9 3B 07 6C 82 67 93 05 6C 51 96 6A 33 86 69 22 B1 FC 1E 6F A2 7F F0 46 0B B4 73 7F F7 31 69 6D 35 58 3A 90 3F FE FA 23 5D DE 13 5D 2E 31 55 5F 10 38 42 86 3E F3 E0 7A AE 09 ED 5C 8C A9 BB 73 0A 09 92 47 9F 7E 67 83 09 0A 96 A6 A9 5D 11 D3 22 FB 66 FD 6F 28 62 2C 4E 2F 4B AD 57 8E 36 E1 05 F7 DB 94 D9 AD D6 1B 96 28 80 04 02 4B 32 F3 1B 9E 87 5E 9A 33 38 84 B5 E8 7C 06 2A BA 13 57 73 EE 48 84 4B 43 3E 0D D1 96 A1 3A 2A 48 51 B7 CA CD 89 7B 31 B4 74 1D EB B5 91 BD AF 20 5F 22 CB 44 12 BD 59 31 9C 68 8E AC 11 84 90 06 9A 65 10 49 B8 13 D8 21 07 3C FF B9 E5 9E 83 57 86 42 A5 9F DB 26 BA E1 25 BF 88 13 46 F7 9F 5B F4 3C 7E 62 BD 5D 72 A4 81 44 29 65 04 3D D0 D4 E5 D5 AE E2 C4 F9 E7 0C E2 80

57 9D 89 BA 5E E6 40 65 75 E3 BF B7 78 4F 16 A0 97 CA AC E7 45 BA CB FB 82 F8 48
8B 1C 95 20 5C F0 2C 93 F7 52 42 70 D4 6E D5 84 FD D9 13 90 9D CB FC 89 85 3B F7
AE A0 C1 0F 89 73 48 17 59 D1 34 99 2F 6A 76 C3 6E 86 D9 1C 1F 0D CC AF F2 08 F9
04 EF B3 81 07 FF 94 A7 81 77 00 A4 B2 73 D7 8F 92 D3 BD 32 A5 06 9E C3 C8 16 35
49 17 9F EB 4B 9E 66 94 F6 21 54 D3 45 7B 59 A6 D1 9C AD 2F 86 B2 09 61 3E 90 6D
E6 70 BF 5D 66 F7 98 5B 5C 0A 0F 7B FA F7 16 8E D3 73 04 5E 9F 0B 5C 93 62 79 6E
90 7C 75 E0 9E 24 2B E8 47 6B 8E BA 58 2B AB 2C 24 13 35 8A 95 03 6A 21 53 06 66
51 B4 63 6B F2 FF CA 54 B1 CC 41 78 40
回复：02 01 00 05 41 01 01 00 00 45 40

导入 RSA2048 密钥对
02 01 02 0C 41 01 02 08 12 03 02 04 00 01 00 01 8D BE 22 62 CA 49 78 92 D0 56 A8
D2 84 2A 57 6F 75 64 F3 7A 00 55 F4 88 93 C2 A4 F6 BB 26 6E A0 BD 3E FA F1 02 69
71 52 1D 7A 53 EC 2F 46 37 C4 9A E2 FF DA 56 3B 8A 4A 61 59 F4 EA 4C C6 E6 EF FF
C4 E8 36 63 AF 9A D3 95 EA E1 4D 7D BD E8 7C C9 3B 07 6C 82 67 93 05 6C 51 96 6A
33 86 69 22 B1 FC 1E 6F A2 7F F0 46 0B B4 73 7F F7 31 69 6D 35 58 3A 90 3F FE FA
23 5D DE 13 5D 2E 31 55 5F 10 38 42 86 3E F3 E0 7A AE 09 ED 5C 8C A9 BB 73 0A 09
92 47 9F 7E 67 83 09 0A 96 A6 A9 5D 11 D3 22 FB 66 FD 6F 28 62 2C 4E 2F 4B AD 57
8E 36 E1 05 F7 DB 94 D9 AD D6 1B 96 28 80 04 02 4B 32 F3 1B 9E 87 5E 9A 33 38 84
B5 E8 7C 06 2A BA 13 57 73 EE 48 84 4B 43 3E 0D D1 96 A1 3A 2A 48 51 B7 CA CD 89
7B 31 B4 74 1D EB B5 91 BD AF 20 5F 22 CB 44 12 BD 59 31 9C 68 8E AC 11 84 90 06
9A 65 10 49 B8 13 D8 21 07 3C FF B9 E5 9E 83 57 86 42 A5 9F DB 26 BA E1 25 BF 88
13 46 F7 9F 5B F4 3C 7E 62 BD 5D 72 A4 81 44 29 65 04 3D D0 D4 E5 D5 AE E2 C4 F9
E7 0C E2 80 57 9D 89 BA 5E E6 40 65 75 E3 BF B7 78 4F 16 A0 97 CA AC E7 45 BA CB
FB 82 F8 48 8B 1C 95 20 5C F0 2C 93 F7 52 42 70 D4 6E D5 84 FD D9 13 90 9D CB FC
89 85 3B F7 AE A0 C1 0F 89 73 48 17 59 D1 34 99 2F 6A 76 C3 6E 86 D9 1C 1F 0D CC
AF F2 08 F9 04 EF B3 81 07 FF 94 A7 81 77 00 A4 B2 73 D7 8F 92 D3 BD 32 A5 06 9E
C3 C8 16 35 49 17 9F EB 4B 9E 66 94 F6 21 54 D3 45 7B 59 A6 D1 9C AD 2F 86 B2 09
61 3E 90 6D E6 70 BF 5D 66 F7 98 5B 5C 0A 0F 7B FA F7 16 8E D3 73 04 5E 9F 0B 5C
93 62 79 6E 90 7C 75 E0 9E 24 2B E8 47 6B 8E BA 58 2B AB 2C 24 13 35 8A 95 03 6A
21 53 06 66 51 B4 63 6B F2 FF CA 54 B1 CC 41 41 40
回复：02 01 00 05 41 01 01 00 00 45 40

写入 AES 密钥：
02 01 00 18 41 01 00 14 05 01 00 10 11 11 11 11 22 22 22 22 33 33 33 33 44 44 44
44 59 40
回复：02 01 00 05 41 01 01 00 00 45 40

5.2 非对称密钥对产生(41 02)

产生非对称密钥对并保存到芯片中。

5.2.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x02
名称	长度（字节）	说明
密钥类型	1	SM2： 0x02 RSA1024：0x11 RSA2048：0x12（密钥生成平均用时 5 秒）
密钥 ID	1	密钥 id 号(0x01-0x08)

5.2.2 响应数据

数据域	值(HEX)
TYPE	0x41
CMD	0x02
cSTACode	见下表
cLen（2 个字节）	00 00

5.2.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.2.4 示例

产生 SM2 密钥对指令，ID 号为 5：
02 02 00 06 41 02 00 02 02 05 42 40
回复：02 02 00 05 41 02 01 00 00 45 40

产生 RSA1024 密钥对指令，ID 号为 1：
02 02 00 06 41 02 00 02 11 01 55 40
回复：02 02 00 05 41 02 01 00 00 45 40

产生 RSA2048 密钥对指令，ID 号为 2：
02 02 00 06 41 02 00 02 12 02 55 40
回复：02 02 00 05 41 02 01 00 00 45 40

5.3 获取非对称密钥ID列表(41 11)

获取非对称密钥 ID 列表。

5.3.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x11
名称	长度（字节）	说明
密钥类型	1	SM2： 0x02 RSA1024：0x11 RSA2048：0x12

5.3.2 响应数据

数据域	值(HEX)
TYPE	0x41
CMD	0x11
cSTACode	见下表
长度（2 字节）	密钥个数
获取非对称密钥 ID 列表信息	假如 COS 中存在 ID 为 0x01, 0x04, 0x06 三对密钥，则 COS 返回 0x010406

