M487 使用 AES 和 SPROM 安全 ISP 升级

NuMicro® 32 位系列微控制器范例代码介绍

文件信息

应用简述	本范例代码使用 M487 通过 ISP Programming tool 下载加密固件后，使用 AES crypto 还原固件内容并进行更新，实现安全下载。
BSP 版本	M480_BSP_CMSIS_V3.06.000
开发平台	NuMaker-PFM-M487 V3.0

The information described in this document is the exclusive intellectual property of Nuvoton Technology Corporation and shall not be reproduced without permission from Nuvoton.

Nuvoton is providing this document only for reference purposes of NuMicro microcontroller and microprocessor based system design. Nuvoton assumes no responsibility for errors or omissions.

All data and specifications are subject to change without notice.

For additional information or questions, please contact: Nuvoton Technology Corporation.

www.nuvoton.com

1. 概述

本范例程序提供用户使用 UART 接口进行固件更新时，可先通过新唐 CryptoTool 进行固件加密，再通过新唐 NuMicro_ISP_Programming_Tool 将加密后的固件写入待更新的 NuMaker-PFM-M487 开发板。M487 在确认接收完成后会調用 SPROM 内部的解密 API，搭配硬件加密加速器，以及储存在 SPROM 的 AES 密钥将加密固件进行解密，而后将固件写入 APROM 完成更新流程。

1.1 原理

固件加密采用 Advanced Encryption Standard (AES) 进行，为一种对称式加解密算法，用作加解密的密钥为同一把，长度可为 128、192 或者 256 bits。方式为将要加密的数据分为数个固定大小的区块进行加密，其优点为安全性高、速度快，为美国国家标准与技术研究院(NIST)所发布。

目前 NIST 针对 AES 算法提供了多种模式，新唐 CryptoTool 采用 AES-CFB-256 ，在进行档案加解密前需设定 256 bits 的密钥，以及 128 bits 的 Initialization Vector (IV)，并指定需做加密档案的位置，以及加密完档案的存放路径及文件名，可参考如下:

