AN10851

Using Code Read Protection in LPC1700

Rev. 01 — 23 July 2009 Application note

Document information

Info	Content
Keywords	LPC1700, CRP, ISP, Code Security
Abstract	Using Code Read Protection (CRP) in LPC1700 devices.

Revision history

Rev	Date	Description
01	20090723	Initial version.

Contact information

For additional information, please visit: http://www.nxp.com

For sales office addresses, please send an email to: salesaddresses@nxp.com

1. Introduction

Code Read Protection is a mechanism that allows users to enable different levels of security in the system so they can protect both their software code and hardware.

LPC1700 devices have three different security levels: CRP1, CRP2, and CRP3. Each mode increases the security level, with CRP3 restricting any access to the device. In this application note we examine all these security levels and how to use them according to the security requirements. We also provide an example to test all of these modes. A Keil MCB1700 evaluation board, Keil uVision3 and Flash Magic tools are used for this.

CAUTION: **Although the example used in this application note was carefully tested, it is recommended that the user initially configure the device to a level lower than CRP3. Once the code is successfully tested, CRP3 can be used with confidence.**

2. Flash memory access methods

In general the LPC1700 flash memory can be accessed in two different ways:

- Using the JTAG flash programming interface: This is the method that Debug tools use in order to download code into the device and start/stop execution.
- Using In-System Programming (ISP): This method is provided by the boot loader using UART0 serial port.

3. Understanding CRP security levels

As the name implies, Code Read Protection (CRP) provides a method for users to protect their code from being read from the device flash. In this way, designers can prevent unauthorized users from obtaining the object code which could be disassembled or downloaded onto another hardware platform. For this purpose, CRP1 (Code Read Protection – Level 1) can be used. In this case, as well as with CRP2 and CRP3, JTAG access is blocked, so there is no way to read/erase/write flash using this method. Using ISP, flash content can't be read; only flash updates can be performed.

A further increase in security levels would involve a way to prevent the code from being modified by unauthorized users, e.g., someone could use ISP in order to partially update the flash (modify some sectors) or hack the code, possibly modifying code behavior, or simply causing the embedded system stop to work as expected. In these cases, CRP2 can be used, adding a restriction to partially update the flash via ISP. In this way, unauthorized users cannot modify the existing code as there is no way to modify some sectors, unless they first erase all flash content, which ultimately means the existing code will be lost.

In a higher level of protection, the user can also prevent others from downloading their own code, which would mean some kind of hardware protection, i.e., it will prevent others from reusing the hardware. In this last case, CRP3 prevents entering ISP by pulling P2.10 low (hardware mechanism which allows entering ISP when there is valid code in the user's flash). In this way, unauthorized users can't use ISP to access the device flash, so this mode provides the maximum level of protection.

The user should note that in effect, with CRP3 there is no way to update the user flash, which means no further code updates are possible. However, the user code could make use of Re-Invoke ISP (one of the In-Application Commands – IAP) which invokes the boot loader in ISP mode.

When we use Re-Invoke ISP, we are breaking CRP3 protection, which ultimately means we are downgrading to level CRP2. Although in this level we can't read the flash, we can download a new code. Of course, the user code should already have this "back door" prepared in order to break CRP3 when necessary, and the mechanism used for this would be kept secret as it will be the key to break with the hardware protection, as we saw above.

Fig 1 shows the different CRP levels and the different access allowed in each case.

