M031 APROM程序綁定UID

NuMicro® 32 位系列微控制器範例代碼介紹

文件資訊

應用簡述	本範例代碼介紹如何通過綁定 MCU 的 UID 碼，實現程序與 MCU 的綁定
BSP 版本	M031_Series_BSP_CMSIS_V3.04.000
開發平台	NuMaker-M032SE V1.3

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

新唐的M031系列MCU，每一顆都有一個96位的唯一ID（UID）碼，本文介紹如何將程序綁定UID碼，以避免他人將MCU中的Bin檔拷貝出來，燒錄到新的MCU，複製出一樣的產品。

1.1 原理

由於M031系列MCU，每一顆都有一個96位的UID碼，所以可在程序中加入對UID碼的判斷，來決定程序的執行流程，這樣儘管將運行正常的MCU固件讀出來燒錄到另外一顆同型號的MCU中，也得不到正常的運行結果，其大致原理如圖1-1所示。

注：使用該方法必須保證產品出廠之前，MCU已經上電運行過一次，以保證存儲在APROM中的初始密鑰被擦除。

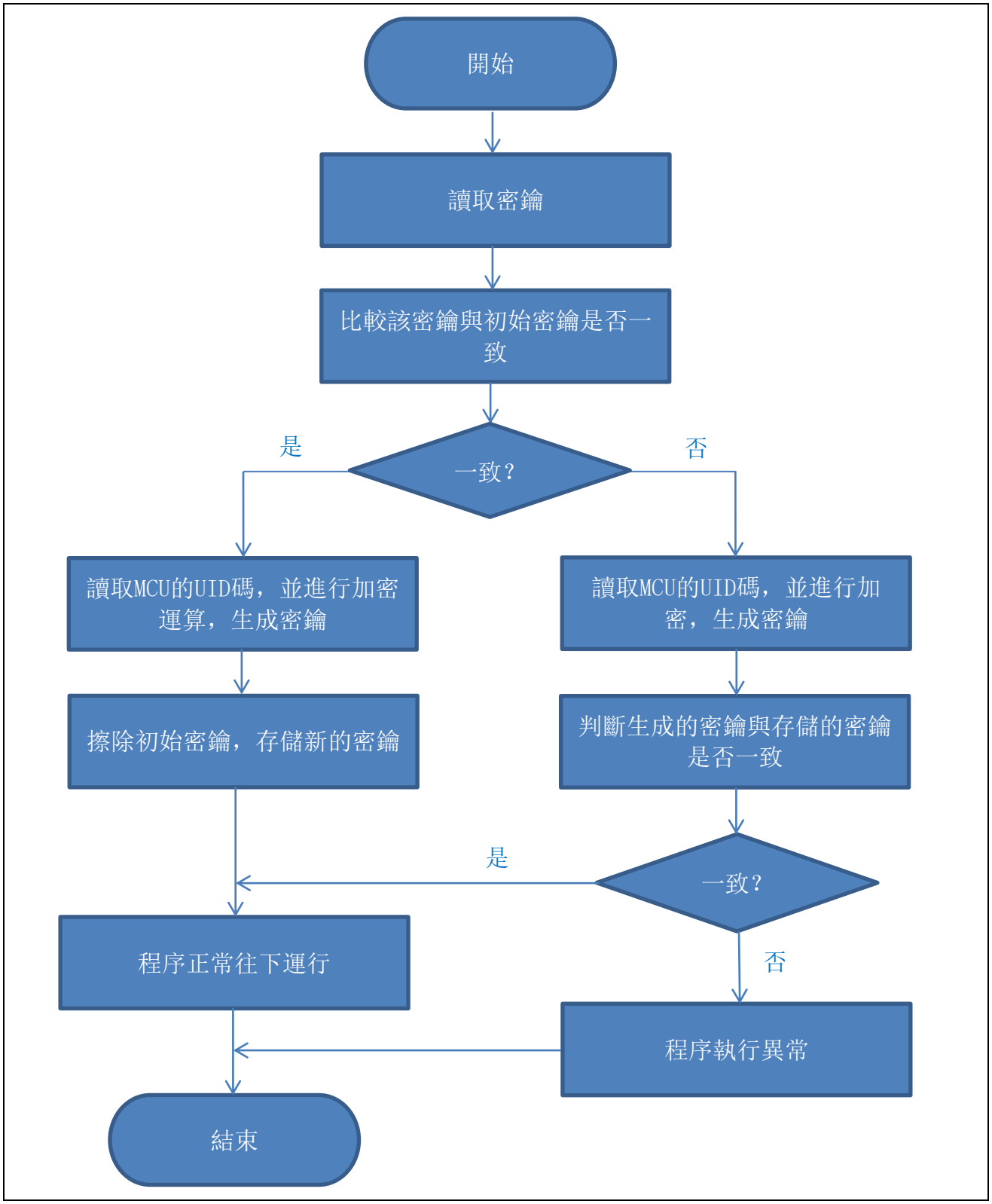
開始
讀取密鑰
比較該密鑰與初始密鑰是否一致
一致?
是
否
讀取MCU的UID碼，並進行加密運算，生成密鑰
讀取MCU的UID碼，並進行加密，生成密鑰
擦除初始密鑰，存儲新的密鑰
判斷生成的密鑰與存儲的密鑰是否一致
一致?
是
否
程序正常往下運行
程序執行異常
結束

