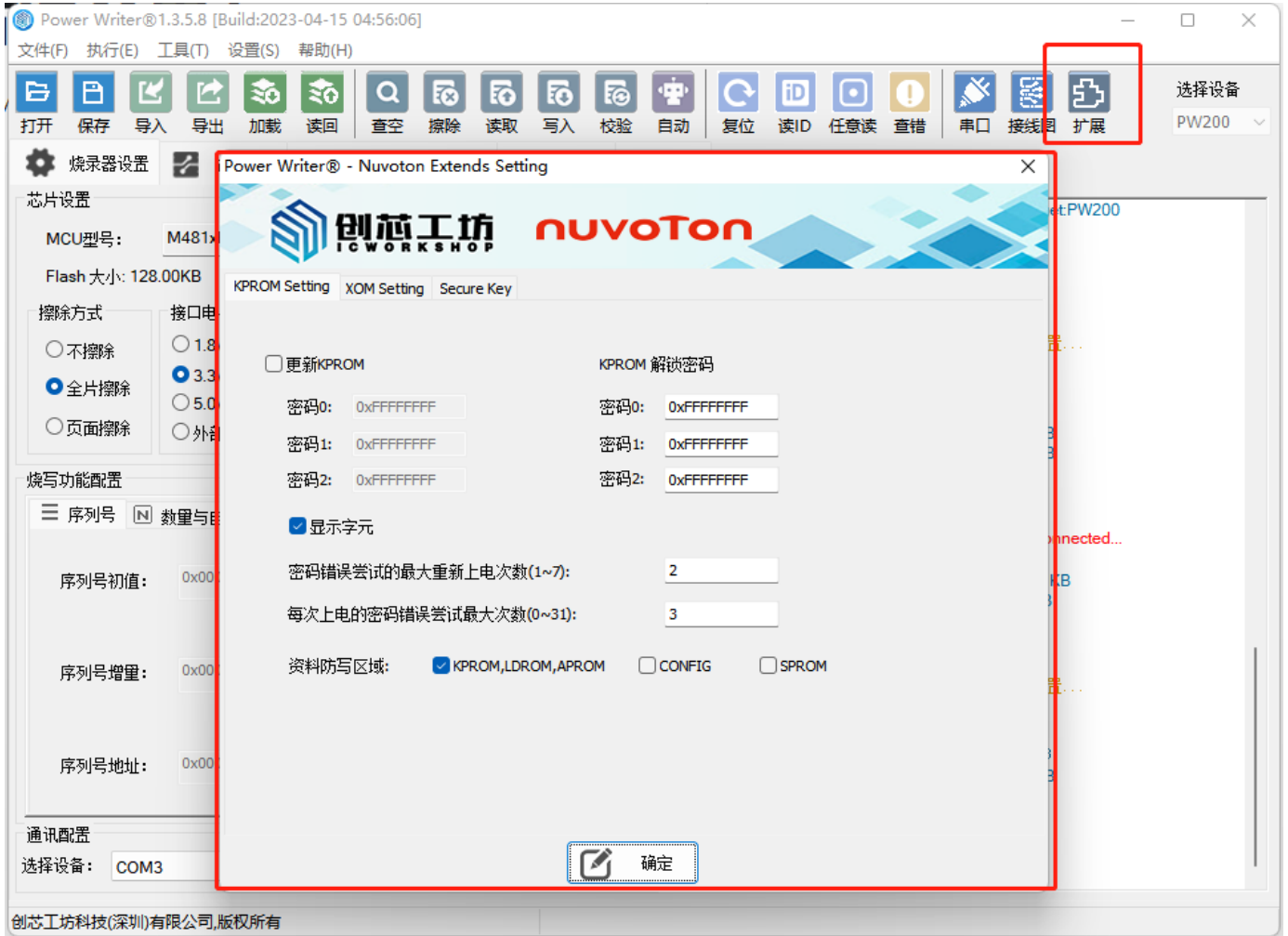
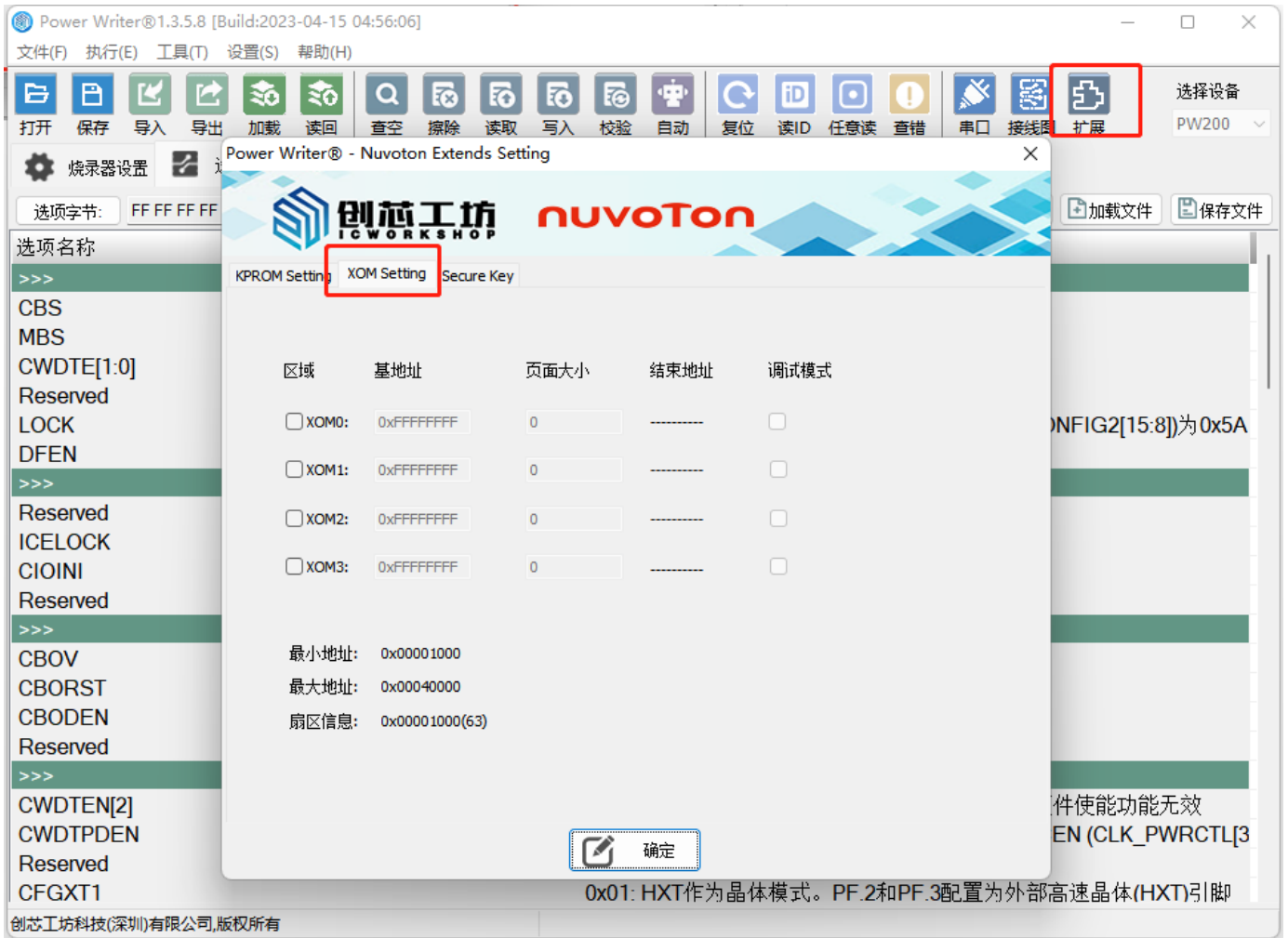


