AN11581

Code Read Protection in LPC1800 and LPC4300

Rev. 1 — 12 August 2014 Application note

Document information

Info	Content
Keywords	LPC1800, LPC4300, CRP, ISP, Code Security.
Abstract	This application note describes how to use Code Read Protection (CRP) in LPC1800 and LPC4300 devices with on-chip flash.

Revision history

Rev	Date	Description
1	20140812	Initial version

Contact information

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

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

1. Introduction

Code Read Protection (CRP) is a mechanism that allows developers to enable different levels of security on-chip memory to protect their software code and hardware.

In the LPC1800 and LPC4300 flash based devices when CRP is enabled, three different security levels are available. Each mode increases the security level, with CRP3 restricting any further access to the device. This application note examines the various security levels and describes how to choose the correct levels based on the user's security needs. Example code is provided to test all of the CRP modes.

CAUTION: Although the example used in this application note was carefully tested, it is recommended that the user initially configures the device to a level lower than CRP3. CRP3 security level can be used after the code has been successfully tested and is irreversible.

2. Flash memory access methods

Developers can access the LPC1800 and LPC4300 flash memory in two ways:

- Using the JTAG/SWD flash programming interface: The debug tools use this method to download code into the device and to start or stop code execution.
- Using In-System Programming (ISP): The boot loader supports this method using the UART0 serial port.

3. Understanding CRP security levels

CRP allows users to protect the code from being read from the device flash. It prevents unauthorized users from obtaining the binary code, disassembling or downloading it onto another hardware platform.

3.1 Code Read Protection disabled

When CRP is disabled, JTAG access is not restricted and no level of security is available to protect user code. It is possible to program, read, write, and erase flash content.

3.2 Code Read Protection Level 1 (CRP1)

When CRP1 is enabled, JTAG access is blocked and it is not possible to read, write, or erase flash content. When ISP is enabled, flash content cannot be read but partial flash updates can be performed.

3.3 Code Read Protection Level 2 (CRP2)

The CRP2 level of security restricts unauthorized users from updating the flash partially or modifying the code behavior. When CRP2 is enabled, no section of the code can be modified or updated without erasing all of the existing flash content. In CRP2 as in CRP1, the flash is read-protected.

3.4 Code Read Protection Level 3 (CRP3)

The CRP3 level of security is the highest mode of protection and restricts unauthorized users from downloading code to any part of the flash. It prevents others from re-using the hardware with their own application. The CRP3 level prevents the use of ISP to access the device flash by pulling the P2_7 to a LOW mode. In CRP3, the flash is read-protected as in CRP1 and CRP2.

While the CRP3 level of security prevents any update to the flash content, the user code can use the Re-Invoke ISP command to invoke the boot loader in the ISP mode. When the Re-Invoke ISP command is used, the CRP3 level of security is downgraded to the CRP2 level. Although in the CRP2 level of security the flash cannot be read, a new set of code can be downloaded. Therefore, it is important to create a provision in the code to allow for this “backdoor entry” event into the flash.

Fig 1 shows the various CRP levels of security and the ISP and JTAG access to the flash allowed in each case.

Note: In-Application Programming (IAP) has no restrictions at any CRP level.

SECURITY LEVEL	ISP ACCESS			JTAG ACCESS
	Read Code	Modify sectors	Full Erase & Download Code	
NO CRP	Enabled	Enabled	Enabled	Enabled
CRP1	Disabled	Enabled	Enabled	Disabled
CRP2	Disabled	Disabled	Enabled	Disabled
CRP3	Disabled	Disabled	Disabled	Disabled

Fig 1. Flash device access according to the CRP level

4. Programming CRP levels

LPC1800 and LPC4300 flash based devices usually contain two flash banks: flash bank A and flash bank B. Some devices have only one flash bank available. Program a CRP pattern at address 0x1A00 02FC for flash bank A or at 0x1B00 02FC for flash bank B depending on the active boot flash bank. Any CRP level that is included in the flash image of the selected bank applies to the entire flash - bank A and bank B.

Fig 2 shows the CRP patterns programmed to implement various security levels.

CRP Security Level	CRP Pattern
CRP Disabled	0xFFFF FFFF
CRP1	0x1234 5678
CRP2	0x8765 4321
CRP3	0x4321 8765

Fig 2. CRP patterns for different CRP levels

The CRP disabled pattern by convention is 0xFFFF FFFF but it can be of any value that does not match the CRP1, CRP2, or CRP 3 values.

5. Using the CRP example

The demonstration code is implemented in three tool chains: Keil MDK, LPCXpresso IDE, and IAR Workbench.

Fig 3 shows the Keil MCB1800/4300 evaluation board with LPC1857/LPC4357 mounted on it and is used in this example. The Evaluation board (OM # 13040) can be ordered from the following link: http://www.nxp.com/demoboard/OM13040.html#overview.