圖 1-1 密鑰判斷流程圖

1.2 執行結果

將程序燒錄到“NuMaker-M032SE V1.3”板子，運行時的打印資訊如圖1-2所示：

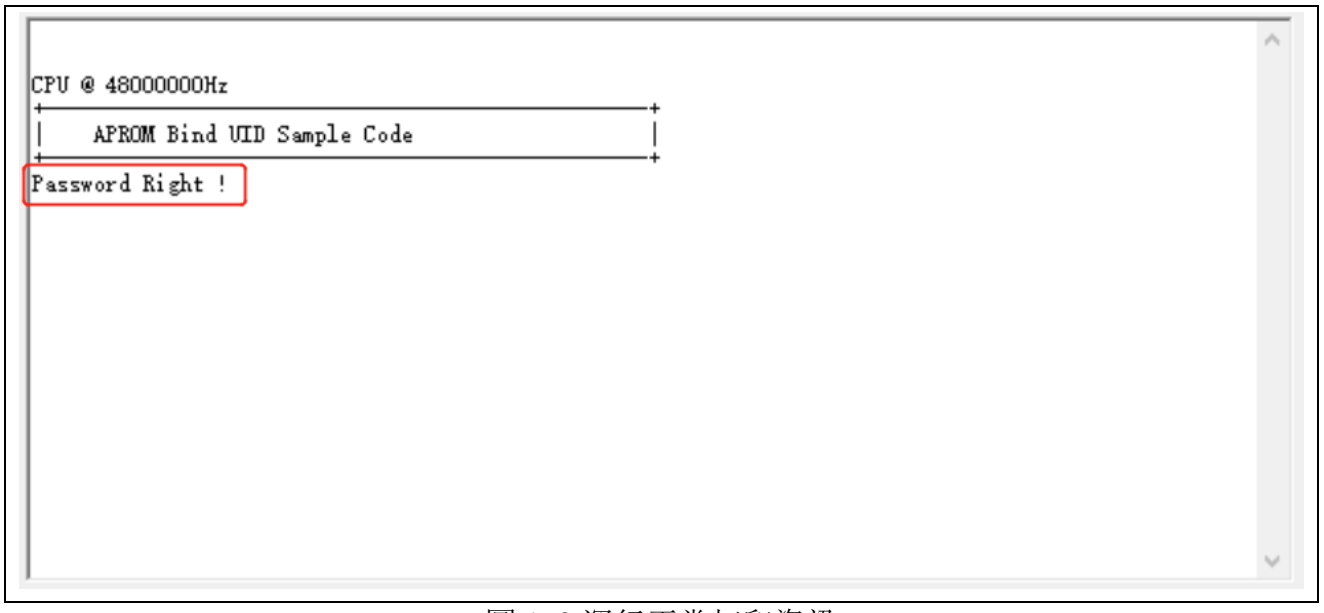

圖 1-2 運行正常打印資訊

通過“NuMicro ICP Programming Tool”從“NuMaker-M032SE V1.3”板子讀出MCU APROM的程序，然後燒錄到另外一塊“NuMaker-M032SE V1.3”板子，運行時，打印印資訊如圖1-3所示：