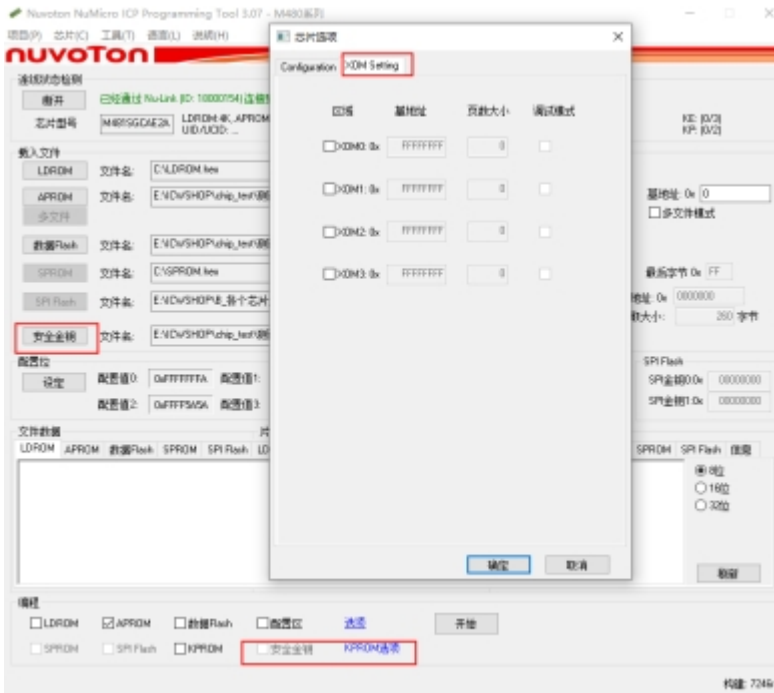
# 3.2.9: Nuvoton芯片怎么用?

由于新唐芯片有一些特殊的功能, 例如M481xG具有KPROM,XOM,安全密钥等功能, PowerWriter软件将其放在扩展设置里





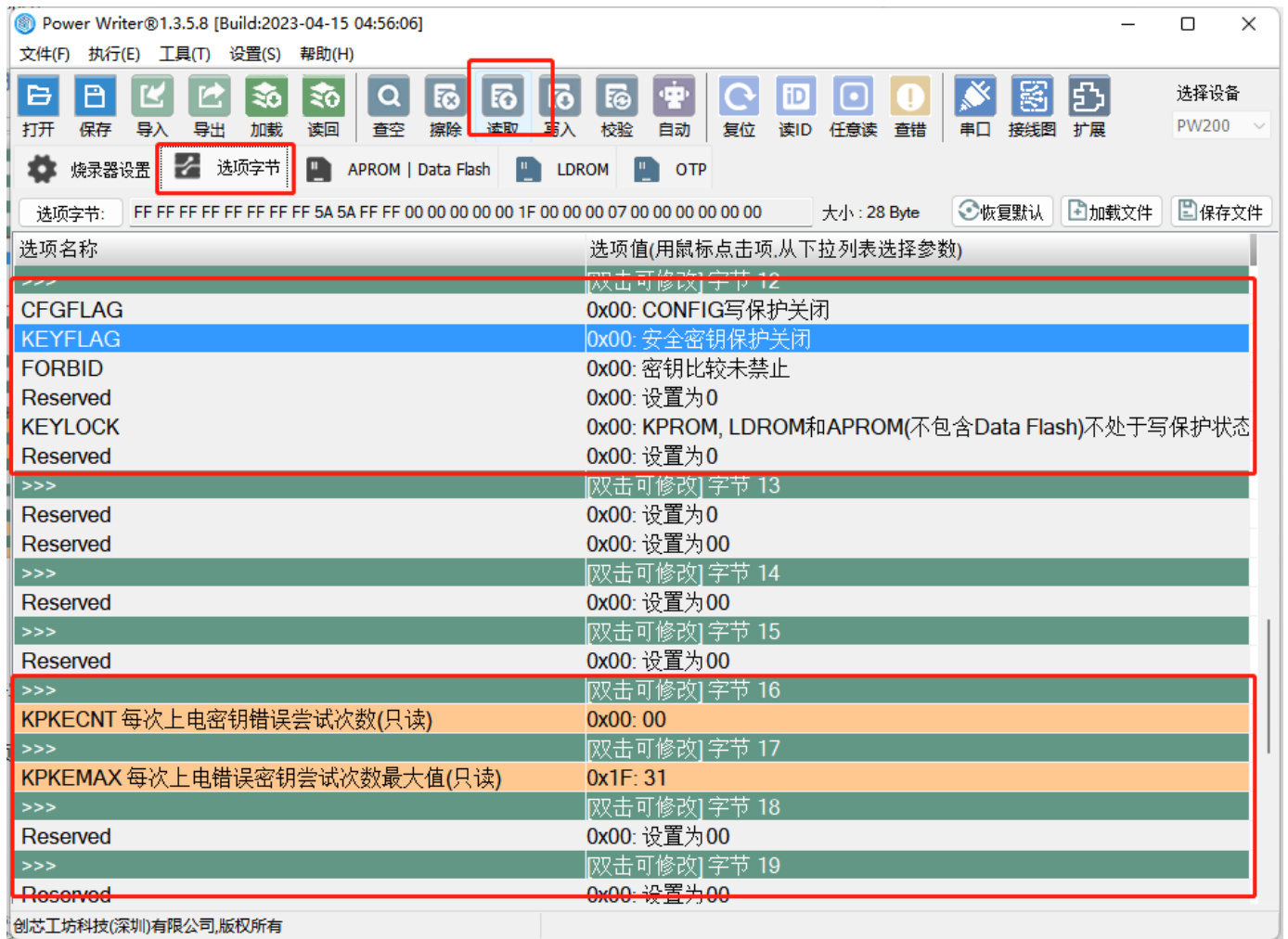
对应新唐工具:



## KPROM设置

# KPROM 状态读取

连接芯片，读取选项字节，可以获取KPROM的状态



# KPROM解锁密码设置

当安全密钥保护使能后,LDROM和APROM处于写保护状态，如果想对其进行写操作，必须输入正确的 KPROM解锁密码，否则会报错

当选项字节CONFIG写保护开启并且要写入选项字节时，KPROM解锁密码输入错误则会触发全片擦除

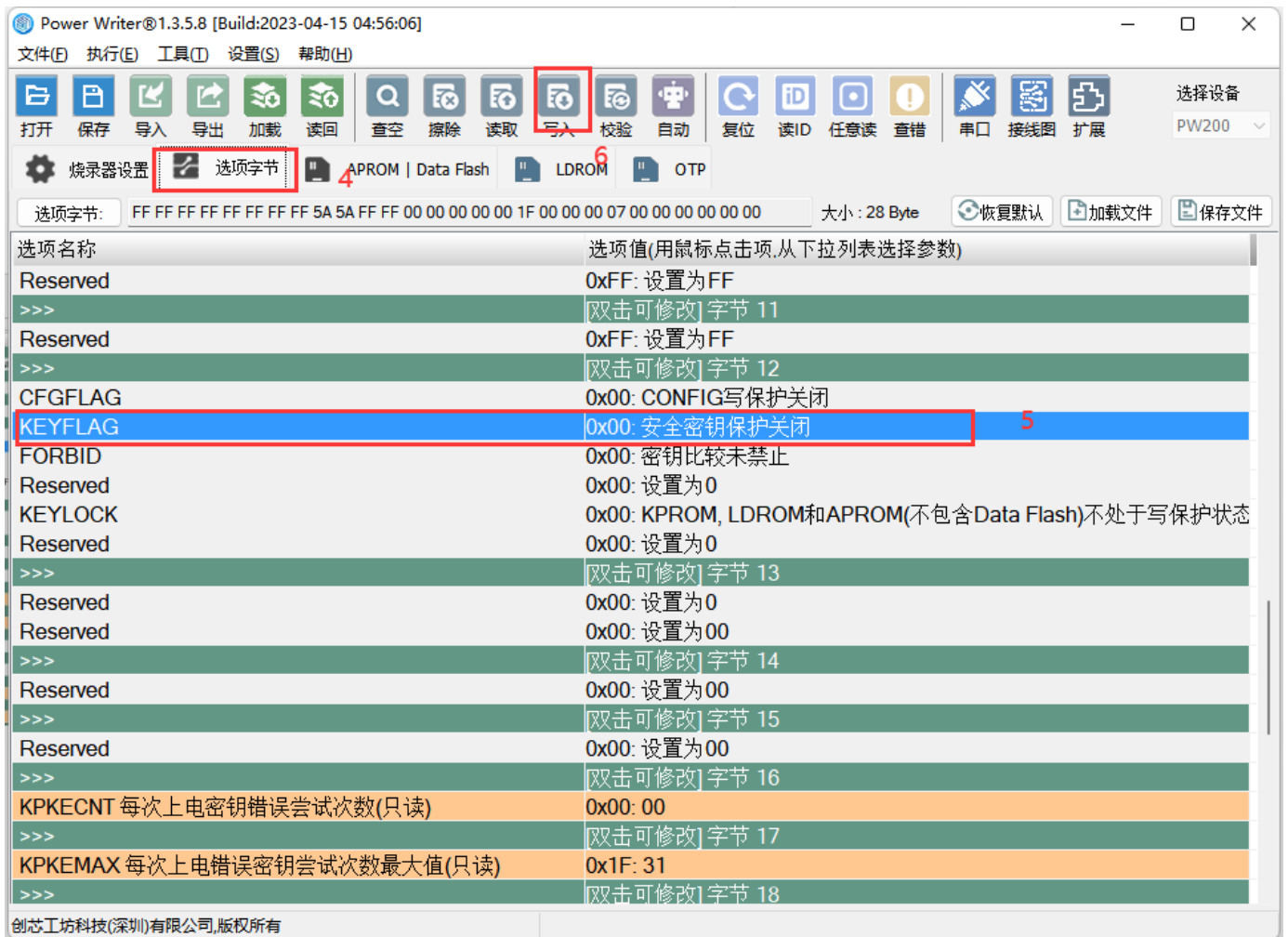


```
2/06-16:08:00:246> M481xG Flash 大小: 256.00KB
2/06-16:08:00:247> M481xG Data Flash size: 4.00 KB
2/06-16:08:00:251> M481xG LDROM size: 4.00 KB
2/06-16:08:00:253> M481xG OTP size: 3.00 KB
2/06-16:08:00:484> Change bank: Single bank
2/06-16:08:00:667> 更新烧录器设置完成...
2/06-16:08:00:907> 更新芯片信息成功...
2/06-16:08:02:086> 目标芯片已连接...
2/06-16:08:02:143> 选项字节已经成功读取!
2/06-16:15:19:923> 更新烧录器设置完成...
2/06-16:15:20:166> 更新芯片信息成功...
2/06-16:15:24:323> [003E] Target KPROM password error...
```