Flash Magic is a PC tool for programming flash based microcontrollers that allows easy access to all the ISP features provided by NXP MCUs. The PC tool can be downloaded from the following link: http://www.nxp.com/redirect/flashmagictool.com/.

To set up the Keil MCB1800/4300 evaluation board:

- Connect a serial cable from UART0 on the Keil board to the PC.
- Connect a USB cable to power the board.

Fig 3. Keil MCB1800/4300 Evaluation Board

5.1 Software settings for LPCXpresso IDE

Support for setting up the CRP memory location is provided via a combination of the Project Wizard, a header file and a number of macros. This support allows specific values to be easily placed into the CRP memory location, based on the user's requirements.

The New Project wizard contains an option to allow linker support for placing a CRP word to be enabled when you create a new project. This is typically enabled by default. This wizard option actually then controls the “Enable CRP" checkbox of the Project Properties linker Target tab. See Fig 4.

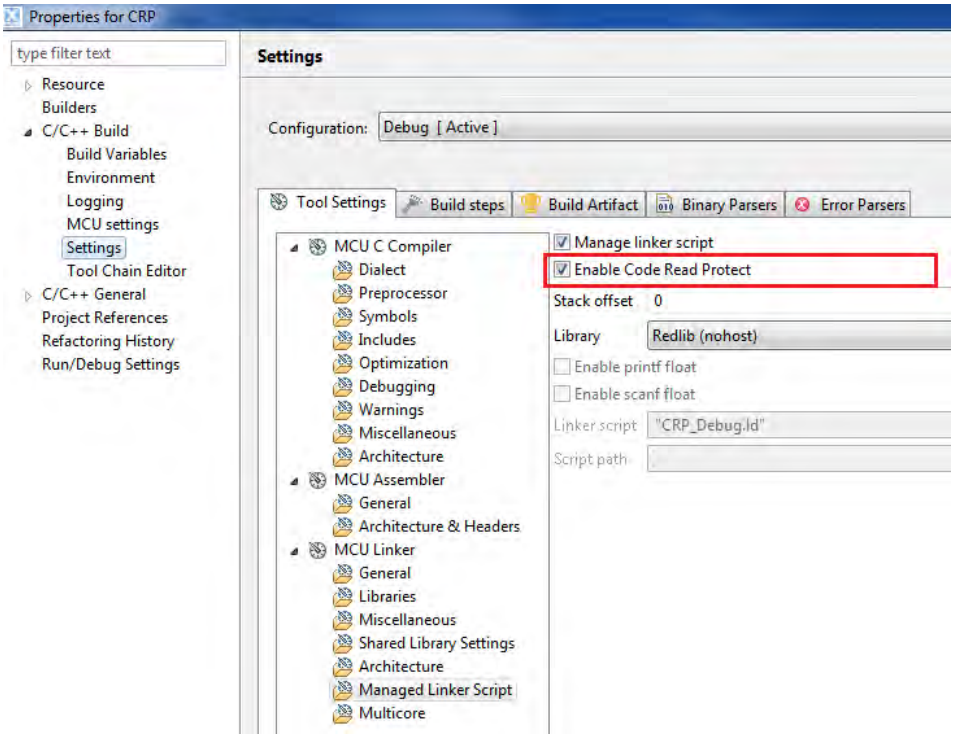

Fig 4. Enable Code Read Protect checkbox

The wizard creates a '*crp.c'* file that defines the *'CRP_WORD'* variable containing the required CRP value. The '*crp.c'* file contains the following statements.

```
1    #include<NXP/crp.h>
2    __CRP const unsigned int CRP_WORD = CRP_CRP1;
```

The different CRP constants needed for implementing the CRP levels can be found in the '*NXP/crp.h'* header file. By changing the CRP_WORD variable, the desired CRP level is achieved.

5.2 Software settings for Keil MDK IDE

Keil MDK uses the startup file *"*.s"*. The following code in Fig 5 is placed in the startup file before the Reset Handler.

```
No_CRP          EQU     0xFFFFFFFF
CRP_Level_1     EQU     0x12345678
CRP_Level_2     EQU     0x87654321
CRP_Level_3     EQU     0x43218765

                IF      :LNOT::DEF:NO_CRP
                AREA    |.ARM.__at_0x1A0002FC|, CODE, READONLY
CRP_Key         DCD     CRP_Level_1
                ENDIF

                AREA    |.text|, CODE, READONLY
```

Fig 5. Excerpt from CRP example

The *CRP_Key can be changed* based on the CRP level of security.

For example, in Fig 5 the CRP level is set to Level 1.

5.3 Software settings for IAR Workbench IDE

Enabling CRP in IAR is a two-step process:

- Edit the ICF file.
- Declare the constants.

Fig 6 shows how to modify the "*.*icf*" file.