5.3.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.3.4 示例

读 SM2 ID 列表：
02 03 00 05 41 11 00 01 02 55 40
回复：02 03 00 06 41 11 01 00 01 02 57 40

读 RSA1024 ID 列表:
02 03 00 05 41 11 00 01 11 46 40
回复：02 03 00 06 41 11 01 00 01 01 54 40

读 RSA2048 ID 列表:
02 03 00 05 41 11 00 01 12 45 40
回复：02 03 00 06 41 11 01 00 01 01 54 40

5.4 获取指定ID的非对称密钥对公钥数据(41 12)

获取指定 ID 的非对称密钥对公钥数据。

5.4.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x12
名称	长度（字节）	说明
密钥类型	1	SM2： 0x02 RSA1024：0x11 RSA2048：0x12
密钥 ID	1	密钥 id 号(0x01-0x08)

5.4.2 响应数据

数据域	值(HEX)
TYPE	0x41
CMD	0x12
状态码	见下表
长度（2 字节）	数据长度
公钥数据	SM2 公钥数据：32 字节 X 加 32 字节 Y RSA1024 公钥数据：4 字节 e 加 128 字节 n 值 RSA2048 公钥数据：4 字节 e 加 256 字节 n 值

5.4.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.4.4 示例

读 SM2 密钥对中 ID 为 5 的公钥数据：

02 04 00 06 41 12 00 02 02 05 54 40

回复：02 04 00 45 41 12 01 00 40 4A 1A 61 52 73 F2 23 C9 E5 AB A4 2E 05 57 7B 4C 03 E7 31 E1 79 02 AF F4 51 82 16 2D 2D 3B 7E C8 5A A0 05 15 B9 95 D9 E2 E3 99 FE A8 83 9F 72 DE D0 2C D5 76 80 4F 49 F0 6B 3D 9C 86 3E 3E 3E D5 49 40

读 RSA1024 密钥对 ID 为 5 的公钥数据：

02 04 00 06 41 12 00 02 11 05 47 40

回复：02 04 00 89 41 12 01 00 84 00 01 00 01 B5 72 85 58 35 82 33 5B 6E 67 28 65 C9 81 2D 68 40 53 43 04 1C EA 34 47 AB 8B B1 73 10 99 E2 2C BE EB EE 62 F4 15 16 28 CC 8A 38 91 AD 00 9B 58 42 E9 08 52 AA 39 BF 0E 88 A3 D0 0B E1 11 12 68 02 CC B6 62 6B DE 76 B2 17 A0 93 26 06 A4 53 BB 64 73 87 B6 85 69 31 33 1D F2 A9 93 CE 64 FD 06 18 7F 89 29 3A 42 79 54 7C 61 68 53 1E 13 85 E6 B6 1A B2 AD 77 DE B9 34 15 89 D6 3B 2F 70 3C 9D 20 40

读 RSA2048 密钥对 ID 为 6 的公钥数据：

02 04 00 06 41 12 00 02 12 05 44 40

回复：02 04 01 09 41 12 01 01 04 00 01 00 01 AF 7D 73 01 9E DE 55 D5 44 2B D4 AF 6C 8B 1F 81 BD 77 09 E9 EF 17 DD 3C FB 18 17 6D E4 E7 CE BA E2 66 DA C6 E7 6B BA 7C 8E D1 92 0E 2A F6 0B DD 7F AC 4F 1A E6 BC 89 36 99 9B 4A 38 57 E7 B6 D0 CC AB 5E 35 2B 1F 33 A5 67 D6 2F 5C 2D 6D 7C 9F CD AB 60 DC C6 CD D8 2F 86 B7 ED BD B5 FA 68 67 7B A8 20 1C DB FA 26 52 BF 95 86 C9 AD D8 68 4C F2 F1 3A 9E 06 D0 B7 22 74 3B 0F 9A 48 DE 7B 1A 66 0D AB DA 52 28 A8 B5 A7 D1 96 05 71 EA 97 DF 8C 83 44 BE 8F CF 7E C7 5E B2 38 DD 77 A2 CC DF 99 75 C6 0D 5F E5 D2 7A F0 DB E8 6E 1D 07 C7 85 7E 36 09 1D D3 40 7F CD 54 B1 52 82 1D E2 89 90 8B 90 FC B7 1E 6E 75 52 6E BD 22 3D 73 F5 9F BD DD 85 4D 7D 19 49 23 ED 8C C1 84 7A D6 39 AF 07 CC 22 91 58 37 C6 49 D4 9C 72 7E 37 1C E4 B0 07 22 63 40 06 4B C1 F4 E4 58 51 EB B5 9D D5 38 87 CF 40

5.5 获取指定ID的非对称密钥对数据(41 13)

获取指定 ID 的非对称密钥对数据。

5.5.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x13
名称	长度（字节）	说明
密钥类型	1	SM2： 0x02 RSA1024：0x11 RSA2048：0x12
密钥 ID	1	密钥 id 号(0x01-0x08)

5.5.2 响应数据

数据域	值(HEX)
TYPE	0x41
CMD	0x13
状态码	见下表
长度（2 字节）	数据长度
密钥数据	SM2 密钥对数据：32 字节 X+32 字节 Y+32 字节 D RSA1024 密钥对数据：4 字节 e+128 字节 n+128 字节 d RSA2048 密钥对数据：4 字节 e+256 字节 n+256 字节 d

5.5.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.5.4 示例

读 SM2 密钥对中 ID 为 5 的密钥数据：

02 04 00 06 41 13 00 02 02 05 55 40

回复：

02 04 00 65 41 13 01 00 60 4E D1 30 6F 43 87 2D 64 90 70 64 24 42 00 5E A3 C1 75
8E 32 C3 87 66 D9 46 B3 D7 B2 2B 2B BF 32 BD 97 AE 97 7F 5C D0 E8 FD 50 E8 40 34
0A AB A8 95 74 40 4F D8 B0 96 A1 81 05 A3 9D 73 76 3B B8 19 89 71 63 AE AE EC FF
D2 E4 0D BE C7 AA 29 62 28 29 5F 4A 99 9F D5 0D A2 09 7F CB A9 1F 7D FE 81 40

读 RSA2048 密钥对 ID 为 6 的密钥数据：

02 04 00 06 41 13 00 02 12 06 46 40

回复：

02 04 02 09 41 13 01 02 04 00 01 00 01 65 FF 66 B2 00 75 CA 74 2C A6 9B 70 05 C5
82 13 54 EA 63 46 A8 93 03 E7 87 71 28 96 5B 7B E7 B4 61 6E 1E 66 A0 89 8E 7D 17
64 D7 9C D9 B3 B2 9D FF 57 35 8D D1 B1 97 A3 5F 3E 81 77 5D AD 8A 54 2A BC 8A D1
3A 3D 6A 6B 52 1B 83 EE A4 3C 5E 8D 0A A9 89 0E F4 11 97 E6 8D 15 40 A4 C5 1D F4
18 BB C3 66 D9 EA 00 4B 13 B6 D4 C3 85 5C 6D 95 9A B8 F9 B7 AB 74 37 B3 94 C8 1B
F1 CA 72 7E 88 6F F6 0A 12 BD E9 4A 8A 2A 33 8B FF 60 59 B6 62 C0 F4 09 9A B9 33
A7 9D A1 09 14 B1 8F C9 27 FA FD 40 D0 2C 8A D4 29 C6 F3 0B BB 77 29 0D 20 60 C4
71 8B 73 07 A5 6B D7 D3 DE DD C7 F1 AB 85 EC 20 A7 A6 51 25 A1 6B 03 32 F4 19 0D
2F C7 25 E3 9E 63 32 1A 22 05 00 2B 33 8D 5C C7 76 26 30 83 93 4A 0C 7C 10 38 82
24 19 9F 50 EC 75 48 D8 75 33 DF B3 F7 5F C5 6A 51 8C 5C C8 5F 76 C6 A4 6D 79 16
B6 93 25 DC 58 5E A7 14 32 5D B6 CA 72 3B 0F 16 FF C2 EF BF 26 4D DE 47 18 F9 D2
D1 B8 7B D6 7D 43 CA 5D 4C 2E 95 9E 61 91 41 3A 5A 78 5B B4 37 62 32 38 CC 93 61
93 2D E8 7B 68 1B 62 43 C5 8E 66 C1 FA E9 9F 37 8D 82 91 42 05 E8 68 D1 1D 53 5C
81 7A E4 FA ED FA 97 3C 3E 52 F2 DA 42 BB 27 44 D2 28 80 A5 64 12 95 CA 37 68 01
37 1D F3 80 71 8B 67 10 D0 3E 9B 49 1C 7F F1 77 21 9A 3C 1C 39 BE 82 B4 3A D4 20
69 8F 06 B5 E6 3E 17 24 37 D4 1A 33 FE 42 20 76 F0 8D 4A CA E0 71 B9 87 36 97 FD
52 5F 74 85 6A 95 6E 33 06 4D 86 AF F8 96 92 F2 3A 33 EF FE F2 A6 C9 61 6D 0C 29
03 9F F5 23 AF 1D 6C 1B 63 E3 4D C3 21 06 5F D2 11 29 F5 BB 8F 3F 5A 6D D9 C3 53
26 39 A9 2E BC 99 96 89 A4 CC 79 5B 1D BF CC D8 EA EE DD 51 D4 AC 1A D1 DB 28 A4
CD F9 6B AF 51 9A AB 98 3B 46 99 E9 C9 40