## 更新KPROM密码

当要更新KPROM时，必须同时勾选更新KPROM和安全密钥使能，KPROM是与选项字节一起写入，点击写入选项字节时会操作KPROM；

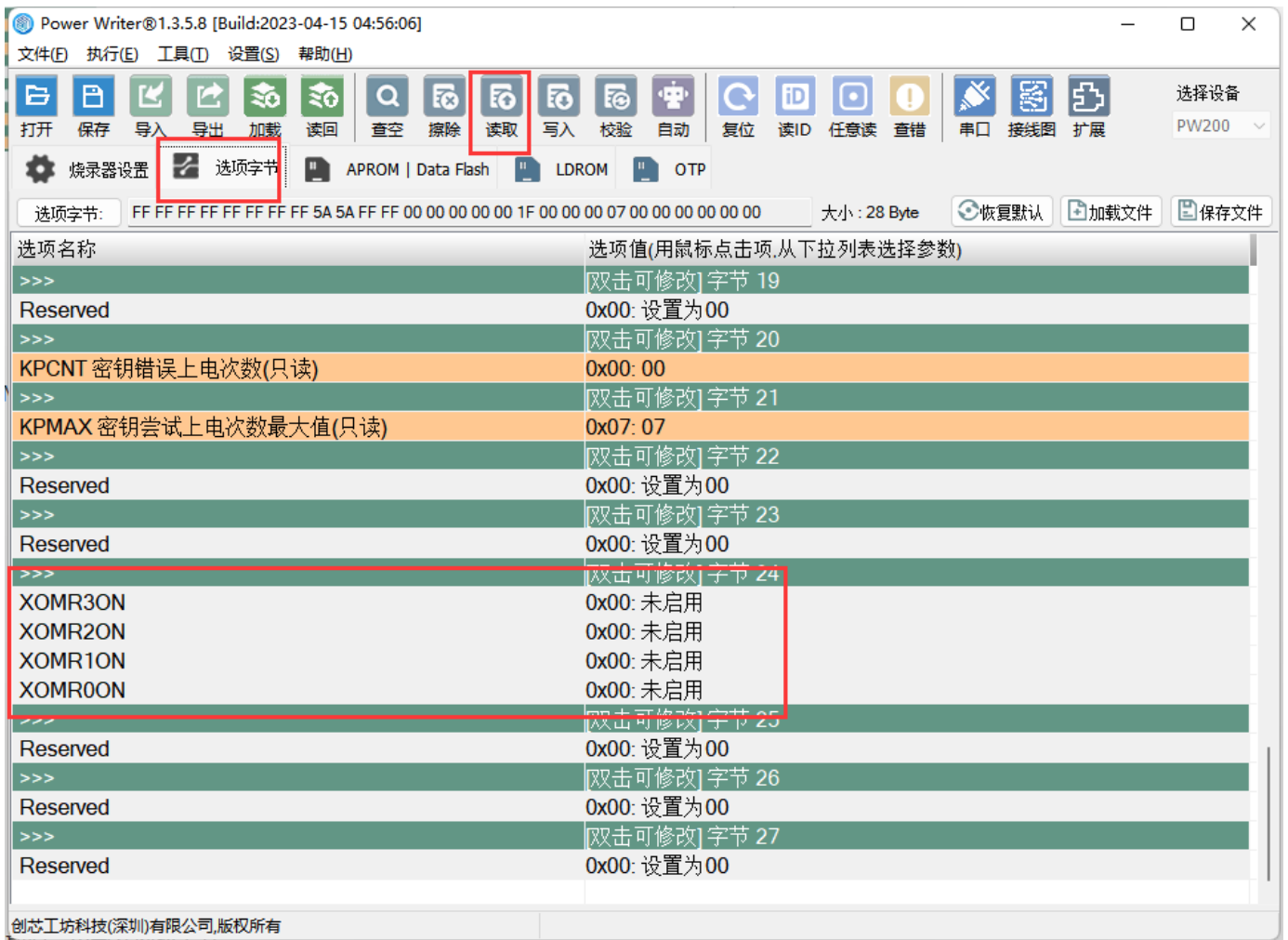




# XOM设置

## XOM 状态读取

选择对应的芯片型号，连接芯片，读取选项字节，可以获取XOM的激活状态：



## XOM 配置写入

填写要读保护的地址, 必须同时勾选使能区域和XOM区域启用, 最后点击写入选项字节

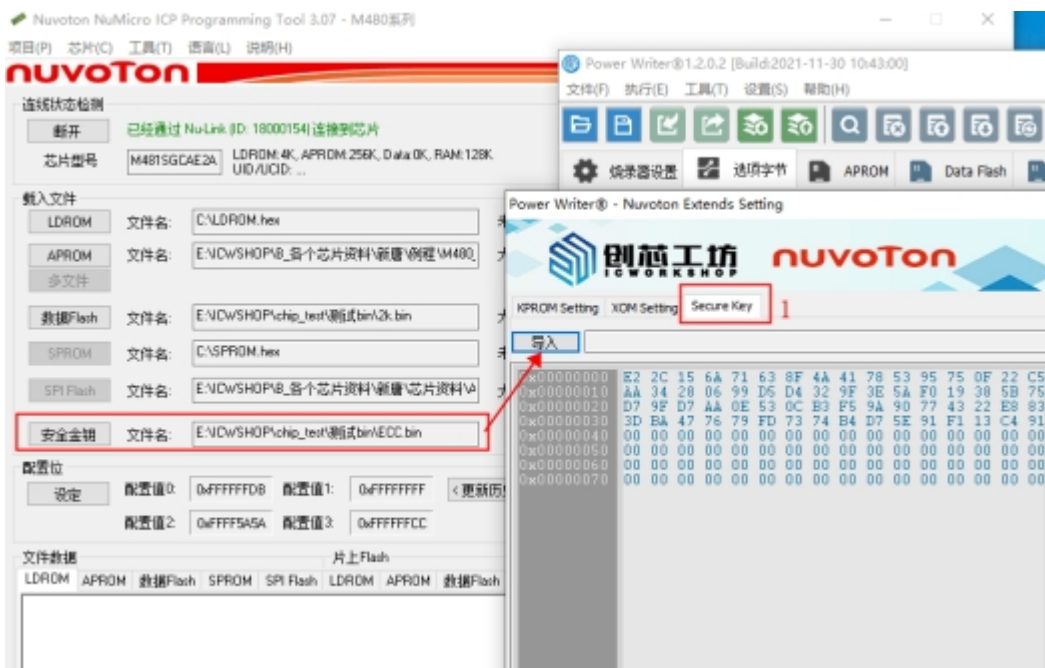


选项名称	选项值(用鼠标点击项,从下拉列表选择)
>>>	[双击可修改] 字节 20
KPCNT 密钥错误上电次数(只读)	0x00: 00
>>>	[双击可修改] 字节 21
KPMAX 密钥尝试上电次数最大值(只读)	0x07: 07
>>>	[双击可修改] 字节 22
Reserved	0x00: 设置为00
>>>	[双击可修改] 字节 23
Reserved	0x00: 设置为00
>>>	[双击可修改] 字节 24
XOMR3ON	0x00: 未启用
XOMR2ON	0x00: 未启用
XOMR1ON	0x00: 未启用
XOMR0ON	0x01: XOM区域0启用
>>>	[双击可修改] 字节 25
Reserved	0x00: 设置为00