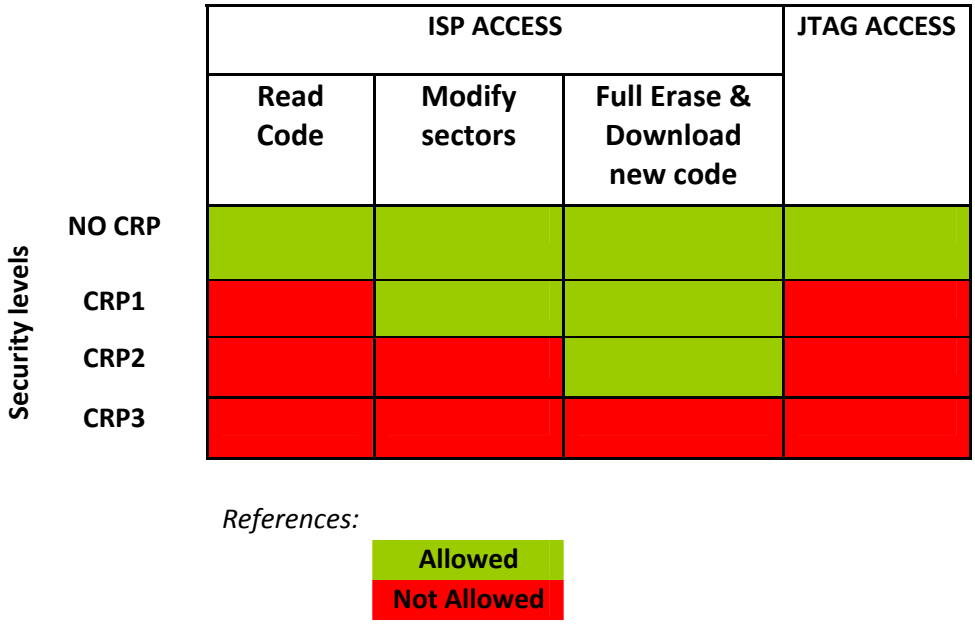

Fig 1. Flash device access according the CRP level.

It's worth noting that In-Application Programming (IAP) has no restrictions in any of these CRP levels.

In this application note, we are accompanying an example code, which includes one mechanism to break CRP3 level, in case it's needed.

4. Using the CRP_example

Unzip the software onto the PC's hard drive, and open the project using Keil tool chain (the evaluation version can be used). In this particular case, Keil version 3.70 was used.

Connect a serial cable between the Keil MCB1700 evaluation board, Serial port 0 (marked as COM0), and the PC's serial COM. Connect a USB cable to power the board from the PC. Please refer to the Keil board user's manual to verify the correct jumper settings (in order to use ISP).

Open Flash Magic (version 5.14 was used in this test) and configure Communications parameters (device, COM port, baud rate, interface, and oscillator). Please refer to the Flash Magic user's manual for more information. Fig 2 shows the initial configuration.

