AN11653

Locking Flash Sectors on the LPC5410x

Rev. 1.0 — 12 October 2015 Application note

Document information

Info	Content
Keywords	LPC54100 series, Security, Flash Sector Protection, CRP
Abstract	This application note introduces the feature of locking flash sectors on the LPC54100 series. When a flash sector is locked, this irreversible feature protects against unwanted write and erase operations. A software example and external library is provided to illustrate the usage.

Revision history

Rev	Date	Description
1.0	20151012	Initial version.

Contact information

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

1. Introduction

On the LPC54100 series microcontroller, each flash sector can be “locked” against write and erase operations. This feature offers protection against intentional and inadvertent changes to the application code and data by permanently disabling the hardware’s ability to change the contents of a locked flash sector. In addition, there exists a Code Read Protection (CRP) feature that protects against unauthorized reads by disabling debugger access and can even disable the ISP pin. While CRP and securing flash sectors can accomplish similar security goals, CRP should not be confused with securing a flash sector because they would achieve these goals differently.

2. Locking flash sectors

A locked flash sector does not allow the alteration of data through any write or erase operations. IAP and ISP write and erase commands return a value as if the operation was successful but the internal voltages that alter the flash sector contents are not actually generated, making locked flash sectors behave like read-only memory. Also, a write or erase operation spanning across locked and unlocked sectors will fail and not alter the contents of any of the targeted sectors.

Locking flash sectors provides the means to protect code or data that should otherwise never be modified. For example, if a product is released to customers with the foresight of including the functionality for firmware updates in the field, it is likely the application is split into two sections: a section that must stay intact to perform the field updates, such as a secondary boot loader, and the rest of the application that can be updated. The secondary boot loader must stay untouched so that it can execute its responsibilities as designed. Under these circumstances, it is possible that an attacker or buggy program can alter the contents of the secondary boot loader. Locking the flash sector that the secondary boot loader resides in protects the secondary boot loader, guaranteeing some degree of functionality of the product that makes it salvageable in the field in case something goes wrong.

2.1 Caveats of locked flash sectors

After executing the flash locking function onto the targeted sectors, it will become locked upon the next reset signal. It is important to note that this process is irreversible, making the usability of the part limited for the rest of its lifetime. If a design makes use of this feature, it should only be activated in the final design phase.

Another caveat when locking flash sectors on the LPC5410x is that the startup code of the application is typically programmed into address 0x0 in flash sector 0. Certain MCU configurations are defined in this sector, such as which CRP setting is enabled. Due to the location of where these settings are defined, if flash sector 0 is locked, the configurations defined in this sector will also become permanent. When using CRP in conjunction with locking flash sector 0, it is important to consider the timing of when these two features are activated because CRP has the potential to disable the ability to trigger ISP mode through hardware and disable the SWD pins.

2.2 Locked flash sectors versus CRP

CRP is another security mechanism on the LPC5410x.There are three levels of CRP, starting at level 1, each providing more security than the previous level. Table 1 compares the differences between the three different CRP levels and locked flash sectors.

For more information on CRP, please refer to the LPC5410x user's manual:

http://www.nxp.com/documents/user_manual/UM10850.pdf

Table 1. CRP and Locked Flash Sector Comparison

	CRP1	CRP2	CRP3	Locked Flash Sector
IAP commands	Write/erase enabled	Write/erase enabled	Write/erase enabled	Read enabled
SWD access	Disabled	Disabled	Disabled	Enabled
ISP commands	Some write/erase enabled	Some erase enabled	Disabled	Read enabled
Process to disable security feature	Use ISP mode	Use ISP mode	Software backdoor to re-enable ISP mode	N/A

CRP is primarily used to prevent snooping of flash contents by disabling SWD access and limiting ISP commands while locking a flash sector prevents tampering of data. While they differ fundamentally, CRP can be used to obtain a similar goal as locking flash sectors. For example, if the goal is to prevent anyone from tampering with the application code or data, CRP level 3 can be used to disable the SWD pins to prevent debugger access and disable ISP mode. In this scenario, it is impossible for anyone to read or write flash data. The problem with this approach is that the necessary security is added by disallowing anyone from accessing the memory – including the programmer. If field updates are a required specification of the product, it would be necessary to implement a backdoor in the application that uses a secondary boot loader to update the firmware on the MCU. This backdoor, as well as the external program interfacing with the backdoor, become vulnerabilities that can be exploited to modify the secondary boot loader as well as any other part of the flash memory.