The *icf* files can be found in the Embedded Workbench installation directory: Embedded Workbench -> arm -> config-> linker->NXP.

```
define symbol __ICFEDIT_intvec_start__ = 0x1A000000;
define symbol __ICFEDIT_crp_start__    = 0x1A0002FC;
/*-Memory Regions-*/
define symbol __ICFEDIT_region_ROM_start__ = 0x1A000300;
define symbol __ICFEDIT_region_ROM_end__   = 0x1B07FFFF;
define symbol __ICFEDIT_region_RAM_start__ = 0x20000000;
define symbol __ICFEDIT_region_RAM_end__   = 0x2000FFFF;

........

place at address mem:__ICFEDIT_intvec_start__ { section .intvec };
place at address mem:__ICFEDIT_crp_start__ { readonly section .crp};
place in ROM_region     { readonly };
```

Fig 6. Modifications in ICF file

Fig 7 shows how to add the CRP constants to the "*main.c*" file.

```
/*CRP constants */
#define NO_CRP          0xFFFFFFFF
#define CRP_Level_1     0x12345678
#define CRP_Level_2     0x87654321
#define CRP_Level_3     0x43218765
const __root uint32_t CRP_WORD@".crp" = CRP_Level_1;
```

Fig 7. Excerpt from CRP example

5.4 Running the application

The demonstration code sets the CRP security levels in flash bank A. If Flash Bank B is the active boot bank, the CRP patterns are written to location 0x1B00 02FC.

Note: Flash Magic tool and UART0 access are required to recover the board. Any CRP change becomes effective only after the device has gone through a power cycle.

Build and download the project after setting the required CRP level in the software.

On power cycling the board, the LED PD_10 starts to blink. JTAG access is blocked, making debugging impossible. In CRP levels 1 and 2, the device can enter ISP mode. Fig 8 shows how to read the security level in the Flash Magic tool.

The *"main.c"* file contains additional modifications that allow a "backdoor entry" into the flash and the CRP3 level to break using a hardware mechanism. In this example, pin P4_0 is used as the trigger to invoke boot loader in the ISP mode. When the button P4_0 is pressed, LED PD_10 is OFF and LED P9_1 is ON indicating that the ISP mode has been entered using the Re-Invoke ISP function. CRP level 3 is downgraded to CRP level 2. Flash Magic can be used to download a new code or erase the chip.

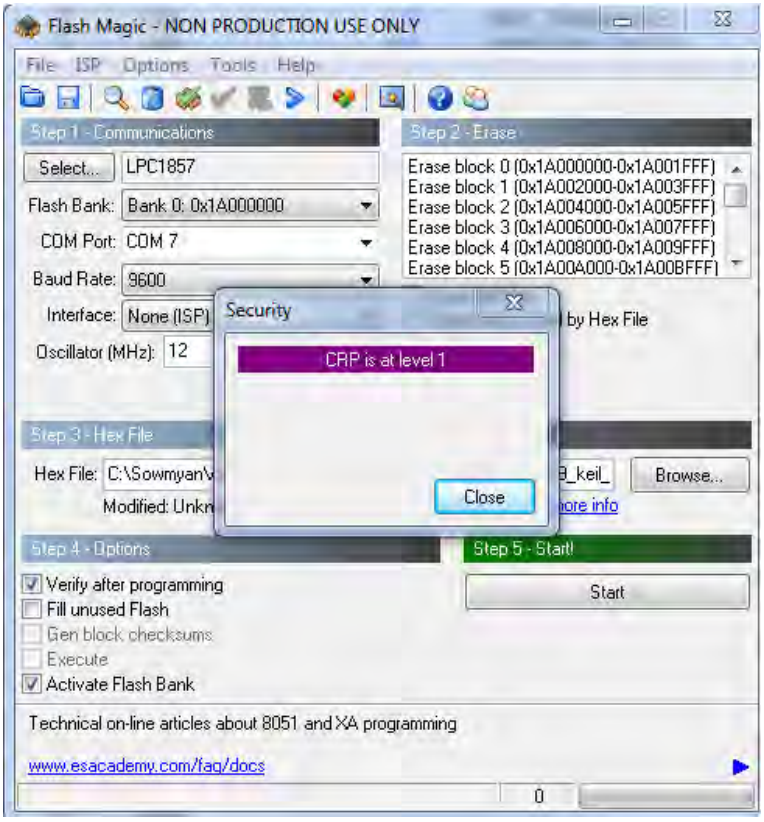

Fig 8. Read security level in Flash Magic

In case the hardware mechanism does not work to break and downgrade the CRP3 level of security, a timer can be included to cause the code to exit the loop after approximately 10 seconds. Although not recommended, this timer can be disabled in the following location at the top "*main.c"* file.

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

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

6. Conclusion

The Code Read Protection (CRP) feature in LPC1800 and LPC4300 provides three levels of security to restrict access to the on-chip flash and the use of JTAG and ISP. Implementing this method adds code level security in the application and provides IP protection.

7. Legal information

7.1 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.

7.2 Disclaimers

Limited warranty and liability — 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.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

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 life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an 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 at 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.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

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 competent authorities.

8. Contents

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

Date of release: 12 August 2014
Document identifier: AN11581