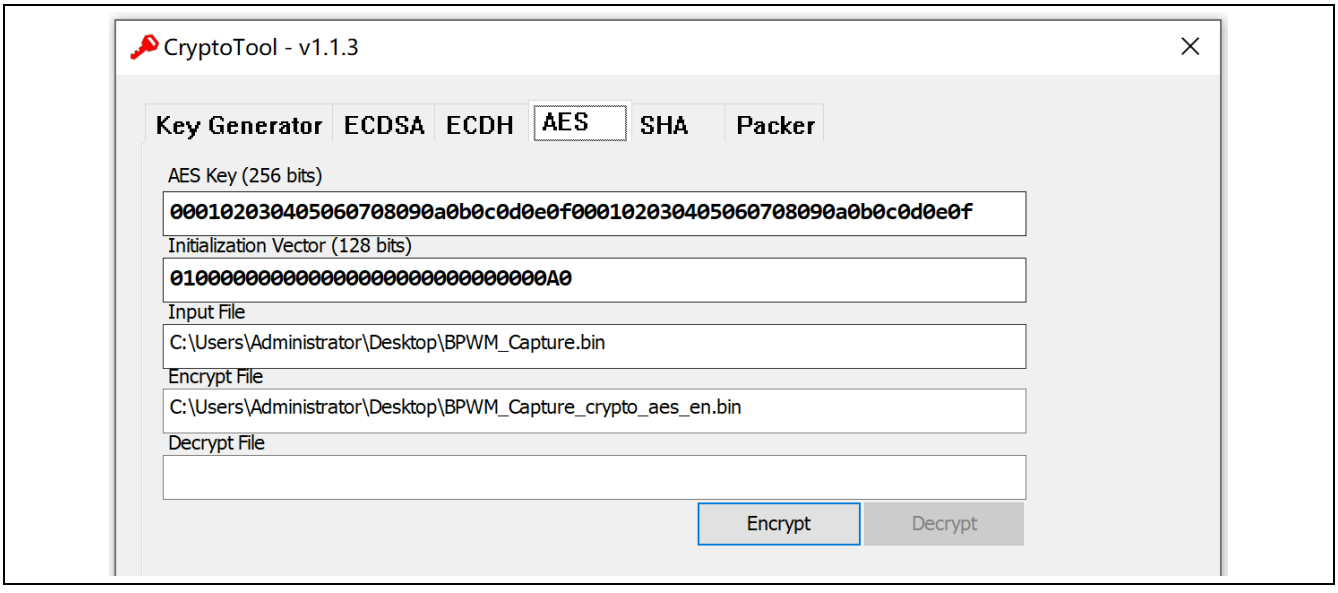


图 1-1 Nuvoton CryptoTool -v1.1.3

1.2 Security Protection Memory (SPROM)

M487 可将内部 SPROM 配置成独立的安全区域，该区域储存的指令(程序代码)无法被读取只能执行，最多有 4K 字节的安全空间，用户可将机密程序代码放在该区域，防止外部程序意外读取数据，以及泄漏客户软件信息，详细说明可参考 M480 Series Technical Reference Manual 章节 6.5.4.4。范例中我们将解密固件所用到的 API 以及 AES 加解密所使用的 IV 放在该区域内。

1.3 执行结果

1.3.1 ISP Bootloader 烧录到 MCU

范例代码执行编译后，会生成两个 bin 文件如下图：

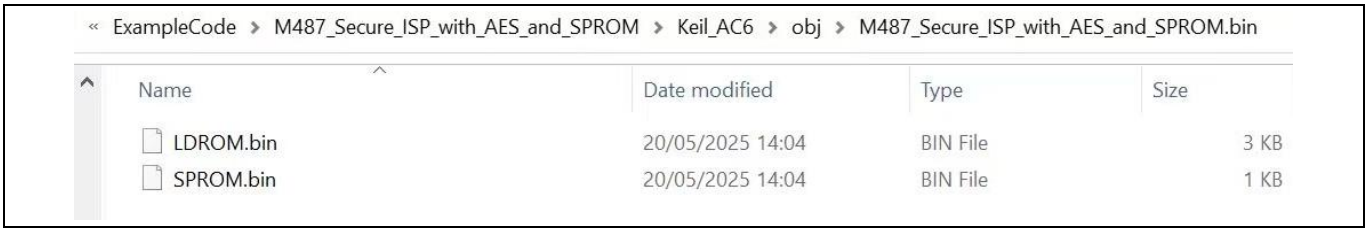


图 1-2 编译后生成的 bin 文档

烧录时使用 NuMicro ICP Programming Tool 软件进行烧录，如图 1-3 ICP 配置，LDROM 选择 “LDROM.bin” ，SPROM 选择 “SPROM.bin” 。

