Binding UID with M031 APROM Firmware

Example Code Introduction for 32-bit NuMicro® Family

Information

Application	This sample code binds UID code to M031 APROM firmware.
BSP Version	M031_Series_BSP_CMSIS_V3.04.000
Hardware	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 Overview

Each M031 series microcontroller (MCU) has a 96-bit unique ID (UID) code. This document introduces how to bind the UID to firmware to avoid the dumped user firmware running in illegal copy product.

1.1 Principle

Firmware can judge the UID code to determine the execution process of MCU. In this way, even if normal MCU firmware is read and downloaded to another MCU with the same part number, the correct operation result cannot be obtained. The general principle of secret key judgment is shown in Figure 1-1. The details of the secret key judgment flow are described in Code Description section.

Note: To use this method, ensure that the MCU has been powered on and run once before the product shipped from the factory, so that the initial secret key stored in APROM has been erased.

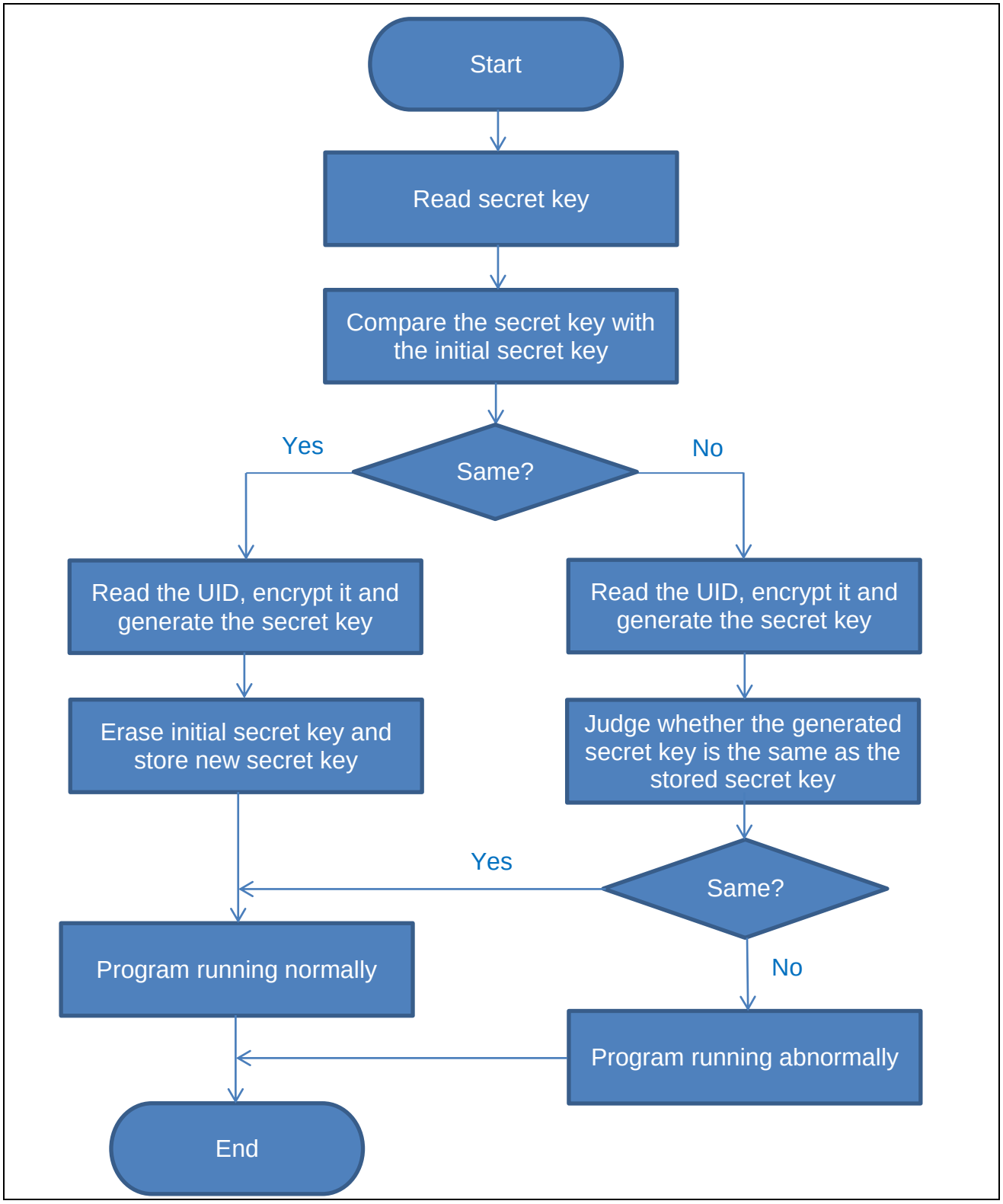

Figure 1-1 Secret Key Judgment Flow

1.2 Demo Result

Download the firmware to NuMaker-M032SE V1.3 board. The printed information during execution is shown in Figure 1-2.

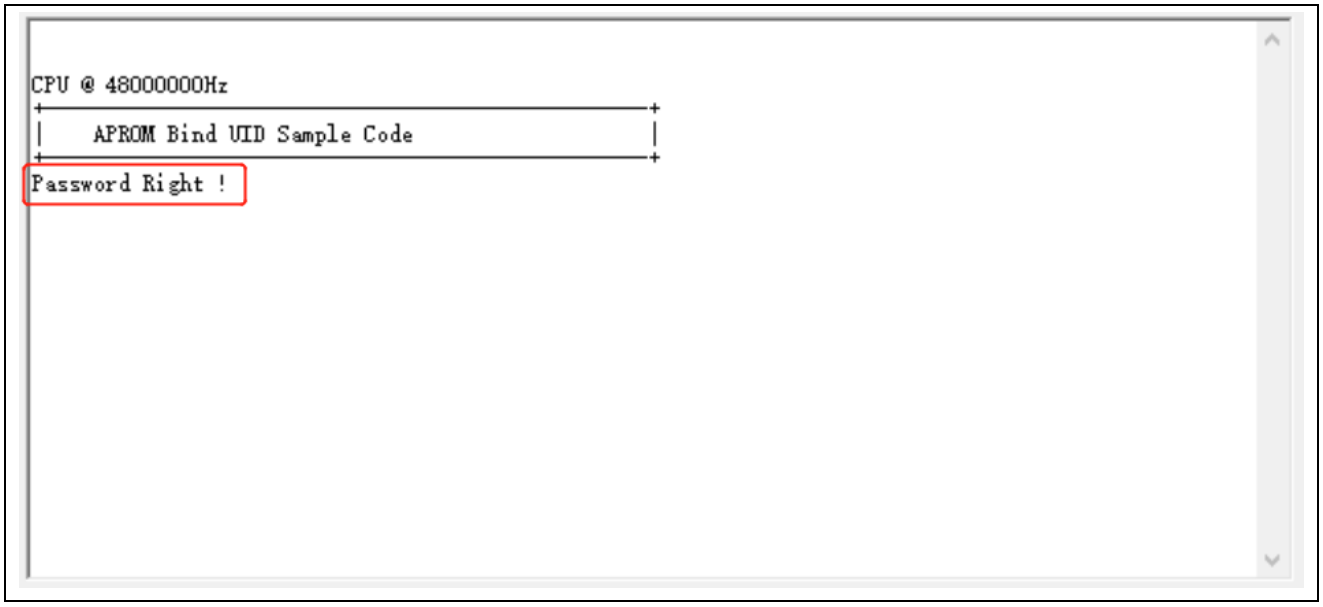

Figure 1-2 Printed Information when Executing Normally

Read the firmware form NuMaker-M032SE V1.3 through NuMicro ICP Programming Tool, and download it to another NuMaker-M032SE V1.3 board. The printed information during execution is shown in Figure 1-3.

