How to test the backdoor key?

I use the pflash example to show you how to set the backdoor. The board I use is frdm-k82. The IDE is Keil.

1 configure the flash configuration to set the backdoor key. I set the key like the picture.

```
/* Flash Configuration */
    .section .FlashConfig, "a"
    .long 0xF0F0F0F0
    .long 0xF0F0F0F0
    .long 0xFFFFFFFF
    .long 0xFFFF3DBF

    .text
    .thumb
```

2 We need to configure the last byte of the flash configuration as BF. ‘B’ means that we enable the backdoor. ‘F’ means that we set the mcu as security state.

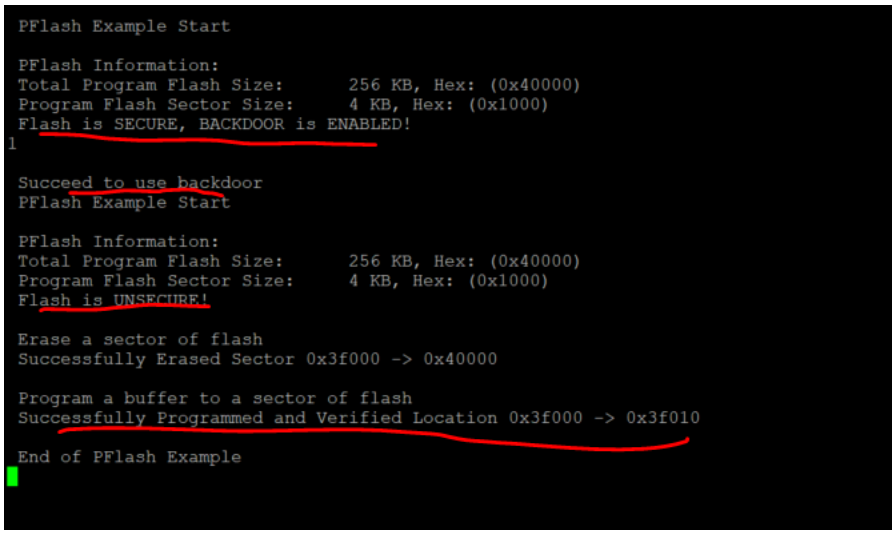
3 In main function, go to line 257. Modify the code like the picture.

```
241             s_buffer_rbc[i] = *(volatile uint32_t *)(destAdrss + i * 4);
242             if (s_buffer_rbc[i] != s_buffer[i])
243             {
244                 error_trap();
245             }
246         }
247
248         PRINTF("\r\n Successfully Programmed and Verified Location 0x%x -> 0x%x \r\n", destAdrss,
249                (destAdrss + sizeof(s_buffer)));
250
251         /* Erase the context we have progeammed before*/
252         /* Note: we should make sure that the sector which will be set as swap indicator should be blank*/
253         FLASH_Erase(&s_flashDriver, destAdrss, pflashSectorSize, kFTFx_ApiEraseKey);
254     }
255     else
256     {
257         uint8_t back_key[]={0xf0,0xf0,0xf0,0xf0,0xf0,0xf0,0xf0,0xf0};
258         status_t p = FLASH_SecurityBypass(&s_flashDriver,back_key);
259         PRINTF("%d\r\n",p == kStatus_FTFx_Success?1:0);
260         if(p == kStatus_FTFx_Success)
261         {
262             PRINTF("\r\n Succeed to use backdoor");
263             goto flashAgain;
264         }
265
266     }
267
268     app_finalize();
269
270     return 0;
271 }
```

The ‘flashAgain’ is here.

```
89
90  int main(void)
91 {
92     ftfx_security_state_t securityStatus = kFTFx_SecurityStateNotSecure; /* Return protecti
93     status_t result;    /* Return code from each flash driver function */
94     uint32_t destAdrss; /* Address of the target location */
95     uint32_t i, failAddr, failDat;
96
97     uint32_t pflashBlockBase  = 0;
98     uint32_t pflashTotalSize  = 0;
99     uint32_t pflashSectorSize = 0;
100
101    /* Init hardware */
102    BOARD_InitPins();
103    BOARD_BootClockRUN();
104    BOARD_InitDebugConsole();
105 flashAgain:
106    /* Clean up Flash, Cache driver Structure*/
107    memset(&s_flashDriver, 0, sizeof(flash_config_t));
108    memset(&s_cacheDriver, 0, sizeof(ftfx_cache_config_t));
109
110    /* Setup flash driver structure for device and initialize variables. */
111    result = FLASH_Init(&s_flashDriver);
112    if (kStatus_FTFx_Success != result)
113    {
114        error_trap();
115    }
```

Here is the result.



Now I explain what happened.

I set the mcu as security mode and enable the backdoor. So the console prints 'the Flash is secure, backdoor is enabled'.

Then it will run my code in line 256. Function 'FLASH_SecurityBypass' is used to set the mcu as unsecurity state by using the backdoor. I use the command 'goto' to run this flash example again. Because the flash is unsecure, it will run normally.