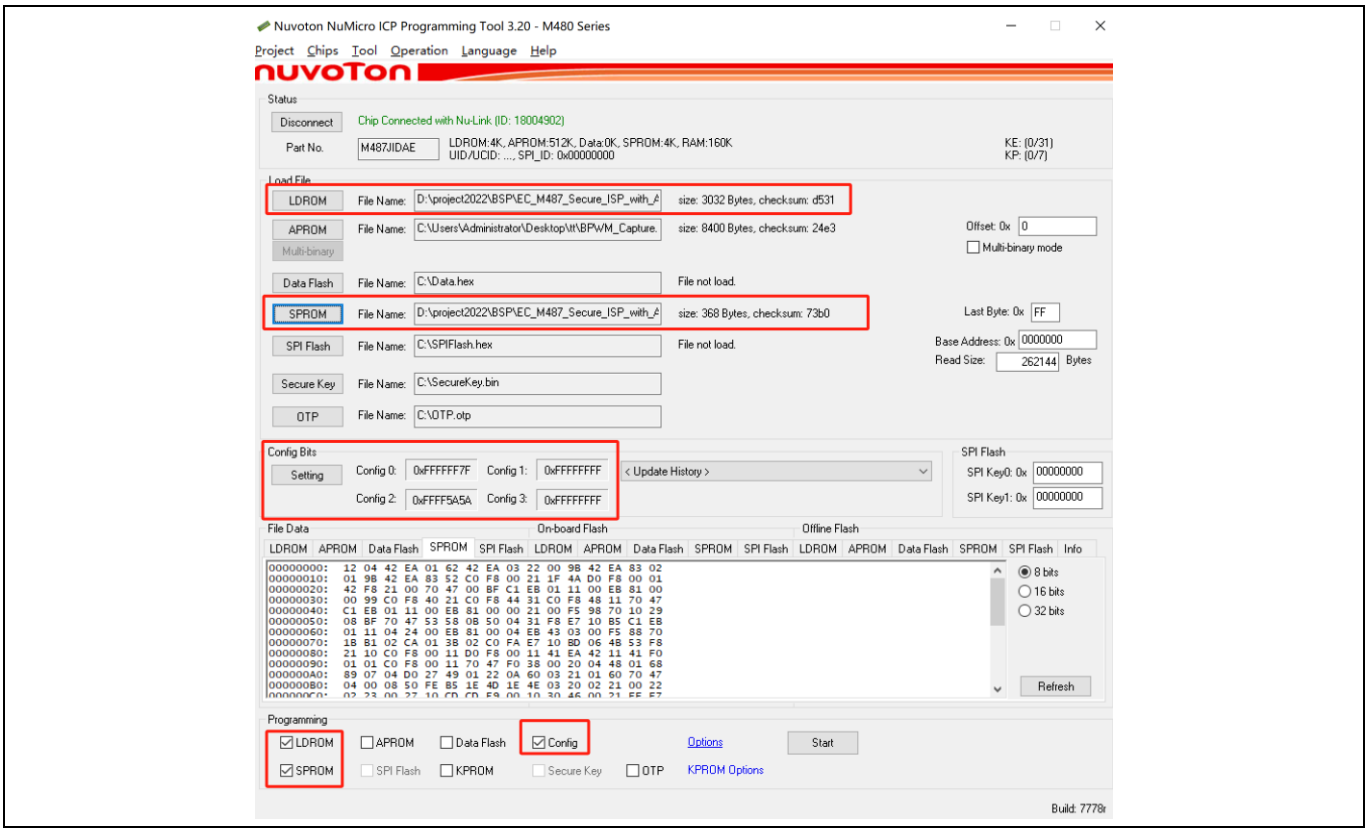


图 1-3 ICP 配置

配置字选择如下图：

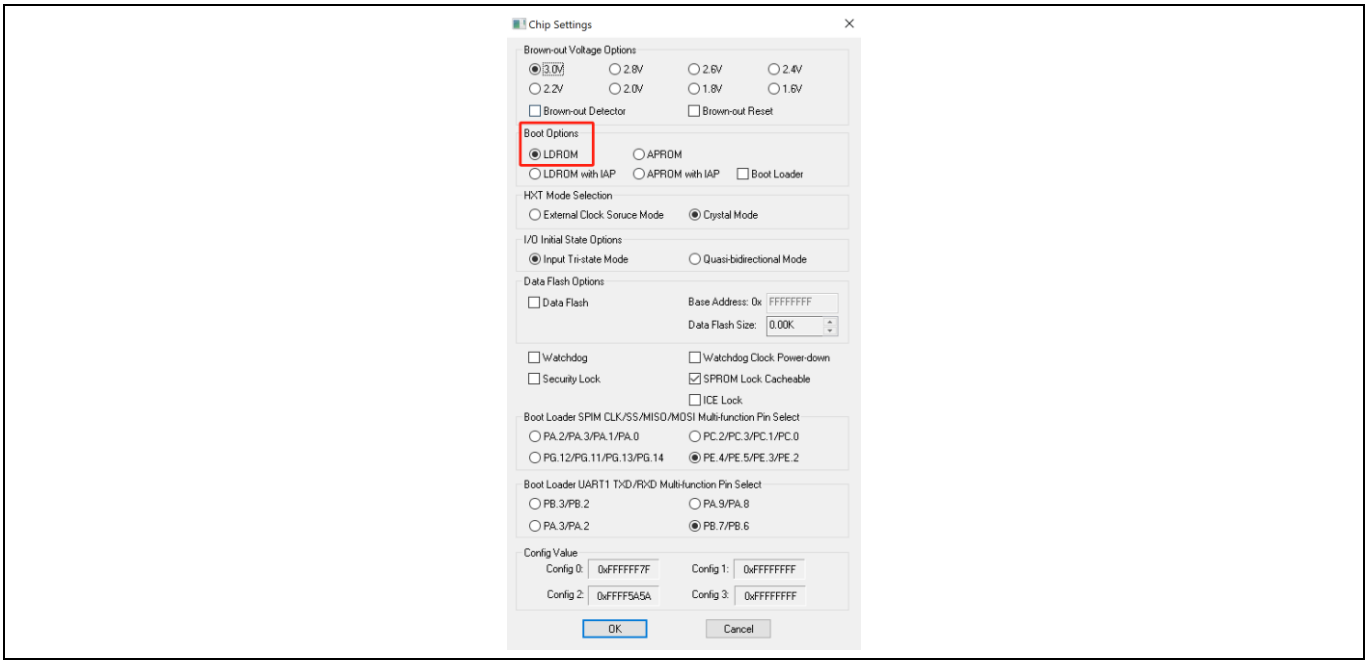


图 1-4 配置字

1.3.2 生成加密 bin 档

烧录后按下图 1-5 使用新唐 CryptoTool 工具加密程序，这里选择 AES 字段，设定 AES key 以及 Initialization Vector。编译 M480 BSP 内任意一范例程序(这里以 Template 例程为例)，并将编译完成的 bin 档复制到 CryptoTool 底下。设定 Input File 及 Encrypt File 的路径，按下 **Encrypt** 按钮，几秒后会在该路径下看到生成的加密 bin 档。