5.6 计算HASH值(41 41)

计算 HASH 值。

5.6.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x41
名称	长度（字节）	说明
算法类型	1	SM3： 0x03 SHA256： 0x13
计算方法	1	完整计算：0x01 分段计算 -- 第一包数据：0x11 分段计算 -- 中间过程数据：0x12 分段计算 -- 结束包数据：0x13
数据	最大 1024 字节	需要计算 hash 的数据

5.6.2 响应数据

数据域	值(HEX)
TYPE	0x41
CMD	0x41
状态码	见下表
cLen（2 字节）	回复数据长度
Hash 结果	Hash 结果

5.6.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.6.4 示例

使用 SM3 算法完整计算一包 HASH 数据：

02 05 00 36 41 41 00 32 03 01 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 03 40

回复：02 05 00 25 41 41 01 00 20 6E 91 8C 34 CC 38 97 47 86 9E 67 41 92 4A 40 11 2F 02 E7 D9 02 DE 52 CE 8B 6C 87 25 B8 7E CC 1F D6 40

分包使用 SM3 算法计算 HASH 数据：

第一包数据：02 06 00 16 41 41 00 12 03 11 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 10 40

回复：02 06 00 05 41 41 01 00 00 02 40

中间数据：02 07 00 16 41 41 00 12 03 12 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D

3E 3F 12 40
回复：02 07 00 05 41 41 01 00 00 03 40

结尾数据：02 08 00 16 41 41 00 12 03 13 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 1C 40
回复：02 08 00 25 41 41 01 00 20 6E 91 8C 34 CC 38 97 47 86 9E 67 41 92 4A 40 11 2F 02 E7 D9 02 DE 52 CE 8B 6C 87 25 B8 7E CC 1F DB 40

使用 SHA256 算法完整计算一包 HASH 数据：
02 05 00 36 41 41 00 32 13 01 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 13 40
回复：02 05 00 25 41 41 01 00 20 B5 F1 F6 CF 51 51 DF 72 9F E8 E8 9C 9E 7E 90 54 C6 D5 0B 4B E0 92 E2 97 8A 9A 9F E3 82 2B 87 B3 53 40

分包使用 SHA256 算法计算 HASH 数据：
第一包数据：02 06 00 16 41 41 00 12 13 11 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 00 40
回复：02 06 00 05 41 41 01 00 00 02 40

中间数据：02 07 00 16 41 41 00 12 13 12 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 02 40
回复：02 07 00 05 41 41 01 00 00 03 40

结尾数据：02 08 00 16 41 41 00 12 13 13 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 0C 40
回复：02 08 00 25 41 41 01 00 20 B5 F1 F6 CF 51 51 DF 72 9F E8 E8 9C 9E 7E 90 54 C6 D5 0B 4B E0 92 E2 97 8A 9A 9F E3 82 2B 87 B3 5E 40

5.7 对称算法加密(41 31)

对称算法加密。

5.7.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x31
名称	长度（字节）	说明
算法类型	1	SM4： 0x04 AES： 0x05
加密模式	1	ECB：01 CBC：02
密钥 ID	1	密钥 ID，1~8
IV 长度	1	如果 IV 值为空，该位发 0；

		如果发送 IV 值，该位固定为 16 字节。
IV 数据	0/16	IV 值,没有 IV 值时数据长度为 0 有 IV 值时长度为 16
要加密的数据	-	要加密的数据

5.7.2 响应数据

数据域	值(HEX)
TYPE	0x41
CMD	0x31
状态码	见下表
长度（2 字节）	加密结果数据长度
加密结果	解密结果

5.7.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.7.4 示例

使用 SM4 ecb 算法加密数据：

02 0C 00 18 41 31 00 14 04 01 04 00 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF 71 40

回复：02 0C 00 15 41 31 01 00 10 02 2E 21 40 A0 A5 F0 0A E0 E2 55 44 92 7A 04 9F AA 40

使用 SM4 cbc 算法加密数据，IV 值是 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34

02 0C 00 28 41 31 00 24 04 02 04 10 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF 62 40

回复：02 0C 00 15 41 31 01 00 10 69 BA 19 57 6D 9B E0 F6 B1 00 1B 2F 4C 6E 73 FB 2A 40

AES ecb 算法加密：

02 0C 00 18 41 31 00 14 05 01 01 00 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF 75 40

回复：02 0C 00 15 41 31 01 00 10 DF BF 00 A7 F3 CF 88 BA 94 13 0D FB E1 3E 15 78 72 40

AES cbc 算法加密：

02 0C 00 28 41 31 00 24 05 02 01 10 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF 66 40

回复：02 0C 00 15 41 31 01 00 10 02 10 D7 BB CF E4 50 BD 8D AF 34 DF 90 70 55 E1

5D 40

5.8 对称算法解密(41 32)

对称算法解密。

5.8.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x32
名称	长度（字节）	说明
算法类型	1	SM4： 0x04 AES： 0x05
加密模式	1	ECB：01 CBC：02
密钥 ID	1	密钥 ID，1~8
IV 长度	1	如果 IV 值为空，该位发 0； 如果发送 IV 值，该位固定为 16 字节。
IV 数据	0/16	IV 值,没有 IV 值时数据长度为 0 有 IV 值时长度为 16
要解密的数据	-	要解密的数据

5.8.2 响应数据

数据域	值(HEX)
TYPE	0x41
CMD	0x32
状态码	见下表
长度（2 字节）	解密结果数据长度
解密结果	解密结果

5.8.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.8.4 示例

使用 SM4 ecb 算法解密数据：

02 0D 00 18 41 32 00 14 04 01 04 00 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF 73 40

回复：02 0D 00 15 41 32 01 00 10 CF FB 0A 22 76 5E FC 9A 31 0B 3E E9 5D 19 09 A7

2F 40

使用 SM4 cbc 算法解密数据，IV 值是 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34
02 0D 00 28 41 32 00 24 04 02 04 10 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34
34 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF 60 40
回复：02 0D 00 15 41 32 01 00 10 FE CA 3B 13 44 6C CE A8 02 38 0D DA 69 2D 3D 93
2F 40

使用 AES ecb 算法解密：
02 0D 00 18 41 32 00 14 05 01 01 00 DF BF 00 A7 F3 CF 88 BA 94 13 0D FB E1 3E 15
78 7D 40
回复：02 0D 00 15 41 32 01 00 10 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF
7A 40

使用 AES cbc 算法解密：
02 0D 00 28 41 32 00 24 05 02 01 10 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34
34 02 10 D7 BB CF E4 50 BD 8D AF 34 DF 90 70 55 E1 41 40
回复：02 0D 00 15 41 32 01 00 10 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF
7A 40