# 安全密钥

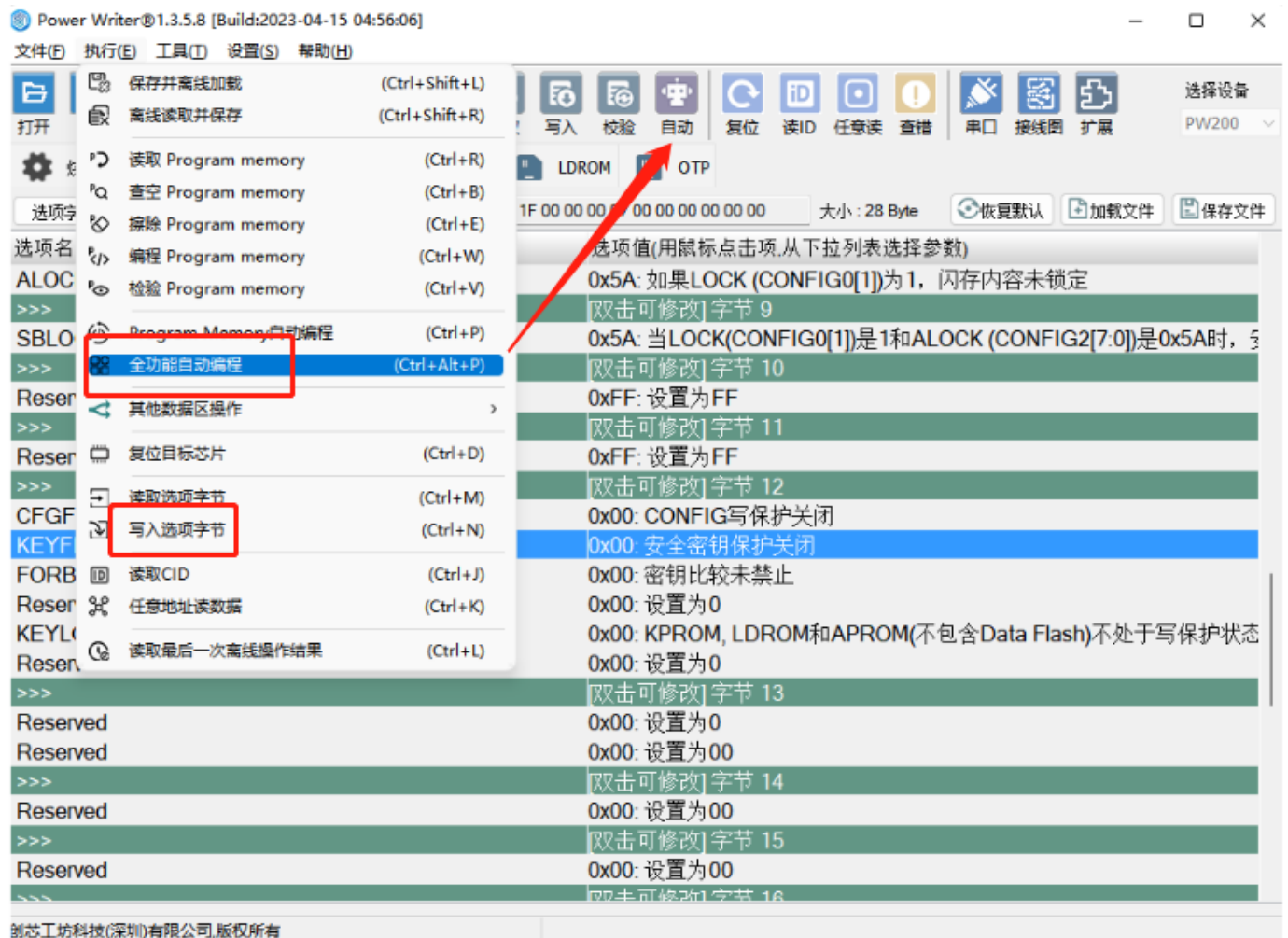
## 安全密钥的导入

在Secure Key中导入安全密钥，操作方法可以参考：Nuvoton NuMicro ICP Programmer 用户指南.pdf



## 安全密钥的配置和写入

勾选BootLoader启动和安全启动加密，然后点击写入选项字节，可以添加固件后点击全自动编程；

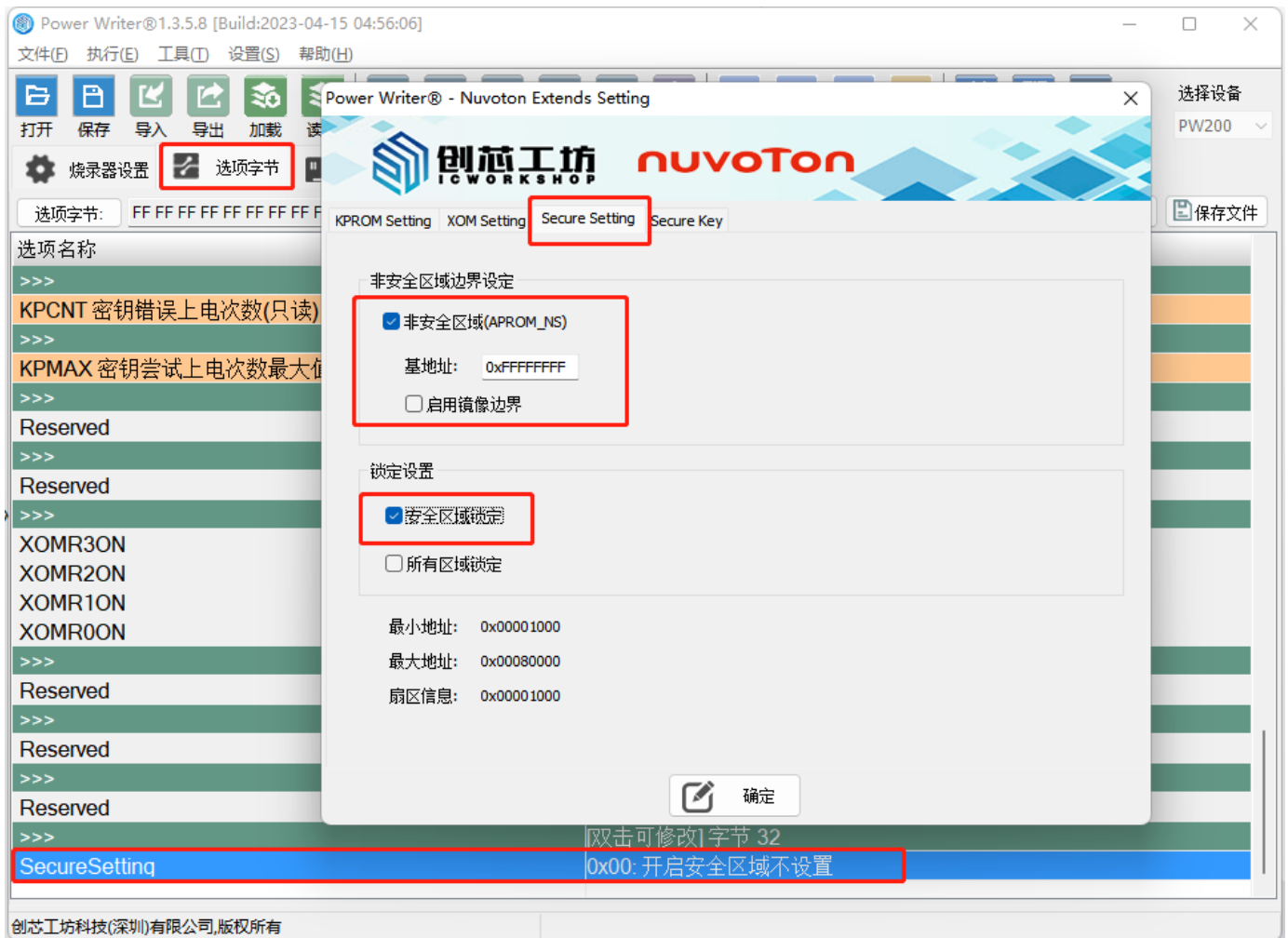


# 安全区域设置



# 安全区域配置方法

这里以M2351为例，打开扩展设置，选择启动非安全区域，写入非安全区域地址，并在选项字节中开启安全区域设置：



# 安全区域解锁方法

锁定设置设定后，芯片将连接不了，需要点击恢复默认，写入选项字节



# MTP设置

## MTP 注意事项

MTP设置属于NUC505的特定功能，烧录器连接芯片时，芯片的PB.3需要拉低使芯片从ICP模式启动；烧录完成后PB.4,PB.3,PA.10,PA.9不能拉低，程序才能正常启动。