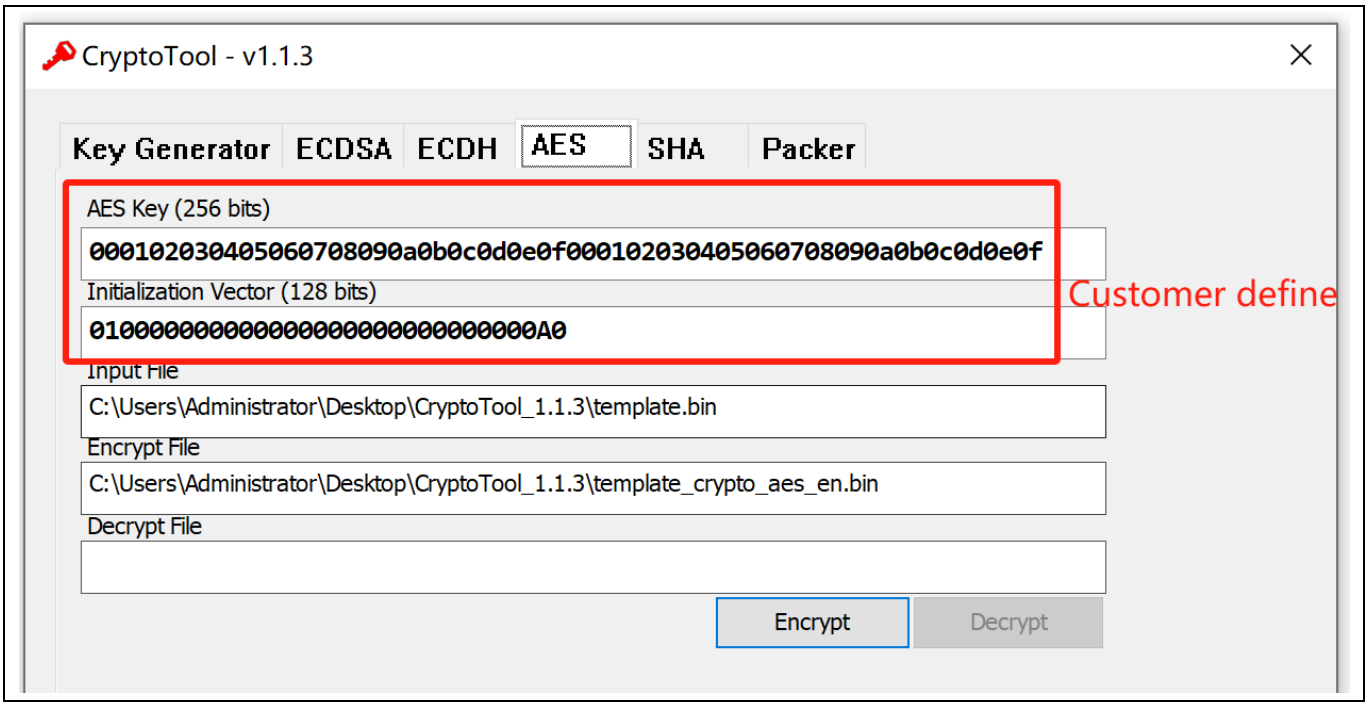


图 1-5 文件加密

1.3.3 執行 ISP 更新 APROM

接着打开新唐 ISP 软件，点击 UART 选择对应串口，点击“**Connect**”，开发板上按 reset 按键，之后会连上新唐 ISP，如下图 1-6，连上后会显示芯片型号，这时选择 APROM 加载刚刚加密后的“*template_crypto_aes_en.bin*”文档，点击“**Start**”进行升级。