5.9 对称算法在线加密(41 35)

对称算法加密，指令中包含算法模式、密钥和输入数据等信息。

5.9.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x35
名称	长度（字节）	说明
算法类型	1	SM1：0x01 SM4：0x04
加密模式	1	ECB：0x01 CBC：0x02
密钥 ID	1	0x00(固定值)
KeyLen	1	密钥长度
Key	16	密钥数据
IV 长度	1	IV 值长度，ECB 模式为 0
IV 数据	16	IV 值数据，ECB 模式为空
要加密的数据	-	要加密的数据

5.9.2 响应数据

数据域	值(HEX)
TYPE	0x41

CMD	0x35
状态码	见下表
长度（2 字节）	加密结果数据长度
加密结果	解密结果

5.9.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.9.4 示例

使用 SM4 ECB 算法加密数据：
02 0C 00 29 41 35 00 25 04 01 00 10 11 11 11 11 22 22 22 22 33 33 33 33 44 44 44 44 00 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF 61 40
回复：02 0C 00 15 41 35 01 00 10 02 2E 21 40 A0 A5 F0 0A E0 E2 55 44 92 7A 04 9F AE 40

使用 SM4 CBC 算法加密数据，IV 值是 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34
02 0C 00 39 41 35 00 35 04 02 00 10 11 11 11 11 22 22 22 22 33 33 33 33 44 44 44 44 10 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF 72 40
回复：02 0C 00 15 41 35 01 00 10 69 BA 19 57 6D 9B E0 F6 B1 00 1B 2F 4C 6E 73 FB 2E 40

使用 SM1 ECB 算法加密数据：
02 0C 00 29 41 35 00 25 01 01 00 10 11 11 11 11 22 22 22 22 33 33 33 33 44 44 44 44 00 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF 64 40
回复：02 0C 00 15 41 35 01 00 10 49 B1 98 CA 54 5C DF B8 45 78 34 ED 63 44 6F 65 70 40

5.10 对称算法在线解密(41 36)

对称算法解密，指令中包含算法模式、密钥和输入数据等信息。

5.10.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x36
名称	长度（字节）	说明
算法类型	1	SM1：0x01 SM4：0x04

加密模式	1	ECB：0x01 CBC：0x02
密钥 ID	1	0x00(固定值)
KeyLen	1	密钥长度
Key	16	密钥数据
IV 长度	1	IV 值长度，ECB 模式为 0
IV 数据	16	IV 值数据，ECB 模式为空
要解密的数据	-	要解密的数据

5.10.2 响应数据

数据域	值(HEX)
TYPE	0x41
CMD	0x36
状态码	见下表
长度（2 字节）	解密结果数据长度
解密结果	解密结果

5.10.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.10.4 示例

使用 SM4 ECB 算法解密数据：

02 0D 00 29 41 36 00 25 04 01 00 10 11 11 11 11 22 22 22 22 33 33 33 33 44 44 44 44 00 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF 63 40

回复：02 0D 00 15 41 36 01 00 10 CF FB 0A 22 76 5E FC 9A 31 0B 3E E9 5D 19 09 A7 2B 40

使用 SM4 CBC 算法加密数据，IV 值是 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34

02 0D 00 39 41 36 00 35 04 02 00 10 11 11 11 11 22 22 22 22 33 33 33 33 44 44 44 44 10 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF 70 40

回复：02 0D 00 15 41 36 01 00 10 FE CA 3B 13 44 6C CE A8 02 38 0D DA 69 2D 3D 93 2B 40

使用 SM1 ECB 算法解密数据：

02 0D 00 29 41 36 00 25 01 01 00 10 11 11 11 11 22 22 22 22 33 33 33 33 44 44 44 44 00 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF 66 40

回复：02 0D 00 15 41 36 01 00 10 95 77 71 26 CE A0 D6 44 EA 67 CE 60 96 43 92 16 45 40

5.11 非对称算法加密(41 21)

非对称算法加密。

5.11.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x21
名称	长度（字节）	说明
算法类型	1	SM2： 0x02 RSA1024：0x11 RSA2048：0x12
密钥 ID	1	密钥 ID，1~8
是否需要填充（填充模式为 pcks#1）	1	不需要填充：0x00 需要填充：0x01（暂不支持）
要加密的数据	-	要加密的数据

5.11.2 响应数据

数据域	值(HEX)
TYPE	0x41
CMD	0x21
状态码	见下表
长度（2 字节）	加密结果数据长度
加密结果	加密结果

5.11.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.11.4 示例

使用 SM2 算法加密数据：

02 0A 00 17 41 21 00 13 02 01 00 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 6D 40

回复：02 0A 00 75 41 21 01 00 70 FF 95 CE 21 EC D2 62 6B EA 72 92 38 68 A9 06 37 1B 4D 74 B9 D8 0C 05 E9 F4 CE 75 57 86 A9 C6 67 DE A9 2F 2D 4E D3 67 5E CC 0A 7D FC 2F 3B 17 18 A8 A3 CD AF 6F CD A1 54 EF 39 62 0B F8 70 F4 C7 08 5E 77 D7 E5 68 5F D2 6D 73 65 FC 6B 7C 9C 95 C8 F5 C6 E5 C8 F9 2A E6 19 1E E0 1E 20 B1 3C DF 82 E2 9F 47 65 D2 F4 BB EB A9 6D 2E E9 9D BD 5E 4D 40

同一组密钥和数据，每次的加密结果是不同的。

RSA2048 算法加密：

02 0A 01 07 41 21 01 03 12 01 00 30 30 30 30 32 32 32 32 33 33 33 33 34 34 34 34
31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 31 31 31 31 32 32 32 32 33 33 33
33 34 34 34 34 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 31 31 31 31 32 32
32 32 33 33 33 33 34 34 34 34 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 31
31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 31 31 31 31 32 32 32 32 33 33 33 33
34 34 34 34 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 31 31 31 31 32 32 32
32 33 33 33 33 34 34 34 34 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 31 31
31 31 32 32 32 32 33 33 33 33 34 34 34 34 31 31 31 31 32 32 32 32 33 33 33 33 34
34 34 34 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 31 31 31 31 32 32 32 32
33 33 33 33 34 34 34 34 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 7D 40

回复：02 01 05 41 21 01 01 00 C2 CD A9 7B 2B 8D 26 B0 37 D2 F4 CE 8D 93 CA 11 5A
8E E9 B5 D0 C4 04 9A 25 2B DC 65 CA 93 93 22 38 5E B2 BD C9 B2 89 09 3C 22 97 F2
97 E0 F2 BD DB B7 3B E7 6D 6A F1 F6 CC 17 BC 44 69 C6 C4 6C DB A8 7E F4 42 7A CF
93 DB 80 AF 50 E1 F5 C3 ED A9 28 E7 ED 66 5E 91 95 A5 FB 86 9C BA 79 D5 78 20 12
88 54 FD DB DA F1 B5 11 6D 2D 71 77 3F 85 11 2A 27 0D 3C FF 27 21 39 B2 48 35 D8
45 F8 EE FB F3 08 CA 04 5D B3 FA 8E 05 97 49 81 DC 7D BC 0C 8B 1B CA 99 9B 97 37
25 C5 CE 0E 4D C5 A6 29 F5 06 A4 1E F0 E4 1A DE F6 C9 2B C3 C7 1A 8B 4F 4F 94 A3
70 DA 75 1D FB B6 F0 8A 97 DB F0 B8 D2 7C C7 CA 3D 9C D4 87 82 14 C3 B4 DF F0 3B
50 34 EB 55 E2 0A 95 51 0C 6F A2 8C 09 B8 69 A0 35 E8 A0 EC 1B 64 15 4D 78 EC C5
43 FD C7 4E 66 2F 4E 5C 92 DE DE 6E 1A 87 D1 E4 B7 F9 DF 5D 93 32 2C AE 0A 40

