AN11292

LPC1800/LPC4300 One-Time Programmable (OTP) configuration

Rev. 1 — 17 December 2012 Application note

Document information

Info	Content
Keywords	LPC1800, LPC4300, One-Time Programmable (OTP)
Abstract	This application note discusses how to program the user-programmable One-Time Programmable (OTP) configuration on the LPC1800 and LPC4300 devices.

Revision history

Rev	Date	Description
1	20121217	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 LPC18xx and LPC43xx are ARM Cortex-M3 and Cortex-M4 based microcontrollers for embedded applications. The ARM Cortex-M3 is a next generation core that offers system enhancements such as low power consumption, enhanced debug features, and a high level of support block integration. The ARM Cortex-M4 includes all this and adds a Floating-point coprocessor and a set of SIMD DSP math instructions.

Also present on the LPC18xx and LPC43xx is an on-chip ROM containing In-System Programming capability, as well as APIs for user code. The flash API implements a simple interface to the on-board flash and One-Time Programmable (OTP) configuration programming functionality.

This application note discusses how to program the user-programmable One-Time Programmable (OTP) configuration on the LPC1800 and LPC4300 families of parts. Key reasons to do this include permanently programming the boot mode selection to remove the need for external pull-ups/pulldowns, and enabling the encrypted boot functionality on “S” variants of the LPC1800/LPC4300 family.

The various topics covered in this application note are as follows:

1. How does OTP work?
2. One-Time Programming (OTP) Configuration Layout
3. OTP API
4. Sample Software
5. Conclusion

2. How does One-Time Programming (OTP) work?

OTP is integrated into the LPC1800/LPC4300 families. Polysilicon fuses are used on the die. The OTP bits start out set to zero, and as each fuse is blown, the corresponding bit changes to a 1. The OTP bit changes are irreversible. The current needed to blow the OTP fuses is taken from the VPP pin on the LPC1800/LPC4300. It can be up to 30 mA for a brief period. During this time, VPP must be kept >= 2.7 V. Some package options for the LPC1800/LPC4300 do not have a VPP pin. In this case, the VPP pin is internally connected to VDDIO, and the VDDIO pin must be kept >= 2.7 V to program the OTP fuses. The programming time for the OTP fuses is 1.6 mS or less.

3. One-Time Programming (OTP) configuration layout

The LPC18xx/LPC43xx's OTP configuration fuses control a number of functions, listed below and on the next page. Normally it is not necessary to read these OTP values directly; they are intended to modify the behavior of the LPC1800/LPC4300 boot ROM.

3.1 OTP memory description (OTP base address 0x4004 5000)

OTP bank	Word	Access	Address offset	Size	Description	Reference
0	0	Pre-programmed; cannot be changed by the user.	0x000	32 bit	Reserved	-
0	1	Pre-programmed; cannot be changed by the user.	0x004	32 bit	Reserved	-
0	2	Pre-programmed; cannot be changed by the user.	0x008	32 bit	Reserved	-
0	3	Pre-programmed; cannot be changed by the user.	0x00C	32 bit	Reserved	-
1	0	User programmable; initial state = 0	0x010	32 bit	General purpose OTP memory 0, word 0, or AES key 0, word 0	-
1	1	User programmable; initial state = 0	0x014	32 bit	General purpose OTP memory 0, word 1, or AES0 key 0, word 1	-
1	2	User programmable; initial state = 0	0x018	32 bit	General purpose OTP memory 0, word 2, or AES0 key 0, word 2	-
1	3	User programmable; initial state = 0	0x01C	32 bit	General purpose OTP memory 0, word 3, or AES0 key 0, word 3	-
2	0	User programmable; initial state = 0	0x020	32 bit	General purpose OTP memory 1, word 0, or AES key 1, word 0	-
2	1	User programmable; initial state = 0	0x024	32 bit	General purpose OTP memory 1, word 1, or AES key 1, word 1	-
2	2	User programmable; initial state = 0	0x028	32 bit	General purpose OTP memory 1, word 2, or AES key 1, word 2	-
2	3	User programmable; initial state = 0	0x02C	32 bit	General purpose OTP memory 1, word 3, or AES key 1, word 3	-
3	0	User programmable; initial state = 0	0x030	32 bit	Customer control data	Table 12
3	1	User programmable; initial state = 0	0x034	32 bit	General purpose OTP memory 2, word 0, or USB ID	Table 13
3	2	User programmable; initial state = 0	0x038	32 bit	General purpose OTP memory 2, word 1	Table 14
3	3	User programmable; initial state = 0	0x03C	32 bit	General purpose OTP memory 2, word 2	Table 14

Fig 1. OTP memory description

3.2 OTP memory bank 3, word 0 – Customer control data (address offset 0x030)

Bit	Symbol	Value	Description
28:25	BOOT_SRC		Boot source selection in OTP. For details, see Table 17.
		0000	External pins
		0001	UART0
		0010	Reserved
		0011	EMC 8-bit
		0100	EMC 16-bit
		0101	EMC 32-bit
		0110	USB0
		0111	USB1
		1000	SPI (via SSP)
		1001	UART3
29	-		Reserved. Do not write to this bit.
30	-		Reserved. Do not write to this bit.
31	JTAG_DISABLE		If this bit set, JTAG cannot be enabled by software and remains disabled. For use of this bit, see Section 4.1.