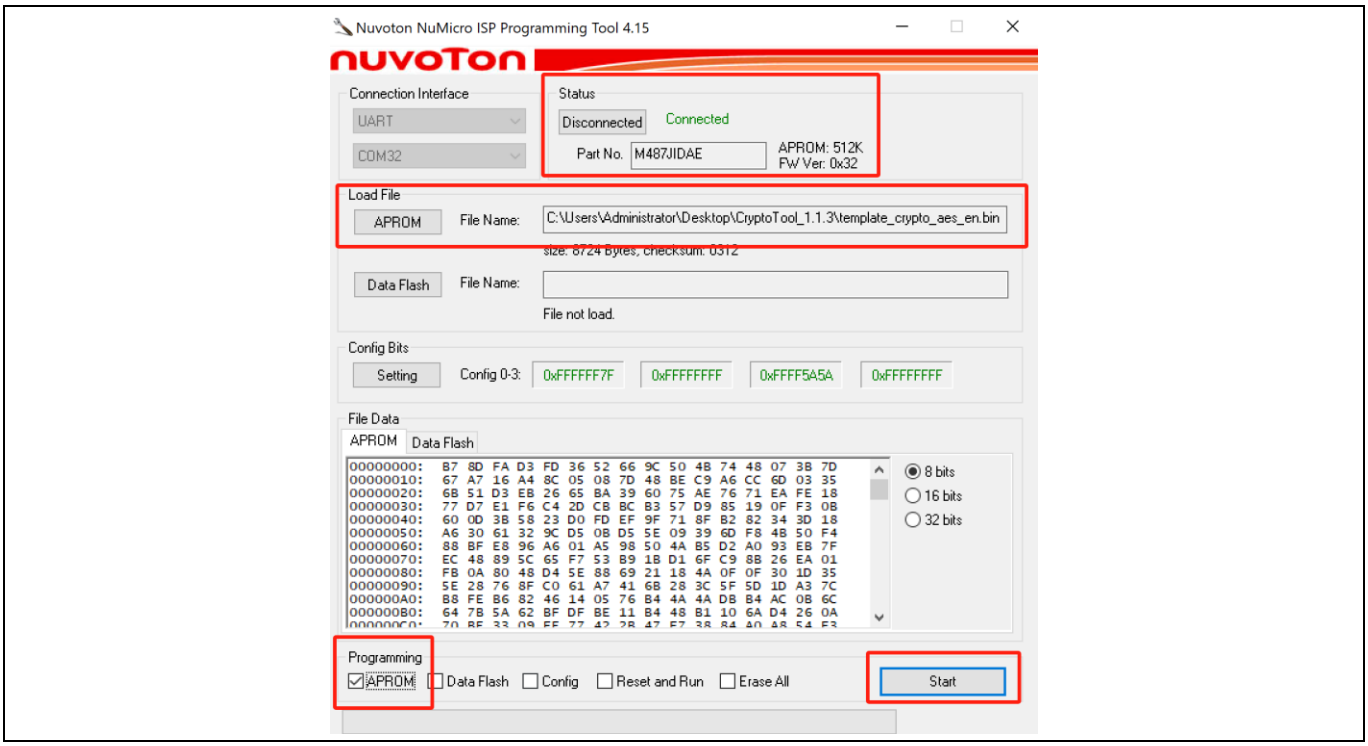


图 1-6 ISP 升级界面

升级后关闭 ISP 软件，打开串口工具，选择相应打印串口，在开发板上按 reset 按键，可以看到 Template 例程打印的 “Hello World” 字样，如下图 1-7，说明 ISP 烧录的加密后的 “*template_crypto_aes_en.bin*” 文档已解密完成并烧录到 APROM 并且正确运行。