5.12 非对称算法解密(41 22)

非对称算法解密。

5.12.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x22
名称	长度（字节）	说明
算法类型	1	SM2： 0x02 RSA1024：0x11 RSA2048：0x12
密钥 ID	1	密钥 ID，1~8
是否需要填充（填充模式为 pcks#1）	1	不需要填充：0x00 需要填充：0x01（暂不支持）
要解密的数据	-	要解密的数据

5.12.2 响应数据

数据域	值(HEX)
TYPE	0x41

CMD	0x22
状态码	见下表
长度（2 字节）	解密结果数据长度
解密结果	解密结果

5.12.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.12.4 示例

使用 SM2 算法解密数据：

02 0B 00 77 41 22 00 73 02 02 00 FF 95 CE 21 EC D2 62 6B EA 72 92 38 68 A9 06 37
1B 4D 74 B9 D8 0C 05 E9 F4 CE 75 57 86 A9 C6 67 DE A9 2F 2D 4E D3 67 5E CC 0A 7D
FC 2F 3B 17 18 A8 A3 CD AF 6F CD A1 54 EF 39 62 0B F8 70 F4 C7 08 5E 77 D7 E5 68
5F D2 6D 73 65 FC 6B 7C 9C 95 C8 F5 C6 E5 C8 F9 2A E6 19 1E E0 1E 20 B1 3C DF 82
E2 9F 47 65 D2 F4 BB EB A9 6D 2E E9 9D BD 5E 4F 40

回复：02 0B 00 15 41 22 01 00 10 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34
6C 40

RSA2048 算法解密：

02 0B 01 07 41 22 01 03 12 02 00 3A 40 D6 3B 55 86 F1 CF 90 E4 E3 D2 64 A8 86 A3
26 04 DB 9A E1 97 02 98 5F 6B F5 7B EF E5 F6 DD 4A 63 BC 28 5D CC 84 64 DD 48 D4
DB F4 A1 63 34 8B CB 4D CE AE 70 B3 22 B8 F4 FC D0 76 60 15 0F 14 73 E5 CF 4C DE
8E 48 29 C1 4D A3 F0 FE 7B DA 8B C6 FD 2A 37 DC 78 FE 7F FD 81 9B CB 4A 1C 03 A8
BB 15 99 25 96 07 65 D1 C9 E3 E5 3F BD CE 02 6A A6 C6 FF 20 74 A8 24 70 77 C6 15
2C 97 F7 3D 38 62 CA 4A 87 CB FD E7 3E 34 CE AD 8B 90 E2 87 33 F8 C4 A5 F0 2A 4D
6D A0 41 59 DF AC 3F 62 E6 A7 7A 01 17 28 73 57 32 E1 B6 92 89 CD BA E4 B8 96 B8
49 78 13 5F 80 5F 89 A0 0C 66 E7 99 97 C3 DB C7 34 59 59 9E 54 EA 27 C7 DF 0E 03
CF 54 74 21 7A 2E C5 42 98 8F E3 A3 E4 D9 E6 78 29 39 B8 7E F4 89 02 14 B2 7B E1
2C 33 71 FD F2 1E A8 F1 6F 84 10 21 FD 44 25 A7 1F 12 AB 29 AB FF F5 00 BE 40

回复：02 0B 01 05 41 22 01 01 00 30 30 30 30 32 32 32 32 33 33 33 33 34 34 34 34
31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 31 31 31 31 32 32 32 32 33 33 33
33 34 34 34 34 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 31 31 31 31 32 32
32 32 33 33 33 33 34 34 34 34 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 31
31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 31 31 31 31 32 32 32 32 33 33 33 33
34 34 34 34 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 31 31 31 31 32 32 32
32 33 33 33 33 34 34 34 34 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 31 31
31 31 32 32 32 32 33 33 33 33 34 34 34 34 31 31 31 31 32 32 32 32 33 33 33 33 34
34 34 34 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 31 31 31 31 32 32 32 32
33 33 33 33 34 34 34 34 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 6C 40

5.13 SM2在线加密(41 25)

命令使用传入的密钥和明文数据进行加密运算并返回加密结果。传入的密钥不会保存，计算完成后自动销毁。

5.13.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x25
名称	长度（字节）	说明
算法类型	1	0x02
密钥 ID	1	0x00(固定值)
密钥	64	公钥 X+公钥 Y
要加密的数据	-	要加密的数据

5.13.2 响应数据

数据域	值(HEX)
TYPE	0x41
CMD	0x25
状态码	见下表
长度（2 字节）	加密结果数据长度
加密结果	加密结果

5.13.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.13.4 示例

使用 SM2 算法加密数据：

02 0A 00 56 41 25 00 52 02 00 4E D1 30 6F 43 87 2D 64 90 70 64 24 42 00 5E A3 C1 75 8E 32 C3 87 66 D9 46 B3 D7 B2 2B 2B BF 32 BD 97 AE 97 7F 5C D0 E8 FD 50 E8 40 34 0A AB A8 95 74 40 4F D8 B0 96 A1 81 05 A3 9D 73 76 3B B8 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 69 40

回复：02 0A 00 75 41 25 01 00 70 2F 9C EB 2C 59 7C 85 3C 61 D1 02 2D 36 1D 27 79 B2 BC BE 9F 83 5D AA 46 BD 23 FD 7F DC 4F 93 E7 FE 02 E0 89 61 FF 82 FA 4D D4 80 9A 2C 8F A3 86 17 0D D5 DE 54 07 FF B1 CE 23 66 25 69 31 55 48 A4 B4 11 C1 51 FE 38 81 DE 31 85 18 4C B9 66 B3 B6 D3 30 FC F3 D7 BE 50 0A 88 32 B5 D5 E4 3C B3 CB 3A 63 AC 33 99 56 CF AA 22 66 CD DA 4B D2 D2 FC 40

同一组密钥和数据，每次的加密结果是不同的。

5.14 SM2在线解密(41 26)

命令使用传入的密钥和密文数据进行解密运算并返回解密后的数据。传入的密钥不会保存，计算完成后自动销毁。

5.14.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x26
名称	长度（字节）	说明
算法类型	1	0x02
密钥 ID	1	0x00(固定值)
密钥	32	私钥 D
要解密的数据	-	要解密的数据

5.14.2 响应数据

数据域	值(HEX)
TYPE	0x41
CMD	0x26
状态码	见下表
长度（2 字节）	解密结果数据长度
解密结果	解密结果

5.14.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.14.4 示例

使用 SM2 算法解密数据：

02 0B 00 96 41 26 00 92 02 00 19 89 71 63 AE AE EC FF D2 E4 0D BE C7 AA 29 62 28 29 5F 4A 99 9F D5 0D A2 09 7F CB A9 1F 7D FE 2F 9C EB 2C 59 7C 85 3C 61 D1 02 2D 36 1D 27 79 B2 BC BE 9F 83 5D AA 46 BD 23 FD 7F DC 4F 93 E7 FE 02 E0 89 61 FF 82 FA 4D D4 80 9A 2C 8F A3 86 17 0D D5 DE 54 07 FF B1 CE 23 66 25 69 31 55 48 A4 B4 11 C1 51 FE 38 81 DE 31 85 18 4C B9 66 B3 B6 D3 30 FC F3 D7 BE 50 0A 88 32 B5 D5 E4 3C B3 CB 3A 63 AC 33 99 56 CF AA 22 66 CD DA 4B D2 D2 2E 40

回复：02 0B 00 15 41 26 01 00 10 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 68 40

5.15 计算签名值(41 51)

计算签名值。

5.15.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x51
Len(2Bytes)		指令数据长度，高字节在前，低字节在后
名称	长度(字节)	说明
算法类型	1	SM2： 0x02 RSA1024： 0x11 RSA2048： 0x12
密钥 ID	1	密钥 ID，1~8
*UserIDLen	2	UesrID 的长度，仅 SM2 时存在
*UserID	最大 512	UserID 的数据，仅 SM2 时存在
MessageLen	2	要签名数据的长度
Message	最大 1024	要签名的数据(最大 1024 字节)