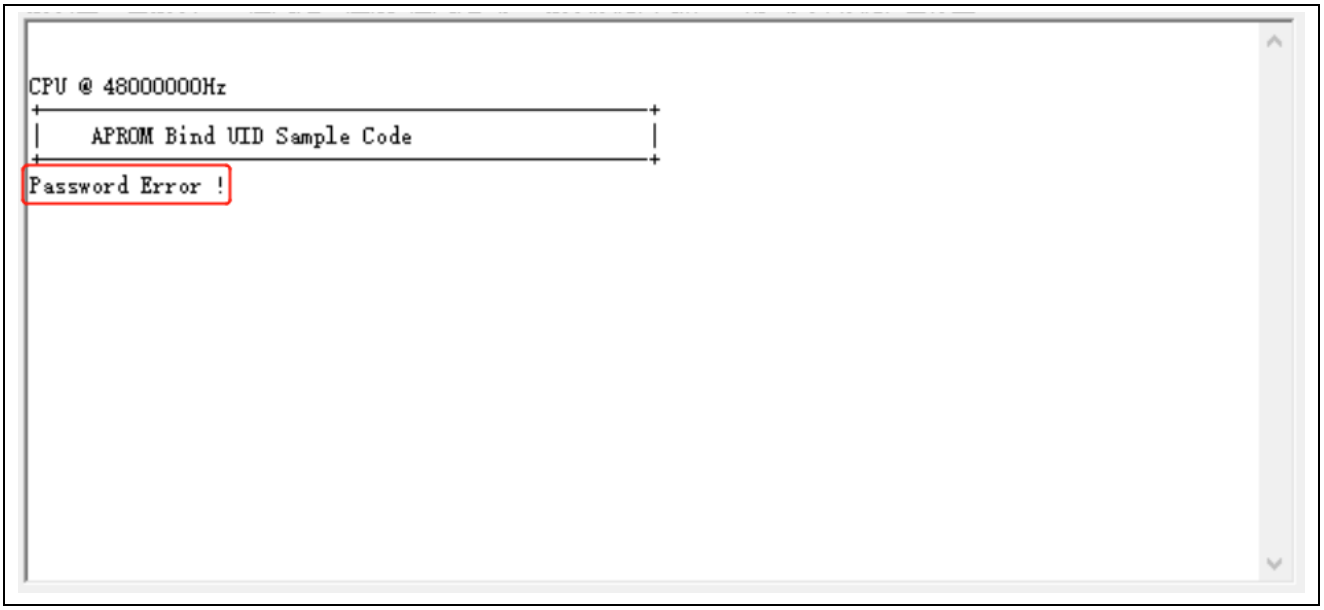

Figure 1-3 Printed Information when Executing Abnormally

2 Code Description

Define initial secret key. Users can define a secret key by themselves.

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

Encrypt the UID. Users can change it according to their encryption algorithm.

```
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;
    }
}
```

Judge whether the secret key is the same as the stored initial key. If yes, erase the initial key, and write the new secret key encrypted by UID. If no, judge whether the secret key encrypted by the UID is the same as the stored secret key.

```
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 Software and Hardware Requirements

3.1 Software Requirements

- BSP version
  - M031_Series_BSP_CMSIS_V3.04.000
- IDE version
  - Keil uVersion 4.74

3.2 Hardware Requirements

- Circuit components
  - NuMaker-M032SE V1.3

4 Directory Information

The directory structure is shown below.

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

Figure 4-1 Directory Structure

5 Example Code Execution

1. Browse the sample code folder as described in the Directory Information section and double-click APROM_Bind_UID.uvproj.
2. Enter Keil compile mode.
   - Build
   - Download
   - Start/Stop debug session
3. Enter debug mode.
   - Run

6 Revision History

Date	Revision	Description
2022.03.08	1.00	1. Initially issued.

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.