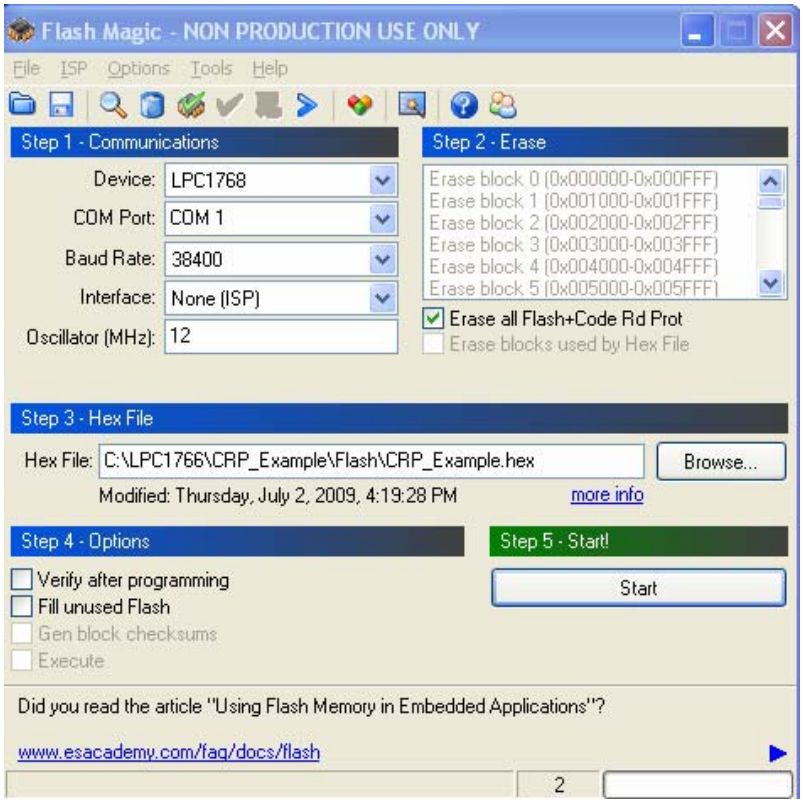

Fig 2. Flash Magic configuration

The code is a modified version of the Blinky example that comes with Keil, but with the CRP level addition. Opening the ***startup_LPC17xx.s*** file, and using the Configuration Wizard, we can select the desired CRP level. Fig 3 shows this.