5.15.2 响应数据

数据域	值(HEX)
TYPE	0x41
CMD	0x51
状态码	见下表
长度（2 字节）	签名结果数据长度
签名结果	签名结果,SM2 为 64 字节,RSA1024 为 128 字节，RSA2048 为 256 字节

5.15.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.15.4 示例

使用 ID 是 5 的 SM2 密钥，计算 SM2 签名值：

02 0E 00 3A 41 51 00 36 02 05 00 10 31 32 33 34 35 36 37 38 31 32 33 34 35 36 37 38 00 20 0A 85 63 A6 4A 9C 8B 24 C5 AD 21 5E C8 8C 33 44 EE 54 2C AC EF E9 EB 11 4C F7 5C 0C C2 08 A9 7A 06 40

UserID 是 31 32 33 34 35 36 37 38 31 32 33 34 35 36 37 38

回复：

```
02 0E 00 45 41 51 01 00 40 95 C6 7D 45 23 A8 72 37 9D A1 7F 6C 98 73 7F 57 BC B0
FC AA CE 23 45 20 0B 7D F0 47 A0 D3 CD EE 8E 78 0F FA 4E F1 89 AB 73 96 2A DE B2
55 40 87 A8 86 88 E2 CB 67 D2 53 04 4F F7 1B 90 69 D7 78 27 40
```

每次签名结果不一致。

使用 ID 是 2 的 RSA 密钥，计算 RSA2048 签名值：

```
02 0E 01 08 41 51 01 04 12 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 12 34 56 78 90 9B 40
```

回复：

```
02 0E 01 05 41 51 01 01 00 4C 9A 9A 0D 1D DB 60 A9 89 39 BF 96 63 EE 83 8D E6 DC
82 FE 55 3F 14 C6 FC D3 5D 19 5E 88 AD 9B 78 42 9C 51 5A 65 4D 05 B0 BE E5 EC AB
F1 CA 02 AA 74 77 C2 C9 C6 81 16 15 B0 C1 38 3D 34 38 51 2B D2 88 58 94 09 CB 36
B0 A4 29 3E 0F CD E8 3B D3 DA 1C CB E1 1C 70 78 13 AE 34 EA FF 31 ED BE 6D E8 C0
79 5D 17 37 1C 20 14 E7 E7 D6 3E 88 D5 E6 5A 2E 7E 1B 09 0B 96 5E C8 D0 DF CC FD
E5 F8 16 4E A8 9E 41 2E 1C 9C 1D 0E 73 CD D9 55 4A 1B F6 F9 07 1E FC 60 26 E7 06
17 FB 7C E3 8D AC 76 AE 18 42 80 BF C5 2C 80 FE 80 0A 8A 99 D0 AF 4A E1 82 1F FD
50 AC 90 76 FC BA 6B 69 6C FC DE F0 BF B5 C1 99 69 37 E7 B8 DD 8C 49 12 3B 76 85
5D 11 09 18 9C F0 20 80 59 01 C8 C5 41 DF 33 48 03 42 59 75 42 1D 95 81 7E E8 35
B3 37 1B B6 A4 C2 D3 C6 7E 0E 31 94 3D CA 49 28 C9 71 21 0B 25 71 86 40
```

5.16 验证签名值(41 52)

验证签名值。

5.16.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x52
Len(2Bytes)		指令数据长度，高字节在前，低字节在后
名称	长度（字节）	说明
算法类型	1	SM2:　　0x02 RSA1024:　0x11 RSA2048:　0x12
密钥 ID	1	密钥 ID，1~8
*UserIDLen	2	UesrID 的长度，仅 SM2 时存在

*UserID	最大 512	UserID 的数据，仅 SM2 时存在
MessageLen	2	要签名数据的长度
Message	最大 1024	要签名的数据(最大 1024 字节)
计算签名得到的签名值	最大 256	计算签名得到的签名值，SM2 为 64 字节，RSA1024 为 128 字节，RSA2048 为 256 字节

5.16.2 响应数据

数据域	值(HEX)
TYPE	0x41
CMD	0x52
状态码	见下表
长度（2 字节）	验签结果数据长度
验签结果	验签正确：01 验签错误：02

5.16.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.16.4 示例

SM2 验签：

02 0F 00 7A 41 52 00 76 02 05 00 10 31 32 33 34 35 36 37 38 31 32 33 34 35 36 37 38 00 20 0A 85 63 A6 4A 9C 8B 24 C5 AD 21 5E C8 8C 33 44 EE 54 2C AC EF E9 EB 11 4C F7 5C 0C C2 08 A9 7A 95 C6 7D 45 23 A8 72 37 9D A1 7F 6C 98 73 7F 57 BC B0 FC AA CE 23 45 20 0B 7D F0 47 A0 D3 CD EE 8E 78 0F FA 4E F1 89 AB 73 96 2A DE B2 55 40 87 A8 86 88 E2 CB 67 D2 53 04 4F F7 1B 90 69 D7 78 39 40

回复：

02 0F 00 06 41 52 01 00 01 01 1B 40

RSA2048 验签：

02 0F 02 18 41 52 02 14 12 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 12 34 56 78 90 21 AD

F6 A5 3B DF 9E 4F 34 F7 36 91 EA 94 A2 1D 56 D3 87 3C 8D 61 D0 94 0D F5 3B 0D 23
D4 75 2D 5E C1 9B C1 02 A2 82 5E E6 4E D7 19 B6 FA D9 56 8B 21 8A A0 0F 11 97 66
F0 CB 42 83 1A C8 B7 BF C6 2A 2E 1F C8 E8 6E 40 99 72 30 8A DE 85 DA 34 9F B8 5D
32 B4 04 A9 3C D0 C0 CF 1E 8A A0 91 55 61 6B 72 DC 77 B1 27 20 03 71 B5 64 39 32
C2 82 A4 A9 47 CC 61 25 B2 22 7C 93 B3 66 CA B0 0C 5A 11 23 1A 06 EF DC 9C 43 DF
B0 9C 58 1F 13 0D AC F6 6F F2 3F E7 E8 6F 4F F1 CC 7C A9 52 27 9A 89 5B 8A 69 C0
D4 58 1F 78 39 93 F6 9A 22 9F 09 25 F5 13 30 2B 6D 31 AC 7C 46 4D FC E8 06 52 5D
8A 03 2B 30 FF 06 1C F7 5B E7 5A EB 17 57 C1 CB BB 75 FF BF 84 24 BC B0 4F 50 E4
BC FF 8A AE D4 FA BE 0F C9 43 90 95 E2 69 A0 0C 23 AB 53 BE E9 FF 13 EF A8 4B 7F
A7 D0 73 06 DC 11 F5 38 D4 84 92 C2 40

回复：

02 0F 00 06 41 52 01 00 01 01 1B 40

5.17 SM2在线签名(41 55)

命令传入密钥、UserID、Message 等参数，计算并返回签名值。传入的密钥等参数不会保存，计算完成后自动销毁。

5.17.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x55
Len(2Bytes)		指令数据长度，高字节在前，低字节在后
名称	长度(字节)	说明
算法类型	1	02(SM2)
密钥 ID	1	00(固定值)
密钥	96	私钥 D+公钥 X+公钥 Y
UserIDLen	2	UserID 的长度
UserID	512	UserID 数据，最大支持 512 字节
MessageLen	2	要签名数据的长度
Message	最大 1024	要签名的数据(最大 1024 字节)