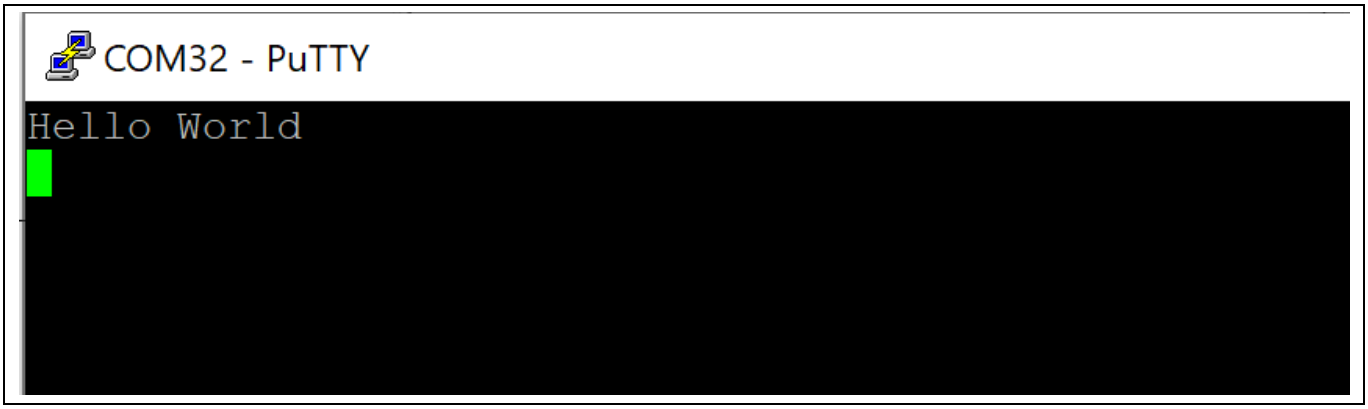


图 1-7 Template 例程打印结果

2. 代码介绍

以下 main()程序实现了范例功能的架构，前半段通过 UART 以及 ISP 协议，将加密的固件写入到 SRAM 区域，后半部在 void UpdateRoutine(void)实现了安全更新的细节，通过 SPROM 进行保护，让黑客无法得知详细流程指令。Secure ISP 程序提供给客户一个安全更新的基本范例，客户可根据其具体需求，改写 UpdateRoutine 的流程，如调整 AES 加解密模式以及 IV 值，由此来完善属于产品本身的更新机制。需注意 M487 的 SRAM 区域只有 160K 字节，所以该范例能夠更新的 APROM（bin 档）大小是有限制的。

```
int main(void)
{
    uint8_t u8SysTickCnt = 0;

    /* Unlock protected registers */
    SYS_UnlockReg();
    /* Init System, peripheral clock and multi-function I/O */
    SYS_Init();
    /* Init UART to 115200-8n1 */
    UART_Init();

    CLK->AHBCLK |= CLK_AHBCLK_ISPCKEN_Msk;
    FMC->ISPCTL |= FMC_ISPCTL_ISPEN_Msk;
    g_apromSize = GetApromSize();
    GetDataFlashInfo(&g_dataFlashAddr, &g_dataFlashSize);
     SYS_UnlockReg();                   /* Unlock protected registers */
    NVIC_EnableIRQ(CRPT_IRQn);
    AES_ENABLE_INT(CRPT);

    SysTick->LOAD = 0xFFFFFF;
    SysTick->VAL  = (0x00);
    SysTick->CTRL = SysTick->CTRL | SysTick_CTRL_CLKSOURCE_Msk
                    | SysTick_CTRL_ENABLE_Msk; /*using cpu clock*/

    g_u8ISPDone = FALSE;
    while (1)
    {

        if ((bufhead >= 4) || (bUartDataReady == TRUE))
        {
            uint32_t lcmd;
            lcmd = inpw(uart_rcvbuf);

            if (lcmd == CMD_CONNECT)
            {
                goto _ISP;
            }
            else
            {
                bUartDataReady = FALSE;
                bufhead = 0;
```

```
            }
        }

        if (SysTick->CTRL & SysTick_CTRL_COUNTFLAG_Msk) /*timeout, then goto APROM*/
        {
            SysTick->VAL = 0;
            u8SysTickCnt++;
            if (u8SysTickCnt >= 5)
            {
                goto _APROM;
            }
        }
    }

_ISP:

    while (1)
    {
        if (bUartDataReady == TRUE)
        {
            bUartDataReady = FALSE;
            ParseCmd(uart_rcvbuf, 64);
            PutString();
        }
       if (g_u8ISPDone == TRUE)
        {
            UpdateRoutine();
            g_u8ISPDone = FALSE;
        }

    }

_APROM:
    SYS->RSTSTS = (SYS_RSTSTS_PORF_Msk | SYS_RSTSTS_PINRF_Msk);
    FMC->ISPCTL &= ~(FMC_ISPCTL_ISPEN_Msk | FMC_ISPCTL_BS_Msk);
    SCB->AIRCR = (V6M_AIRCR_VECTKEY_DATA | V6M_AIRCR_SYSRESETREQ);

    /* Trap the CPU */
    while (1);
}
```