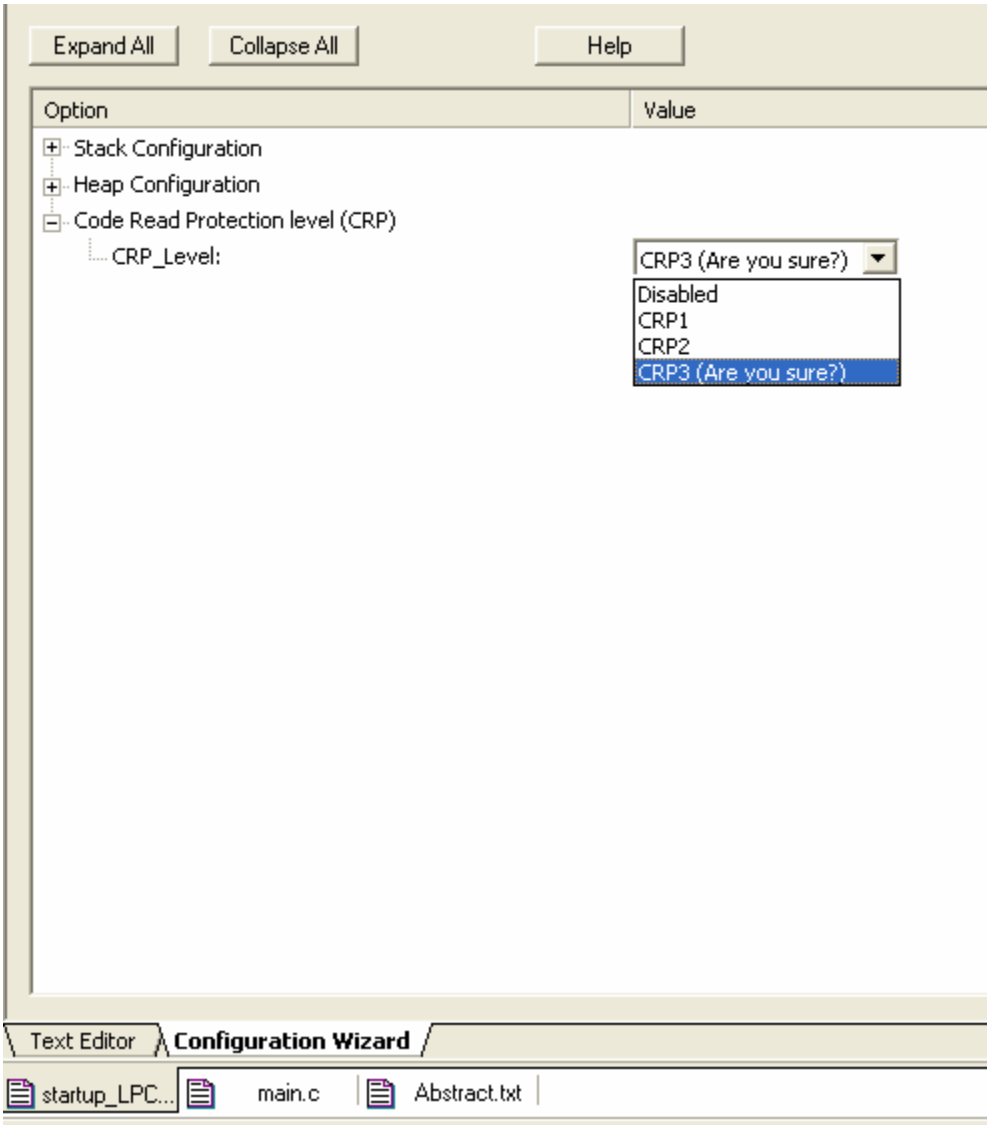

Fig 3. Configuring the CRP level

The ***main.c*** file contains additional modifications which allow breaking CRP3 using a hardware mechanism. In this example, we are using the central button of the Joystick (connected to P1.20) as the trigger to invoke boot loader in ISP mode. Please refer to Fig 3.

```
64      gpio->FIOPIN |=  led_mask[num];
65      Delay(200);
66      gpio->FIOPIN &= ~led_mask[num];
67      Delay(100);
68      /* detect if user pressed Re-Invoke button  */
69      if ((GPIO1->FIOPIN & 0x00100000) == 0)
70        break;
71      /* if timeout is enabled, check timeout     */
72      if (SysTickCnt > TIMEOUT && TIMEOUT)
73        break;
74    }
75
76    /* Re-Invoke ISP  */
77    __disable_irq();
78    command[0] = 57;       // Reinvoke ISP command
79    iap_entry (command, result);
80
81    /* code should not get here... */
82    while(1);
83  }
```

1

2

3

Fig 4. Code modification in main.c file

In line (1), we are reading P1.20 in order to detect if the user pressed the Joystick central button. When pressed, this input goes low and then the break is executed causing the exit of the loop which keeps the LEDs blinking.

As an additional way to ensure the CRP3 protection will be broken, and in case the above mechanism fails, a timer is included which will cause the code to exit the loop after approximately 10 seconds. See line (2). Although not recommended, this timer can be disabled in the following define located at the top of the ***main.c*** file;

```
#define TIMEOUT     10000           /* Timeout   (0 to disable)        */
```

The purpose of this timer is to ensure that the hardware will not be blocked with CRP3 while running these tests. In a real application, this timer would not make sense, and a more robust and secure mechanism should be considered.

Finally, in line (3), the IAP command (57 – Re-Invoke ISP) is called which will invoke the boot loader in ISP, so the user will be able to download a new code using the Flash Magic tool. In this way, as CRP3 protection was broken, the device will be in CRP2 level.

When a code with CRP3 mode enabled is downloaded into the device, Flash Magic will alert the user with a message as shown in Fig 5.

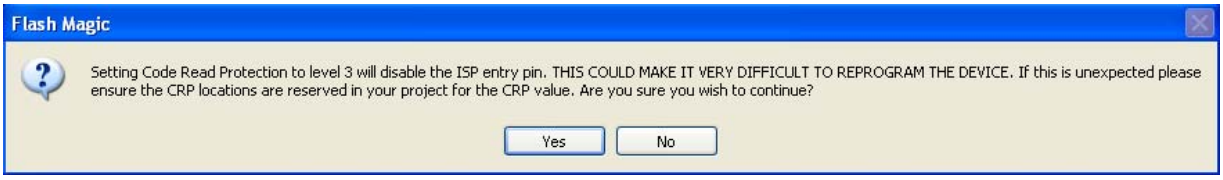

Fig 5. Message shown when Flash Magic detects the code has CRP3 enabled

5. Legal information

5.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

5.2 Disclaimers

General — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in medical, military, aircraft, space or life support equipment, nor in applications where failure or malfunction of a NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors accepts no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is for the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from national authorities.

5.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are property of their respective owners.

6. Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, email to: salesaddresses@nxp.com

Date of release: 23 July 2009
Document identifier: AN10851_1