5.17.2 响应数据

数据域	值(HEX)
TYPE	0x41
CMD	0x55
状态码	见下表
长度（2 字节）	签名结果数据长度
签名结果	固定 64 字节

5.17.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.17.4 示例

SM2 在线签名：

02 0E 00 9A 41 55 00 96 02 00 19 89 71 63 AE AE EC FF D2 E4 0D BE C7 AA 29 62 28
29 5F 4A 99 9F D5 0D A2 09 7F CB A9 1F 7D FE 4E D1 30 6F 43 87 2D 64 90 70 64 24
42 00 5E A3 C1 75 8E 32 C3 87 66 D9 46 B3 D7 B2 2B 2B BF 32 BD 97 AE 97 7F 5C D0
E8 FD 50 E8 40 34 0A AB A8 95 74 40 4F D8 B0 96 A1 81 05 A3 9D 73 76 3B B8 00 10
31 32 33 34 35 36 37 38 31 32 33 34 35 36 37 38 00 20 0A 85 63 A6 4A 9C 8B 24 C5
AD 21 5E C8 8C 33 44 EE 54 2C AC EF E9 EB 11 4C F7 5C 0C C2 08 A9 7A D4 40

回复：

02 0E 00 45 41 55 01 00 40 2A 3A 50 A1 34 D6 84 5E 85 4C 9A D0 69 75 3D 08 67 A6
85 98 4A 7F EB E6 1E EE 11 64 2E 81 34 4C 70 9E 94 3A 4A C6 A5 20 8E 4C 9C 91 28
2D AE 43 EE 88 08 4D 86 7A 6F AB 04 C8 88 10 B1 41 88 4E CC 40

同一组密钥和数据，每次的签名结果是不同的。

5.18 SM2在线验签(41 56)

命令传入公钥、UserID、Message、签名值等参数，验证签名值并返回结果。传入的公钥等参数不会保存，计算完成后自动销毁。

5.18.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x56
Len(2Bytes)		指令数据长度，高字节在前，低字节在后
名称	长度（字节）	说明
算法类型	1	02(SM2)
密钥 ID	1	00(固定值)
密钥	64	公钥 X+公钥 Y
UserIDLen	2	UserID 长度
UserID	512	UserID 数据，最大支持 512 字节
MessageLen	2	签名数据的长度
Message	最大 1024	签名的数据(最大 1024 字节)
签名值	64	待验证的签名值

5.18.2 响应数据

数据域	值(HEX)

TYPE	0x41
CMD	0x56
状态码	见下表
长度（2 字节）	验签结果数据长度
验签结果	验签正确：01 验签错误：02

5.18.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.18.4 示例

SM2 在线验签：

02 0F 00 BA 41 56 00 B6 02 00 4E D1 30 6F 43 87 2D 64 90 70 64 24 42 00 5E A3 C1
75 8E 32 C3 87 66 D9 46 B3 D7 B2 2B 2B BF 32 BD 97 AE 97 7F 5C D0 E8 FD 50 E8 40
34 0A AB A8 95 74 40 4F D8 B0 96 A1 81 05 A3 9D 73 76 3B B8 00 10 31 32 33 34 35
36 37 38 31 32 33 34 35 36 37 38 00 20 0A 85 63 A6 4A 9C 8B 24 C5 AD 21 5E C8 8C
33 44 EE 54 2C AC EF E9 EB 11 4C F7 5C 0C C2 08 A9 7A 2A 3A 50 A1 34 D6 84 5E 85
4C 9A D0 69 75 3D 08 67 A6 85 98 4A 7F EB E6 1E EE 11 64 2E 81 34 4C 70 9E 94 3A
4A C6 A5 20 8E 4C 9C 91 28 2D AE 43 EE 88 08 4D 86 7A 6F AB 04 C8 88 10 B1 41 88
4E D6 40

回复：

02 0F 00 06 41 56 01 00 01 01 1F 40

5.19 计算MAC值(41 61)

计算 MAC 值。

5.19.1 命令格式

数据域		值(HEX)
TYPE		0x41
CMD		0x61
名称	长度（字节）	说明
密钥 ID	1	SM4 密钥 ID，1~8
IV 值	16	IV 值
要计算 MAC 值的数据	-	要计算 MAC 值的数据

5.19.2 响应数据

数据域	值(HEX)
TYPE	0x41
CMD	0x61
状态码	见下表
长度（2 字节）	计算的 MAC 值数据长度
计算的 MAC 值	计算的 MAC 值

5.19.3 状态码

STA	说明
0x62	指令参数错误
0x01	指令执行成功

5.19.4 示例

指令：

02 10 00 29 41 61 00 25 04 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 65 45 12 34 3E 40

回复：02 10 00 15 41 61 01 00 10 93 D5 2F C0 00 A6 2F D1 E6 3B C4 82 FD 5B A9 F4 A5 40

6 根密钥指令详解(21)

6.1 支持机型

如下机型支持本章接口：MH1721 QFN16

6.2 导入根密钥(21 01)

导入根密钥。防拆功能开启后，拆机时硬件会自动清除此根密钥数据。

6.2.1 命令格式

数据域		值(HEX)
TYPE		0x21
CMD		0x01
名称	长度	说明
根密钥数据	最大 64 字节	导入根密钥，最大长度 64 字节，写入长度为 4 的整数倍

6.2.2 响应数据

无

6.2.3 状态码

STA	说明
0x22	写操作失败

6.2.4 示例

导入根密钥 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34
指令：
02 01 00 14 21 01 00 10 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 25 40
回复：02 01 00 05 21 01 01 00 00 25 40

6.3 读根密钥(21 02)

读根密钥。

6.3.1 命令格式

数据域		值(HEX)
TYPE		0x21
CMD		0x02
名称	长度	说明

数据长度	2 字节	需要获取根密钥的字节数，最大 64 字节

6.3.2 响应数据

序号	长度	说明
1	最大 64	读取根密钥数据，最大 64 字节

6.3.3 状态码

STA	说明
0x21	读操作失败

6.3.4 示例

读 16 字节根密钥数据指令：
02 02 00 06 21 02 00 02 00 10 35 40
回复：02 02 00 15 21 02 01 00 10 31 31 31 31 32 32 32 32 33 33 33 33 34 34 34 34 25 40

6.4 清除根密钥数据(21 03)

清除根密钥数据。

6.4.1 命令格式

数据域	值(HEX)
TYPE	0x21
CMD	0x03

6.4.2 响应数据

无

6.4.3 状态码

STA	说明
0x62	指令参数错误

6.4.4 示例

指令：02 03 00 04 21 03 00 00 25 40
回复：02 03 00 05 21 03 01 00 00 25 40

7　防拆模块指令详解(31)

7.1 支持机型

有如下机型支持本章接口：MH1721 QFN16

7.2 使用流程

1. 先发送“配置静态低/高电平触发模式”指令配置对应的防拆管脚为高电平触发或者低电平触发，然后发送“开启防拆检测”指令即可开启防拆，或者直接发送“配置并开启外部防拆”设置并打开防拆。

2. 发送“查询攻击状态”指令查询是否有防拆管脚触发，防拆管脚触发后芯片硬件电路会清除根密钥数据；

7.3 配置并开启外部防拆 (31 01)

配置外部防拆模块并开启防拆检测。

7.3.1 命令格式

数据域		值(HEX)
TYPE		0x31
CMD		0x01
序号	长度	说明
1	4	配置并开启指定 Tamper 防拆端口触发模式；每两个 bit 位对应一路防拆配置， 如 bit0-bit1 为第一路，bit2-bit3 为第二路，…. Bit 值定义 00：不使能 01：使能动态防拆 1x:　使用为静态防拆，如果此路防拆支持两种电平触发，则 10 为低电平触发，11 为高电平触发，如果此路防拆只有一种触发电平，则 10 和 11 都为开启静态防拆 Bitmap b0-b1：ext_s0 开启使能位 b2-b3：ext_s1 开启使能位 b4-b5：ext_s2 开启使能位 …

		B22-b23：ext_s11 开启使能位 rsvd[b31:b24]
注		此指令也可以通过 31.02 +31.04 两个指令或者 31.03 +31.04 两指令分步执行，结果一样 MH 1721 只有 4 路外部防拆传感器（最多 2 路动态或者 4 路静态），即只要设置 b0-b7 共 8 个位