以下 UpdateRoutine() 程序实现了 AES 解密文件，核心是要实现 AES engine 做加解密时密钥的写入及功能测试，其中关键的 AES key 透过 au32MyAESKey 数组实现，用户在孰悉操作后可自由替换成实际产品所使用的密钥。AES 密钥属性，建议设定为加密后的 SPROM 常量，这样可确保该密钥只能被 AES engine 所取用，由此达到完整的保护。

```
void UpdateRoutine(void)
{

    uint32_t StartAddress = 0x0000,  TotalLen;
    TotalLen = g_au32Encryptedimage[0];
```

```
    /*---------------------------------------
    *  step 1, decrypt image
    *  AES-256 CFB mode decrypt fw image
    *---------------------------------------*/
    AES_Open(CRPT, 0, 0, AES_MODE_CFB, AES_KEY_SIZE_256, AES_IN_OUT_SWAP);
    /* Use key in key store */
    AES_SetKey(CRPT, 0, (uint32_t *)au32MyAESKey, AES_KEY_SIZE_256);
    AES_SetInitVect(CRPT, 0, (uint32_t*)au32MyAESIV);
    AES_SetDMATransfer(CRPT, 0, (uint32_t)&g_au32Encryptedimage[1],
                       (uint32_t)au8OutputData, TotalLen);
     g_AES_done = 0;
    AES_Start(CRPT, 0, CRYPTO_DMA_ONE_SHOT);
    while (!g_AES_done);

    /* step 2, update APROM */
    FMC_ENABLE_AP_UPDATE();
     EraseAP(FMC_APROM_BASE,g_apromSize); /* erase APROM */
    WriteData(StartAddress, StartAddress + TotalLen, (uint32_t *)au8OutputData);

    return;
}
```

3. 软件与硬件需求

3.1 软件需求

- BSP 版本
  - M480_BSP_CMSIS_V3.06.000
- IDE 版本
  - Keil uVersion 5.41

3.2 硬件需求

- 电路组件
  - NuMaker-PFM-M487 V3.0
- 线路示意图
  - 将 UART0 的 pin 脚通过 ICE 连接到 PC UART，以连接 ISP 和显示范例代码的执行结果。