### 6.2.3 系统上电设置

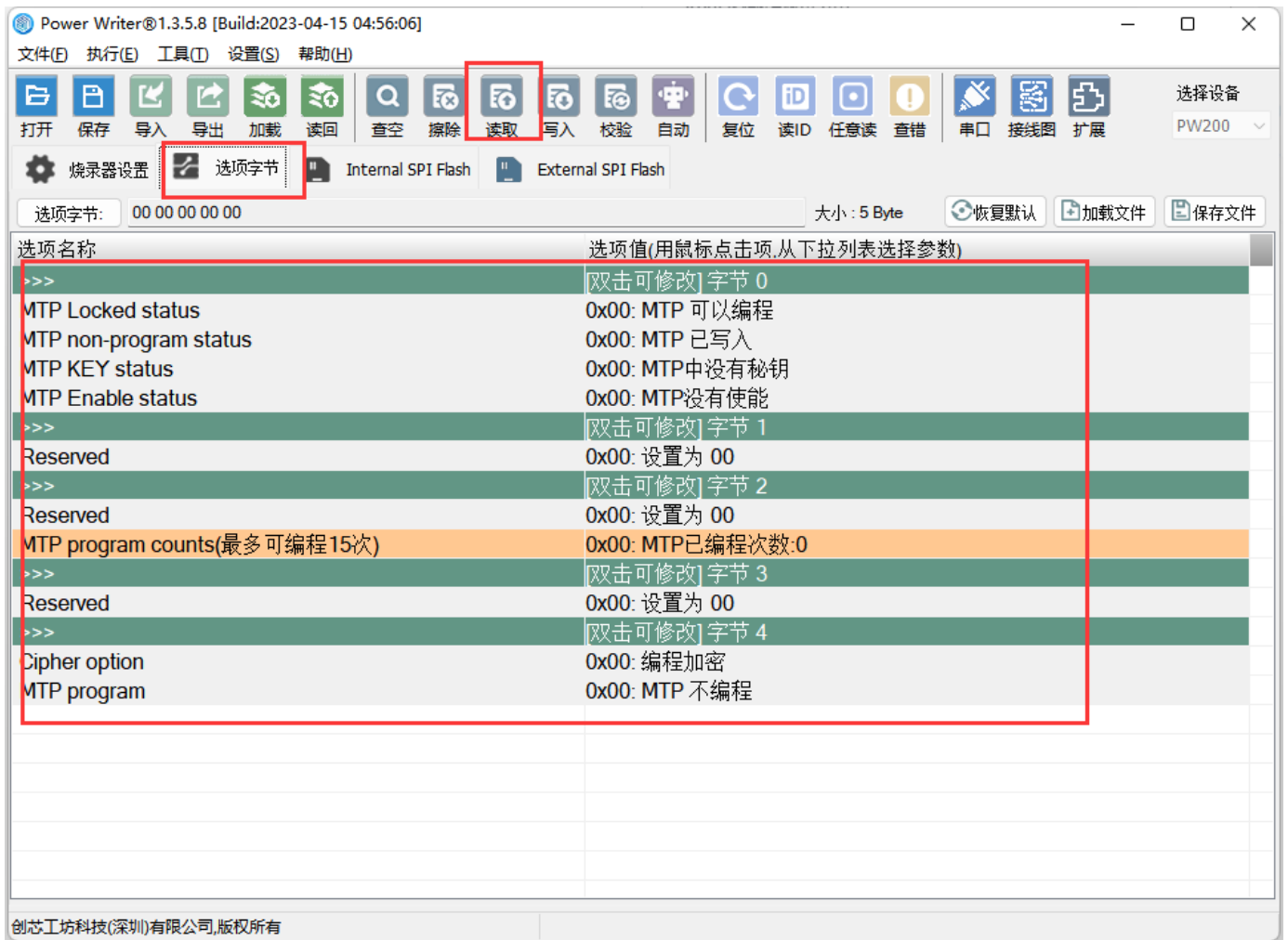
当芯片上电或是复位时需要配置上电设置让芯片进入指定状态。由于在复位期间每个引脚在上电设置时都有对应的内部上拉电阻，如果应用需要设置为0，那么在对应的引脚上需要增加合适的下拉。

PB.4	PB.3	PA.10	PA.9	描述	寄存器映射
1	1	1	1	从内部的 MCP SPI Flash 启动	SYS_BOOTSET[3:0]
1	1	1	0	从 USB 启动	SYS_BOOTSET[3:0]
1	1	0	1	从外部 SPI Flash 启动	SYS_BOOTSET[3:0]
1	0	1	1	从 ICP 模式启动	SYS_BOOTSET[3:0]
0	1	1	1	内部 SPI Flash SWDICE 模式	SYS_BOOTSET[3:0]
0	1	1	0	外部 SPI Flash SWDICE 模式	SYS_BOOTSET[3:0]