Fig 2. OTP memory bank 3, word 0

3.3 OTP memory bank 3, word 1 – General purpose OTP memory 2, word 0, or USB ID (address offset 0x034)

Bit	Symbol	Description
15:0	USB_VENDOR_ID	If USB_ID_ENABLE bit not set, it is used as general purpose OTG memory 2, word 0, GP2_0.
31:16	USB_PRODUCT_ID	

Fig 3. OTP memory bank 3, word 1

3.4 OTP memory bank 3, word 2/3 – General purpose OTP memory 2, word 1/2 (address offset 0x038/0x03C)

Bit	Symbol	Description
31:0	GP2_1	General purpose OTG memory 2, word 1.

Fig 4. OTP memory bank 3, word 2/3

4. OTP API

The OTP API exists in the LPC1800/LPC4300 ROM. It can be accessed via a jump table whose address is stored in ROM at 0x1040 0104. The API calls use ARM's Procedure Call Standard for the ARM Architecture for accepting and returning parameters.

4.1 OTP API calls

Table 1. OTP API calls

API call	Jump table entry	Description
`uint32_t ROM_otp_Init(void)`	0	Returns LPC_OK if init succeeds.
`uint32_t otp_ProgBootSrc(uint32_t src)`	1	Programs the boot mode. Returns LPC_OK if successful.
`uint32_t otp_ProgJTAGDis(void)`	2	Permanently disables JTAG and SWD ports.
`uint32_t otp_ProgUSBID(uint32_t prod_id, uint32_t vend_id)`	3	Programs a USB product and vendor ID to be used during USB DFU firmware updates.
`uint32_t otp_ProgGP0(uint32_t data, uint32_t mask)`	8	Program general purpose OTP bits 0. Only bits set both in data and mask will be programmed.
`uint32_t otp_ProgGP1(uint32_t data, uint32_t mask)`	9	Program general purpose OTP bits 1. Only bits set both in data and mask will be programmed.
`uint32_t otp_ProgGP2(uint32_t data, uint32_t mask)`	10	Program general purpose OTP bits 2. Only bits set both in data and mask will be programmed.
`uint32_t otp_ProgKey1(uint8_t *key)`	11	Programs AES key 1. Key should be presented as a C array with the least-significant byte first.
`uint32_t otp_ProgKey2(uint8_t *key)`	12	Programs AES key 2. Key should be presented as a C array with the least-significant byte first.
`uint32_t otp_GenRand(void)`	13	Returns a random number from the hardware random number generator.

Here is a list of error codes that may be returned by the OTP functions above.

4.2 OTP API error codes

Table 2. OTP API error codes

Error code	Error name
0x00000000	LPC_OK
0xFFFFFFFF	ERR_FAILED
0x00010001	ERR_API_INVALID_PARAMS
0x00010002	ERR_API_INVALID_PARAM1
0x00010003	ERR_API_INVALID_PARAM2
0x00010004	ERR_API_INVALID_PARAM3
0x00010005	ERR_API_MOD_INIT
0x00070001	ERR_OTP_WR_ENABLE_INVALID
0x00070002	ERR_OTP_SOME_BITS_ALREADY_PROGRAMMED
0x00070003	ERR_OTP_ALL_DATA_OR_MASK_ZERO
0x00070004	ERR_OTP_WRITE_ACCESS_LOCKED
0x00070005	ERR_OTP_READ_DATA_MISMATCH
0x00070006	ERR_OTP_USB_ID_ENABLED
0x00030001	ERR_SEC_AES_KEY_ALREADY_PROGRAMMED

5. Sample software

The sample software demonstrates how to call the OTP API in the LPC1800/LPC4300 on-chip ROMs.

5.1 otprom.[c|h]

Otprom .c contains code to initialize function pointers to point to each of the ROM OTP API functions. Otprom.h declares the function prototypes.

5.2 OTP boot source project

The OTP project, when built and run, will program the boot mode to boot from external QSPI flash. After the boot mode is programmed, the part will always attempt to boot from an external QSPI flash even without the use of external pull-ups or pulldowns.

5.3 AES key project

The AES key project, when built and run, will program an AES key to support secure booting from an LPC18S00 or LPC43S00 part and then blow the JTAG disable fuse. After the key is programmed, the part will not boot except from an encrypted program image and debugging will no longer be possible. The encrypted program image can be created with the use of the image_manager_aes.exe executable; contact your local NXP support team for this binary. We manage distribution of this executable due to US export regulations.

6. Conclusion

In conclusion, the on-chip OTP ROM API can be used to permanently configure the LPC1800/LPC4300 parts to consistently boot from the same boot source with fewer external components, and it can be used to configure tamper-resistant encrypted booting in the LPC18S00/LPC43S00 parts.

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. 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.

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.

7.3 Trademarks

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

8. Contents

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

Date of release: 17 December 2012
Document identifier: AN11292