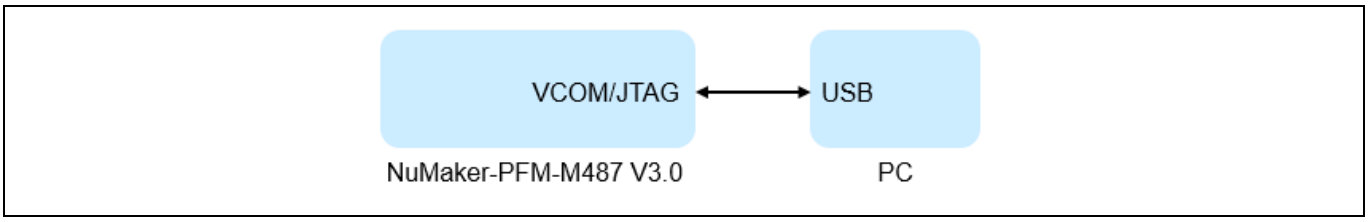


图 3-1 线路示意图

4. 目录信息

目录结构如下图所示。

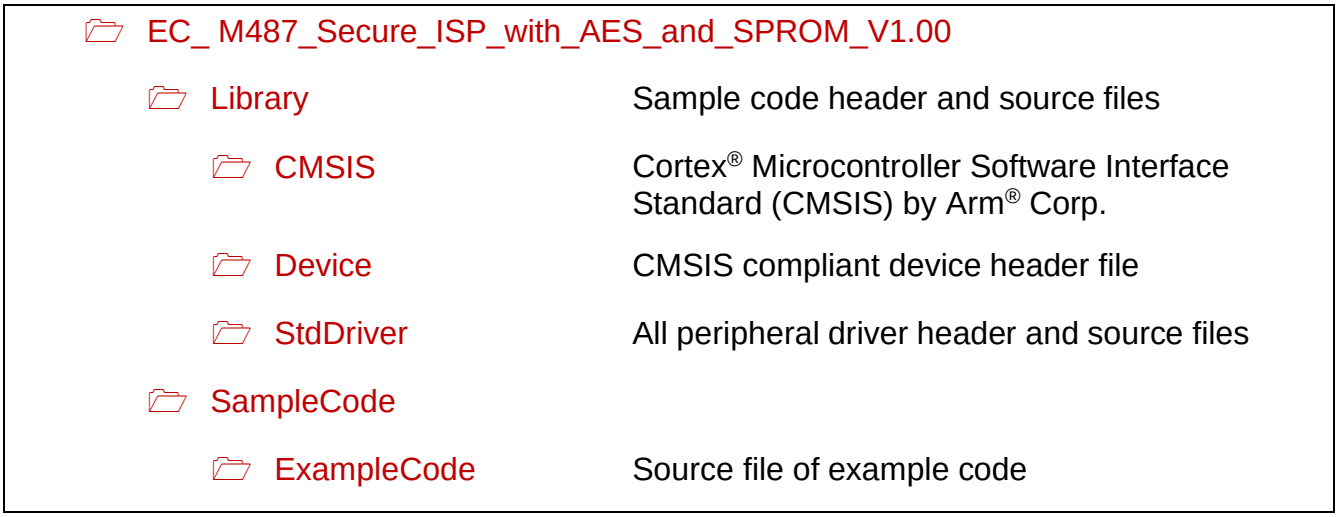


图 4-1 目录信息

5. 范例程序执行

1. 根据目录信息章节进入 ExampleCode 路径中的 KEIL 文件夹，双击 *M487_Secure_ISP_with_AES_and_SPROM.uvprojx*。
2. 进入编译模式界面
   - 编译
   - 下载代码至内存
   - 进入 / 离开仿真模式
3. 进入仿真模式界面
   - 执行代码

6. 修订纪录

Date	Revision	Description
2025.04.24	1.00	初始发布。

Important Notice

Nuvoton Products are neither intended nor warranted for usage in systems or equipment, any malfunction or failure of which may cause loss of human life, bodily injury or severe property damage. Such applications are deemed, "Insecure Usage".

Insecure usage includes, but is not limited to: equipment for surgical implementation, atomic energy control instruments, airplane or spaceship instruments, the control or operation of dynamic, brake or safety systems designed for vehicular use, traffic signal instruments, all types of safety devices, and other applications intended to support or sustain life.

All Insecure Usage shall be made at customer's risk, and in the event that third parties lay claims to Nuvoton as a result of customer's Insecure Usage, customer shall indemnify the damages and liabilities thus incurred by Nuvoton.

Please note that all data and specifications are subject to change without notice.
All the trademarks of products and companies mentioned in this datasheet belong to their respective owners.