表 6.2-1 系统上电设置指南

# MTP 状态读取

连接芯片，读取选项字节，可以获取MTP的激活状态：



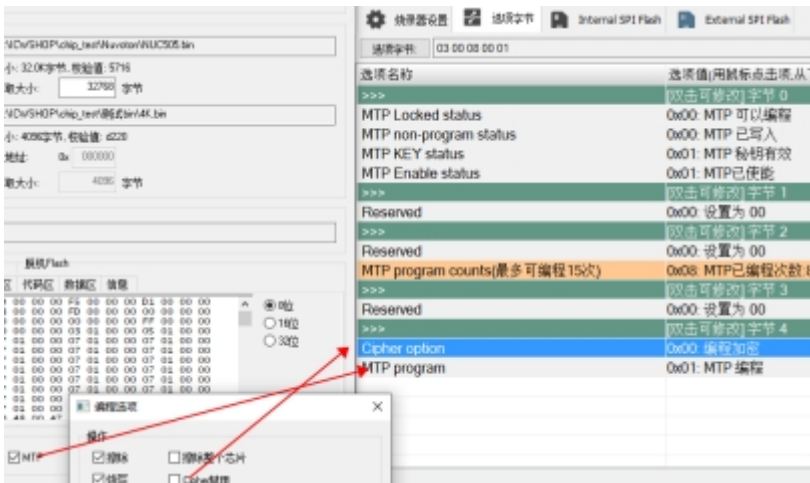
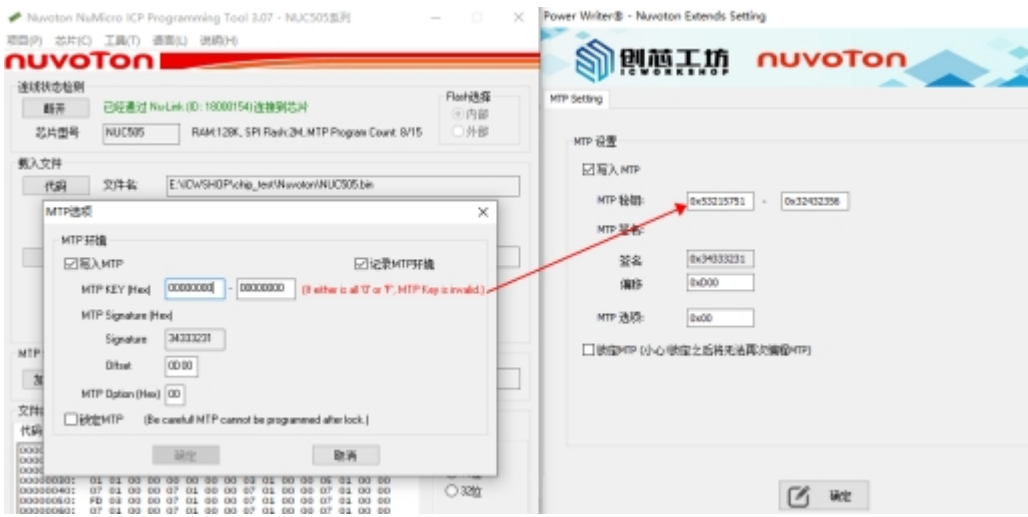
## MTP 配置方法

在Nuvoton扩展设置中的MTP Setting填入正确的数值,需要更新MTP时, 需要同时勾选写入MTP和MTP编程;

\* MTP 秘钥: 0x53215751 -0x32432356 //这个随机填写, 非全0和非全ff

\*程序固件需在偏移地址设定签名, 自定义:

```
const uint32_t signature attribute((at(0x00000d00))) = 0x34333231;
```



当MTP被编程时，代码验证将自动激活。Flash上的代码(或要写入SPIFlash的文件)必须通过代码验证流。NUC505将搜索偏移地址的0~16KBSPIFlash（或文件要写入SPIFlash），以检查偏移地址上是否有正确的签名（与NUC505MTP中的数据进行比较，参见图2-1）。如果没有签名，则启动或编程操作将失败。这种保护机制称为芯片外内存保护，所以要编程加密时，需要添加不小于16K的固件,不编程加密时则不用：

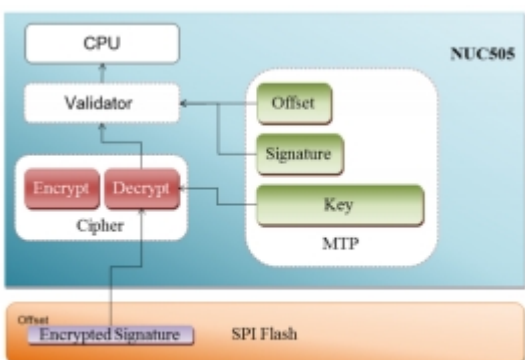
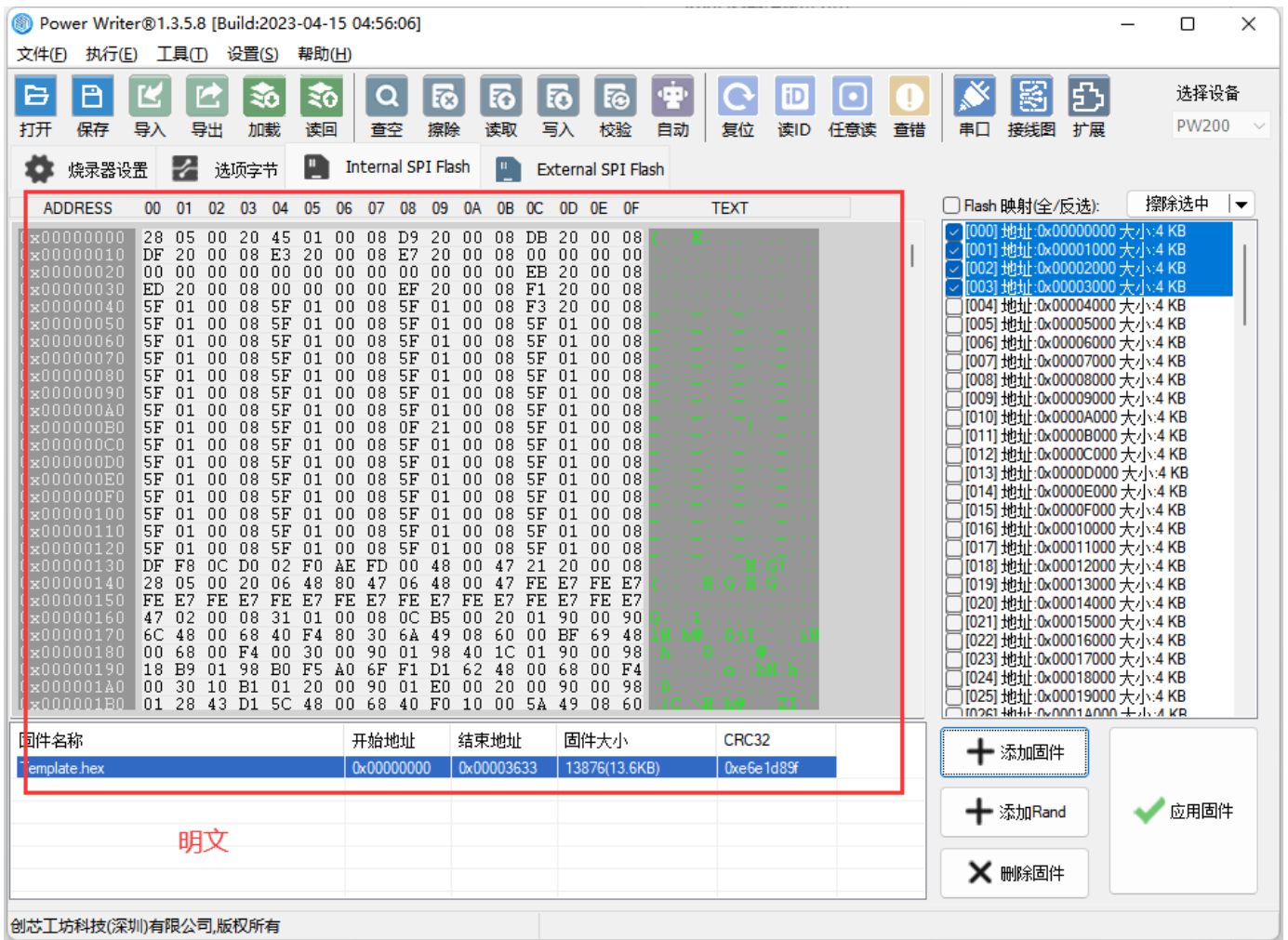
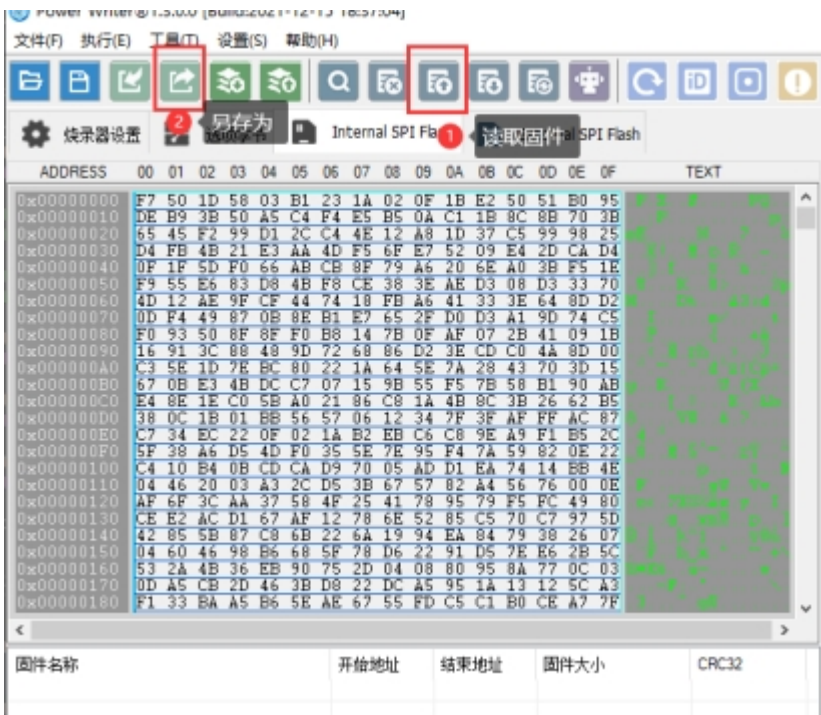