7.3.2 响应数据

无

7.3.3 状态码

STA	说明
0x11	模块打开失败
0x72	传入的 tamper 端口号无效

7.3.4 示例

指令：02 01 00 08 31 04 00 04 00 00 00 0F 37 40（开启 0~3 路防拆）
回复：02 01 00 05 31 04 01 00 00 30 40

7.4 配置静态触发模式(31 02)

配置指定 Tamper 为静态触发模式。

7.4.1 命令格式

数据域		值(HEX)
TYPE		0x31
CMD		0x02
序号	长度	说明
1	2	配置指定端口为静态模式并指定触发攻击电平 Bit 值定义 0：低电平攻击 1：高电平攻击 Bitmap b0：ext_s0 静态电平攻击类型 b1：ext_s1 静态电平攻击类型 b2：ext_s2 静态电平攻击类型 … b11：ext_s11 静态电平攻击类型 rsvd[b15:b12]

		如该端口只有一种静态攻击电平，则对应 bit 位的值为 0 和 1 时都是指把该端口设置成静态触发模式
注		MH 1721 只有 4 路外部防拆传感器（最多 2 路动态或者 4 路静态），即只要设置 b0-b3 共 4 个位

7.4.2 响应数据

无

7.4.3 状态码

STA	说明
0x62	指令参数错误
0x72	传入的 tamper 端口号无效

7.4.4 示例

指令：02 02 00 06 31 02 00 02 00 03 36 40 (配置 ext_s0 和 1 高电平触发)
回复：02 02 00 05 31 02 01 00 00 35 40

7.5 配置动态模式(31 03)

配置指定 Tamper 为动态模式。

7.5.1 命令格式

数据域		值(HEX)
TYPE		0x31
CMD		0x03
序号	长度	说明
1	2	配置指定 Tamper 为动态模式 Bit 值定义 0：不使能 1：使能 Bitmap b0：ext_s0 动态传感器模式 b1：ext_s1 动态传感器模式 b2：ext_s2 动态传感器模式 … b11：ext_s11 动态传感器模式 rsvd[b15:b12]
注		MH 1721 只有 4 路外部防拆传感器（最多 2 路动

	态或者 4 路静态），即只要设置 b0-b3 共 4 个位

7.5.2 响应数据

无

7.5.3 状态码

STA	说明
0x62	参数无效
0x71	动态模式引脚非成对

7.5.4 示例

指令：02 03 00 06 31 03 00 02 00 03 36 40 (ext_s0 和 1 动态传感器模式)
回复：02 03 00 05 31 03 01 00 00 35 40

7.6 开启或者关闭防拆检测(31 04)

开启防拆检测功能。

7.6.1 命令格式

数据域		值(HEX)
TYPE		0x31
CMD		0x04
序号	长度	说明
1	2	开启指定防拆端口； Bit 值定义 0：不使能 1：使能 Bitmap b0：ext_s0 开启使能位 b1：ext_s1 开启使能位 b2：ext_s2 开启使能位 … b11：ext_s11 开启使能位 rsvd[b15:b12]
注		MH 1721 只有 4 路外部防拆传感器（最多 2 路动态或者 4 路静态），即只要设置 b0-b3 共 4 个位

7.6.2 响应数据

无

7.6.3 状态码

STA	说明
0x11	模块打开失败
0x72	传入的 tamper 端口号无效

7.6.4 示例

指令：02 04 00 06 31 04 00 02 00 0F 3A 40（开启 0~3 路防拆）
回复：02 04 00 05 31 04 01 00 00 35 40

7.7 查询攻击状态(31 06)

查询攻击状态寄存器。

7.7.1 命令格式

数据域	值(HEX)
TYPE	0x31
CMD	0x06

7.7.2 响应数据

序号	长度	说明
1	3	获取的攻击状态记录 Bit 值定义 0：无攻击 1：有攻击 Bitmap b0：ext_s0 攻击中断状态位 b1：ext_s1 攻击中断状态 b2：ext_s2 攻击中断状态 … b11：ext_s11 攻击中断状态 b12：高电压攻击中断状态位 b13：低电压攻击中断状态位 b14：高温攻击中断状态位 b15：低温压攻击中断状态位 b16：电压毛刺检测中断状态位 b17：32K 时钟频率检测中断状态位 b18：Mesh 攻击中断状态位

		rsvd[b19] b20：SSC 攻击中断状态位 rsvd[b23:b21]

7.7.3 状态码

STA	说明
0x63	数据域长度错误

7.7.4 示例

指令：02 06 00 04 31 06 00 00 35 40
回复：02 06 00 08 31 06 01 00 03 00 00 03 38 40（ext_s0 和 ext_s1 触发）

7.8 清除攻击状态(31 07)

清除攻击状态值。

7.8.1 命令格式

数据域	值(HEX)
TYPE	0x31
CMD	0x07

7.8.2 响应数据

无

7.8.3 状态码

STA	说明
0x63	数据域长度错误

7.8.4 示例

指令：02 07 00 04 31 07 00 00 35 40
回复：02 07 00 05 31 07 01 00 00 35 40

7.9 配置端口拉电阻使能(31 08)

配置指定 Tamper 端口内部拉电阻使能。

7.9.1 命令格式

数据域	值(HEX)
TYPE	0x31

CMD		0x08
序号	长度	说明
1	2	配置对应端口号的内部拉电阻使能； Bit 值定义 0：拉电阻不使能 1：拉电阻使能 Bitmap b0：ext_s0 拉电阻使能 b1：ext_s1 拉电阻使能 b2：ext_s2 拉电阻使能 … b11：ext_s11 拉电阻使能 rsvd[b15:b12]
注		MH1721 只有 4 路外部防拆传感器（最多 2 路动态或者 4 路静态），即只要设置 b0-b3 共 4 个位

7.9.2 响应数据

无

7.9.3 状态码

STA	说明
0x62	指令参数错误
0x72	传入的 tamper 端口号无效

7.9.4 示例

指令：02 08 00 06 31 08 00 02 00 0F 3A 40 （开启 ext_s0 到 ext_s4 的上拉/下拉）
回复：02 08 00 05 31 08 01 00 00 35 40

7.10 开启或者关闭内部传感器(31 09)

开启/关闭指定的内部传感器。

7.10.1 命令格式

数据域		值(HEX)
TYPE		0x31
CMD		0x09
序号	长度	说明
1	1	配置指定的内部传感器开启 Bit 值定义 0：不使能

		1：使能 Bitmap b0：高电压传感器开启 b1：低电压传感器开启 b2：高温传感器开启 b3：低温传感器开启 b4：32K 频率传感器开启 b5：Mesh 传感器开启 b6：电压毛刺传感器开启 revd[b7]
注		MH1721 只有 4 路内部传感器（b0：高电压传感器、b1：低电压传感器、b4：32K 频率传感器、b6：电压毛刺传感器）

7.10.2 响应数据

无

7.10.3 状态码

STA	说明
0x62	参数无效

7.10.4 示例

指令：02 09 00 05 31 09 00 01 0F 3A 40（开启高低压，高低温传感器）
回复：02 09 00 05 31 09 01 00 00 35 40

7.11 查询内部传感器开启状态(31 0B)

查询内部 sensor 的状态是开启或者关闭。

7.11.1 命令格式

数据域	值(HEX)
TYPE	0x31
CMD	0x0B

7.11.2 响应数据

数据域		值(HEX)
TYPE		0x21
CMD		0x0B
序号	长度	说明

1	1	Bit 值定义 0：关闭 1：开启 Bitmap b0：高电压传感器开启状态 b1：低电压传感器开启状态 b2：高温传感器开启状态 b3：低温传感器开启状态 b4：32K 频率传感器开启 b5：Mesh 传感器开启 b6：电压毛刺传感器开启 revd[b7]
注		MH1721 只有 4 路内部传感器（b0：高电压传感器、b1：低电压传感器、b4：32K 频率传感器、b6：电压毛刺传感器）

7.11.3 状态码

STA	说明
0x62	参数无效