3. Flash sector locking software example

3.1 Objective

This application note provides a software example based on the LPCOpen software platform of NXP and supports three IDE toolchains: Keil MDK, IAR EWARM, and LPCXpresso.

The objective is to illustrate the usage of IAP commands on a locked and unlocked sector. The software example debugs to SRAM, which means the application can only be executed during a debug session and will be lost on a power cycle or reset.

3.2 Requirements

1. Keil MDK, IAR EWARM, and LPCXpresso.
2. NXP LPCXpresso LPC54102 Board.

3.3 Flash sector locking library

The software example attached to this application note provides a library with the necessary API to lock a flash sector. This library operates on a per sector basis. The size of an LPC5410x flash sector is 32 kB and the size of a page is 256 bytes. Table 2 lists the different sectors and their corresponding memory mapped address range on the LPC5410x. Only sectors 0-7 are applicable for variants of the LPC5410x that only have 256 kB of flash.

Table 2. LPC5410x Flash Sectors

Sector Number	Sector size (kB)	Page Numbers	Address Range
0	32	0 – 127	0x0000 0000 - 0x0000 7FFF
1	32	128 – 255	0x0000 8000 - 0x0000 FFFF
2	32	256 – 383	0x0001 0000 - 0x0001 7FFF
3	32	384 – 511	0x0001 8000 - 0x0001 FFFF
4	32	512 – 639	0x0002 0000 - 0x0002 7FFF
5	32	640 – 767	0x0002 8000 - 0x0002 FFFF
6	32	768 – 895	0x0003 0000 - 0x0003 7FFF
7	32	896 – 1023	0x0003 8000 - 0x0003 FFFF
8	32	1024 – 1151	0x0004 0000 - 0x0004 7FFF
9	32	1152 – 1279	0x0004 8000 - 0x0004 FFFF
10	32	1280 – 1407	0x0005 0000 - 0x0005 7FFF
11	32	1408 – 1535	0x0005 8000 - 0x0005 FFFF
12	32	1536 – 1663	0x0006 0000 - 0x0006 7FFF
13	32	1664 – 1791	0x0006 8000 - 0x0006 FFFF
14	32	1792 – 1919	0x0007 0000 - 0x0007 7FFF
15	32	1920 – 2047	0x0007 8000 - 0x0007 FFFF

3.3.1 Library functions

To lock a flash sector, the library and the ‘C’ header file supplied in the software example must be used. While locking a flash sector, the flash memory is not available for code execution, so it is a requirement that the application be executed from SRAM. The following tables show detailed information about the library.

Table 3. LPC5410x Flash sector locking function

Function Name	write_erase_secure_user_sector(unsigned start, unsigned end, unsigned cclk)
Input	**Param0:** Start sector number. **Param1:** End sector number. **Param2:** System clock frequency in kHz.
Status Code	LOCK_SUCCESS | INVALID_SECTOR | SECTOR_ALREADY_LOCKED | NOT_EXECUTING_IN_RAM | WRONG_PART
Description	This function is capable of locking one or more sectors of the on-chip flash memory. Once a sector has been locked, the ability of the hardware to alter the contents of the selected sector is forever lost.

Table 4. LPC5410x Flash

Function Name	write_erase_secure_get_version(void)
Input	None
Return value	Library version number.
Description	This function will return the current library version number.

Table 5. Library status codes

Status Code Value	Status Code Name	Description
300	LOCK_SUCCESS	The requested flash sector or sectors were successfully locked.
301	INVALID_SECTOR	The requested start and/or end sectors are invalid. The lock request fails.
302	SECTOR_ALREADY_LOCKED	One or more of the inputted sectors have already been locked. The lock request fails.
303	NOT_EXECUTING_IN_RAM	Application not executing in RAM. The lock request fails.
304	WRONG_PART	Library is not executing on the LPC5400 series. The lock request fails.