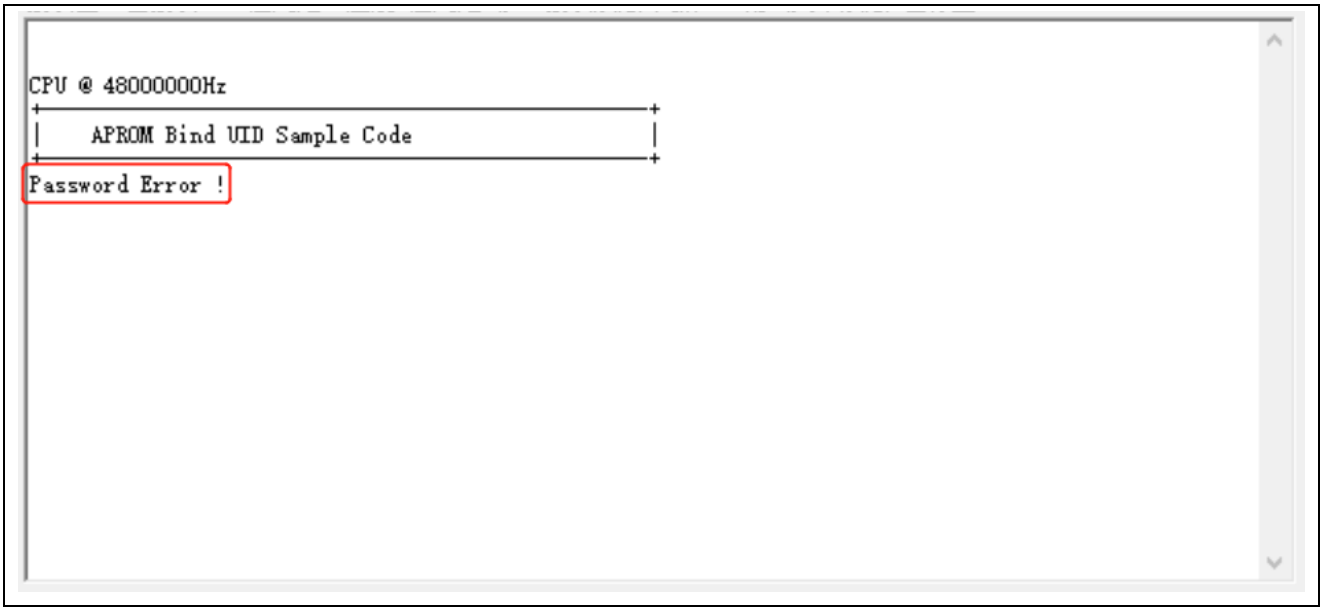

圖 1-3 運行異常打印資訊

2 代碼介紹

初始密鑰設置（用戶可自行更改）：

```
#define INIT_PASSWORD_0       0x12121212 /* Define by user */
#define INIT_PASSWORD_1       0x34343434 /* Define by user */
#define INIT_PASSWORD_2       0x56565656 /* Define by user */
```

將 UID 進行加密（使用者可以根據自己的加密算法進行更改）：

```
void UID_Encrypt(uint32_t au32Uid[3])
{
    uint8_t i;

    /* Encrypt the UID, users can change it according to their encryption algorithm */
    for(i = 0; i < 3; i++)
    {
        au32Uid[i] = (~au32Uid[i]) * 5 / i;
    }
}
```

判斷密鑰與初始密鑰是否一致，若一致，則擦除初始密鑰，寫入由 UID 加密後的新密鑰；若不一致，判斷 UID 加密後的密鑰與存儲的密鑰是否一致：

```
uint8_t UID_PasswordCheck(void)
{
    uint8_t i;
    uint32_t au32Uid[3];
    uint32_t *pu32Password = (uint32_t *)g_au32Password;

    if((pu32Password[0] == INIT_PASSWORD_0) && (pu32Password[1] == INIT_PASSWORD_1)
    && (pu32Password[2] == INIT_PASSWORD_2))
    {
        UID_Read(au32Uid);
        UID_Encrypt(au32Uid);
        UID_PasswordWrite(au32Uid);
    }
    else
    {
        UID_Read(au32Uid);
        UID_Encrypt(au32Uid);

        for(i = 0; i < 3; i++)
        {
            if(au32Uid[i] != pu32Password[i])
            {
                return 0;
            }
        }
    }

    return 1;
}
```

3 軟體與硬體需求

- **軟體需求**
  - BSP 版本
    - M031_Series_BSP_CMSIS_V3.04.000
  - IDE 版本
    - Keil uVersion 4.74
- **硬體需求**
  - 電路元件
    - NuMaker-M032SE V1.3

4 目錄資訊

EC_M031_APROM_Bind_UID_V1.00	
Library	Sample code header and source files
CMSIS	Cortex® Microcontroller Software Interface Standard (CMSIS) by Arm® Corp.
Device	CMSIS compliant device header file
StdDriver	All peripheral driver header and source files
SampleCode	
ExampleCode	Source file of example code

圖 4-1 目錄資訊

5 範例程式執行

1. 根據目錄資訊章節進入 ExampleCode 路徑中的 KEIL 資料夾，雙擊 APROM_Bind_UID.uvproj。
2. 進入編譯模式介面
   a. 編譯
   b. 下載代碼至記憶體
   c. 進入 / 離開除錯模式
3. 進入除錯模式介面
   a. 執行代碼

6 修訂紀錄

Date	Revision	Description
2022.03.08	1.00	1. 初始發布.

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.