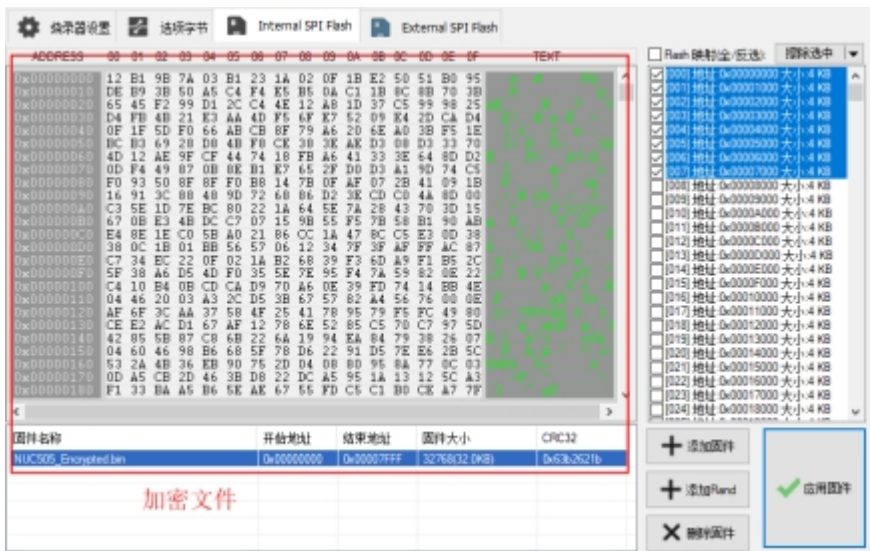
Figure 2-1 Code Validation Flow

使用编程加密时，添加明文固件：



不是用编程加密时，可以先读取加密后的固件另存为，再添加：



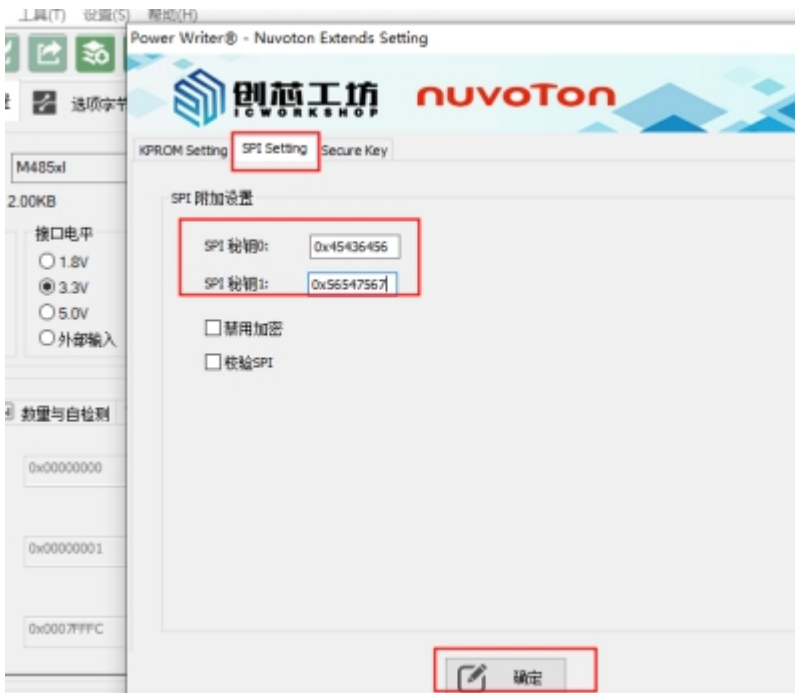


点击写入选项字节，或者全自动烧录，或离线加载烧录

## SPI Flash 加密设置

### SPI Flash 加密设置方法

选择对应芯片，例如M485xl，打开扩展设置选择SPI Setting，密钥0和和密钥1填写非0数值,确定后烧录时芯片会自动加密烧录；




提示

[下载本页PDF文件](#)

标签:

FAQ

Nuvoton

 编辑本页