AN10809

LPC29xx flash features

Rev. 01 — 13 April 2009 Application note

Document information

Info	Content
Keywords	LPC29xx, flash
Abstract	This Application Note describes the features of embedded flash of the LPC29xx device. Code protection, signature generation and JTAG security are introduced and discussed. Software examples to access these features are also presented in associated Zip file.

Revision history

Rev	Date	Description
01	20090413	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

The LPC2900 includes up to 768 kB flash memory system. This memory can be used for both code and data storage. Flash memory can be programmed in-system via JTAG. The LPC2900 embedded Flash offers some special features: JTAG security, sector security, customer information storage, and signature generation.

2. Hardware and software

2.1 IDE toolchain

The Code supplied was developed with an evaluation version of Keil's uVision MDK V3.42c.

2.2 Evaluation board

The Keil MCB2900 evaluation board with a LPC2919/01 mounted is used in this application note. The code was also verified on a Hitex LPC2929/39 development board.

3. Flash features

As mentioned in the introduction, the LPC2900 Flash has some special features that will be introduced in the following sections. The features include:

- Signature Generation
- Sector Protection
- JTAG Security

3.1 Signature generation

The flash module contains a built-in hardware signature generator. This generator can produce a 128-bit signature (MISR) from a range of the flash memory. There is a 128-bit signature reflected by the four registers FMSW0, FMSW1, FMSW2 and FMSW3. There is also a 16-bit signature which is reflected by the FMS16 register.

The signature generated by the flash memory is used to verify the flash memory contents. The generated signature can be compared with an expected signature generated by software. It eliminates the time- and code-consuming procedure of reading back the entire contents.

The address range for generating a signature must be aligned on flash-word boundaries. Like erasing a sector or burning a page, the generation of a signature is an asynchronous action; i.e. after starting generation the module begins calculating the signature, and during this process any access to the flash results in wait-states. To serve interrupts or perform other actions this critical code must be located outside flash memory region (e.g. internal RAM or TCM). The code that initiates the signature generation must also be located outside flash memory.

The snapshot shown in Fig 1 from the Keil IDE shows the 128-bit signature values calculated in software (refSignature) matching the hardware generated signature (signatureValue).

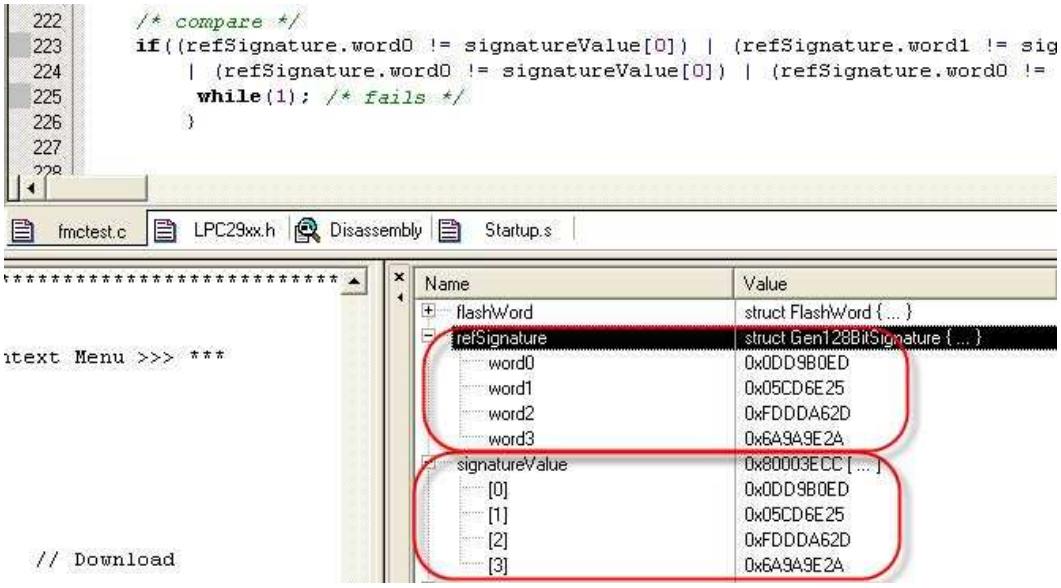

Fig 1. 128 bit signature values

The 16-bit signature can be generated in a similar manner.

3.2 Sector protection

To enable sector protection, it is necessary to program portion of the index sector of the Flash. The index sector is a special part of the flash array used for configuring flash parameters such as sector security, JTAG access and so on, Care should be taken when programming the index sector as the device JTAG can be disabled if the appropriate value is programmed. Once programmed the index sector cannot be erased.

The index sector becomes accessible when the FS_ISS bit in the FTCR register is set. During index sector programming ECC should be disabled. In the FTCTR register, set bits 29 and 28 to disable ECC. The index sector can also be used to program customer-specific information. Index sector page 5 (32 flash words) can be programmed at the customer's discretion.

