TN00004

LPC134x sector lock mechanism for write/erase protection

Rev. 1 — 13 February 2012 **Technical note**

Document information

Info	Content
Keywords	Locking sectors, write/erase protection, ARM-based microcontroller, LPC1342FBD48, LPC1342FHN33, LPC1343FBD48, LPC1343FHN33, LPC134x

Revision history

Rev	Date	Description
1	20120213	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. Write/erase protection

In the NXP ARM-based LPC134x microcontroller, each flash sector can be protected against write/erase operation. This feature allows the application to protect the sensitive code/data against tampering. If the Code Read Protection (CRP) feature is enabled, then the sensitive code/data is also protected against unauthorized reads. Refer to the appropriate user manual for a description of the CRP feature.

Altering the contents of a protected sector is not possible. The write or erase operation (via ISP or IAP) on a protected sector succeeds but the internal erase/programming voltages to alter the flash sector contents are not generated. The write/erase protection feature is irreversible. Activate it only in the final design phase to avoid unusable parts/application boards. If CRP is enabled along with the write/erase protection on sector 0, then the CRP feature is also irreversible. However, if implemented by the system designer, an application executing from the internal memory can still communicate with the external world. If the flash sectors of this type of application are not protected against write/erase, they can be erased/programmed. A write/erase operation spanning across protected and unprotected sectors does not alter the contents of either protected or unprotected sectors.

The write/erase protection is enabled by calling the write_erase_secure_user_sector() function. This function is available in the library file. A ‘C’ header file (write_erase_secure.h) is also provided. While sectors are being protected, the flash memory is not available for code execution. Therefore, it is important to relocate functions in RAM during run time. Refer to the linker documentation for details. The following section describes the functions available in the library. The function return codes are described in Table 4.

1.1 Current release

write_erase_secure_2_00_LPC_23xx_24xx_ADS_1_2.a

write_erase_secure_2_00_LPC_23xx_24xx_gcc_3_4_2.a

1.2 write_erase_secure Library Functions

1.2.1 write_erase_secure_user_sector(unsigned start, unsigned end, unsigned cclk)

Table 1. write_erase_secure_user_sector function description

Function	write_erase_secure_user_sector(unsigned start, unsigned end, unsigned cclk)
Input Parameters	start: Start Sector Number end: End Sector Number: Should be greater than or equal to start sector number. cclk: System Clock Frequency (cclk) in kHz.
Return Code	SUCCESS | INVALID_SECTOR | SECTOR_ALREADY_SECURED | NOT_EXECUTING_IN_RAM | WRONG_PART
Description	This function is used to enable the write/erase protection on one or more sectors of on-chip Flash memory. A write/erase operation spanning across protected and unprotected sectors does not alter the contents of either protected or unprotected sectors. Sector protection is effective after a reset cycle.

1.2.2 write_erase_secure_boot_sector(unsigned cclk)

Table 2. write_erase_secure_boot_sector function description

Function	write_erase_secure_boot_sector(unsigned cclk)
Input Parameters	cclk: System Clock Frequency (cclk) in kHz.
Return Code	SUCCESS | SECTOR_ALREADY_SECURED | NOT_EXECUTING_IN_RAM | WRONG_PART
Description	This function is used to enable the write/erase protection on the boot sector of on-chip Flash memory. Sector protection is effective after a reset cycle.

1.2.3 write_erase_secure_get_version(void)

Table 3. write_erase_secure_get_version function description

Function	write_erase_secure_get_version(void)
Input Parameters	none
Return Code	Library version number(0x0000xxyy). Where xx is the major and yy is the minor version number.
Description	This function is used to get the write_erase_secure library version number.

Table 4. write_erase_secure Library Functions Return Codes Summary

Return Code	Mnemonic	Description
300	SUCCESS	Function is executed successfully.
301	INVALID_SECTOR	Sector number is invalid or end sector number is greater than start sector number.
302	SECTOR_ALREADY_SECURED	One or more sectors are already protected.
303	NOT_EXECUTING_IN_RAM	write_erase_secure Library function is not executing in RAM.
304	WRONG_PART	write_erase_secure Library function is executing in wrong part.

2. Legal information

2.1 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.

2.2 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.

2.3 Trademarks

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

3. Contents

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

Date of release: 13 February 2012
Document identifier: TN00004