3.4 Flash sector locking software example

This software example contains IAP code that will modify flash sector 15, erasing and then writing a distinguishable sequence of numbers that is viewable in an IDE's memory window. There is a macro called "FLASH_LOCK_ENABLE" located on line 58 of the flash_sector_locking.c source file. This macro can be changed to a non-zero value to enable the application to lock flash sector 15. Once the application is executed as-is to write a recognizable pattern to flash sector 15, the flash sector locking code should be enabled and then re-compiled. When a new debug session has started, the memory window will show that the flash contents from the last debug session are still present. When the program runs, an IAP erase will erase the contents, lock the flash sector, and then attempt to write the same sequence of numbers.

1. Connect the USB cable to the J6 micro USB port to power-up the LPCXpresso V2 LPC54102 evaluation board.
2. Open the included project file for the IDE you wish you work with. Compile the chip and board libraries.
3. Compile the flash sector locking project. Erase the flash, download the new application and start a new debug session.
4. Run the program until the program reaches the while(1) loop at the end of main() and open the IDE's memory window to the start of flash sector 15 (address 0x0007 8000). The flash contents should look like Figure 1.

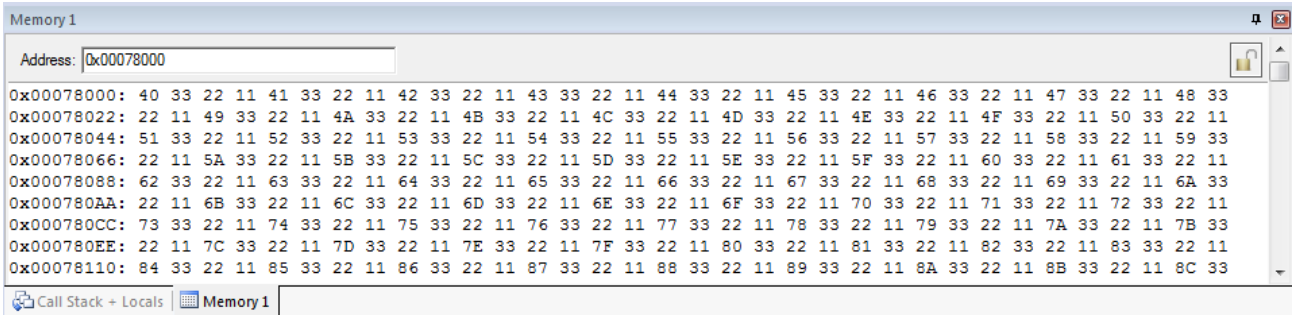

Fig 1. Result of IAP write before locking flash sector 15

5. Change the FLASH_SECTOR_LOCK_ENABLE macro to a value of 1 and re-compile the code. **This will make the contents of flash sector 15 permanent.**
6. Start a new debug session. The application will lock the flash sector and then proceed to do the same erase and write operations. Step through each function call to see where the flash contents is changed.
7. Exit the current debug session, apply a reset, and enter a new debug session. Step through each function call and notice that the flash contents do not change like they did in the previous debug session.

4. Conclusion

For applications that require security over the application code and data, the user has two choices: CRP or locking the flash sectors. CRP fulfills this goal by disallowing anything to connect to the MCU. Realistically, this is not practical so a backdoor is typically implemented in software so that the developer can still update the application. This means that there is still the possibility for an attacker to obtain access to the MCUs memory. The only way to guarantee the integrity of the flash memory is to lock the flash sectors of interest. This will permanently disable the ability of the hardware to alter any cell in a locked flash sector, making the flash sector tamper-proof. Use this feature with caution because it is permanent when activated.

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

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. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

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 and its suppliers accept 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.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

5.3 Licenses

Purchase of NXP <xxx> components
<License statement text>

5.4 Patents

Notice is herewith given that the subject device uses one or more of the following patents and that each of these patents may have corresponding patents in other jurisdictions.

<Patent ID> — owned by <Company name>

5.5 Trademarks

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

<Name> — is a trademark of NXP Semiconductors N.V.

6. List of figures

7. List of tables

8. Contents

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

Date of release: 12 October 2015

Document identifier: Locking Flash Sectors on the LPC5410x