Sector protection is a feature for setting sectors to Read-Only. It is possible to enable this feature for each individual sector. Once it has been enabled it is no longer possible to write (erase/burn) to the sector. This feature can be used, for example, to prevent a boot sector from being replaced. For each sector in flash memory there is a corresponding flash-word in the index sector that defines whether it is secured or not. After enabling flash memory security, this feature is not activated until the next reset.

Index sector pages 6 and 7 are used to control the Sector security features. To enable the sector security, a 128bit flash word (4 times 0x0000 0000) is programmed to the appropriate flash-word address in the index sector. Table 1 shows the correlation between the flash sectors and the corresponding index sector address.

Table 1. Index sector flash-words

Flash memory address range		Index sector page #	Flash memory sector #	Flash-word address (FS_ISS bit set)
0x2000 0000 -	0x2000 1FFF	6	11	0x2000 0CB0
0x2000 2000 -	0x2000 3FFF	6	12	0x2000 0CC0
0x2000 4000 -	0x2000 5FFF	6	13	0x2000 0CD0
0x2000 6000 -	0x2000 7FFF	6	14	0x2000 0CE0
0x2000 8000 -	0x2000 9FFF	6	15	0x2000 0CF0
0x2000 A000 -	0x2000 BFFF	7	16	0x2000 0E00
0x2000 C000 -	0x2000 DFFF	7	17	0x2000 0E10
0x2000 E000 -	0x2000 FFFF	7	18	0x2000 0E20
0x2001 0000 -	0x2001 FFFF	6	0	0x2000 0C00
0x2002 0000 -	0x2002 FFFF	6	1	0x2000 0C10
0x2003 0000 -	0x2003 FFFF	6	2	0x2000 0C20
0x2004 0000 -	0x2004 FFFF	6	3	0x2000 0C30
0x2005 0000 -	0x2005 FFFF	6	4	0x2000 0C40
0x2006 0000 -	0x2006 FFFF	6	5	0x2000 0C50
0x2007 0000 -	0x2007 FFFF	6	6	0x2000 0C60
0x2008 0000 -	0x2008 FFFF	6	7	0x2000 0C70
0x2009 0000 -	0x2009 FFFF	6	8	0x2000 0C80
0x200A 0000 -	0x200A FFFF	6	9	0x2000 0C90
0x200B 0000 -	0x200B FFFF	6	10	0x2000 0CA0

3.3 JTAG security

There are two levels of security implemented on the LPC2900, soft and hard security. These are described in more detail below.

3.3.1 Soft security

To enable JTAG security, a 128-bit flash word (4 times 0x7FFF FFFF) is programmed to the address 0x2000 0A30 in the index sector. After the next power on reset, JTAG access will be disabled but can be re-enabled by software.

In the case of soft security, software must enable JTAG during startup before a counter in the LPC2900 security block reaches 0. Otherwise the JTAG will remain disabled.

To re-enable JTAG and override this JTAG security setting, it is necessary to have a piece of code in the Flash (in the user program or application) that sets bit 0 in the SEC_DIS register (0xE000 1B00) to '1' before the counter times out. If the counter has expired before the SEC_DIS is set, the JTAG will remain locked. The counter runs off OSC1M, and the counter register is 11 bits, or 2047 counts.

The SEC_STA (0xE00 1B04) register can be monitored to determine the current status of JTAG security. The FEAT3 (0xE000 010C) register bit 31 indicates the state of security for the LPC2900 regardless of the override in the SEC_DIS register.

```
123 ;*******************************************************************************
124 ;*  Reset Entry                                                                *
125 ;*  Function : void ResetInit(void)                                            *
126 ;*      Parameters                                                             *
127 ;*          input  : None                                                      *
128 ;*          output : None                                                      *
129 ;*******************************************************************************
130 ResetInit
131
132     BL      Release_Security  ; write 1 to 0xe0001b00 to release security
133
134     ; Set global core configurations
135     MRC     p15, 0, r4, c1, c0, 0   ; Read CP15
136     ORR     r4, r4, #DTCM_enabled   ; Enable Data TCM
137     ; At power up, the interrupt vector is mapped to addr. 0 already,
138     ; enabling instruction TCM will wipe out the mirror of the
139     ; vector table. A remap will be performed there after. */
140     ORR     r4, r4, #ITCM_enabled   ; Enable Instruction TCM
141     ORR     r4, r4, #WB_enabled      ; Enable Write Buffer
142     MCR     p15, 0, r4, c1, c0, 0   ; Write CP15
143
144     BL      InitStack       ;Initialize the stack
145     BL      VectorRemap
146
147     BL      TargetResetInit ;Initialize the target board
148                     ;Jump to the entry point of C program
149
150     B       __main
```

Fig 2. Startup.s code snippet

Fig 2 contains a snippet of code from Startup.s showing the call to 'Release_Security' function.

3.3.2 Hard security

In this case, following the procedure outlined above for soft security, JTAG access is disabled. The code in flash does not attempt to set SEC_DIS to '1' and thus the device JTAG remains locked.

4. Program code

See associated software in the zip file "LPC29xx_samplecode.zip".

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: 13 April 2009
Document identifier: AN10809_1