AN11649

LPC18Sxx/43Sxx Hardware Versus Software AES Benchmark

Rev. 1.0 — 18 February 2015 Application note

Document information

Info	Content
Keywords	LPC18Sxx, LPC43Sxx, Hardware AES
Abstract	The application note illustrates the difference in encryption/decryption speed of the on-chip hardware AES engine versus software AES implementation.

Revision history

Rev	Date	Description
1.0	20150218	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 LPC18Sxx/43Sxx devices are ARM Cortex-M4 based microcontrollers for embedded applications which include an ARM Cortex-M0 coprocessor, up to 264 kB of SRAM, security features with AES engine, advanced configurable peripherals such as the State Configurable Timer/PWM (SCTimer/PWM) and the Serial General-Purpose I/O (SGPIO) interface, two High-speed USB controllers, Ethernet, LCD, an external memory controller, and multiple digital and analog peripherals.

The AES engine is used for encryption and decryption of the boot image and data with DMA support and is programmable via ROM-based APIs. Two One-Time Programmable (OTP) memory banks (128 bit each) are available for AES key storage.

2. Software encryption vs hardware encryption

The AES -128 implemented in software uses the CPU resources for performing encryption and decryption operations. In hardware encryption, the AES engine is integrated on-chip, therefore, encryption and decryption operations are performed without involvement of the CPU. This offloads the CPU, allowing it to perform other tasks and improve system performance.

Hardware encryption has several advantages over software encryption. Hardware encryption is:

- Fast as a dedicated hardware block is used for encryption process.
- Keys are secure as they are stored in OTP memory banks.
- Prevention of brute force and cold boot attacks.
- Authentication is done in the hardware.
- Independent of Operating System.
- Reduction in code size as encryption is done in hardware.

This application note illustrates the performance boost obtained using hardware encryption.

3. Hardware setup

The LPC43S37 LPCXpresso V3 board (OM # 13073) is used in this application note. The board can be ordered from:
http://www.nxp.com/demoboard/OM13073.html

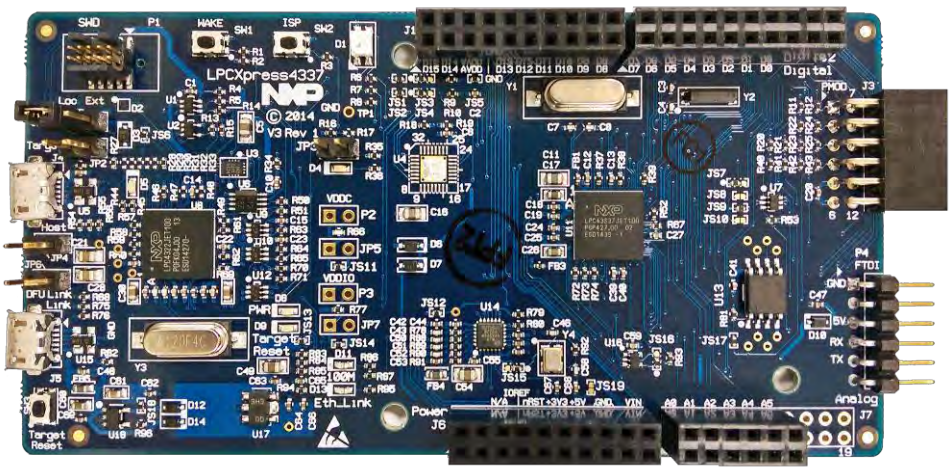

Fig 1. LPC43S37 LPCXpresso V3 Development Board

4. Installation of CMSIS DAP debugger firmware

LPC43S37 LPCXpresso V3 board supports CMSIS DAP interface feature along with a VCOM/I2C/SPI bridge. The LPC Link-2 Configuration Tool (LCT) is used to program the firmware into the board.

The tool can be downloaded from the following link:

http://www.lpcware.com/lpclink2-config-tool

The advantage of CMSIS DAP interface is that it can be used with all the three tool chains – LPCXpresso IDE, Keil MDK, and IAR Embedded Workbench. Otherwise, separate debuggers, such as, LPCLink-2, UlinkME, or Jlink can be used based on the tool chain used for development.

To program the firmware image onto the LPC4322 on the target board, connect a Micro-AB USB cable to J5 connector with a jumper on JP6. See Fig 2.

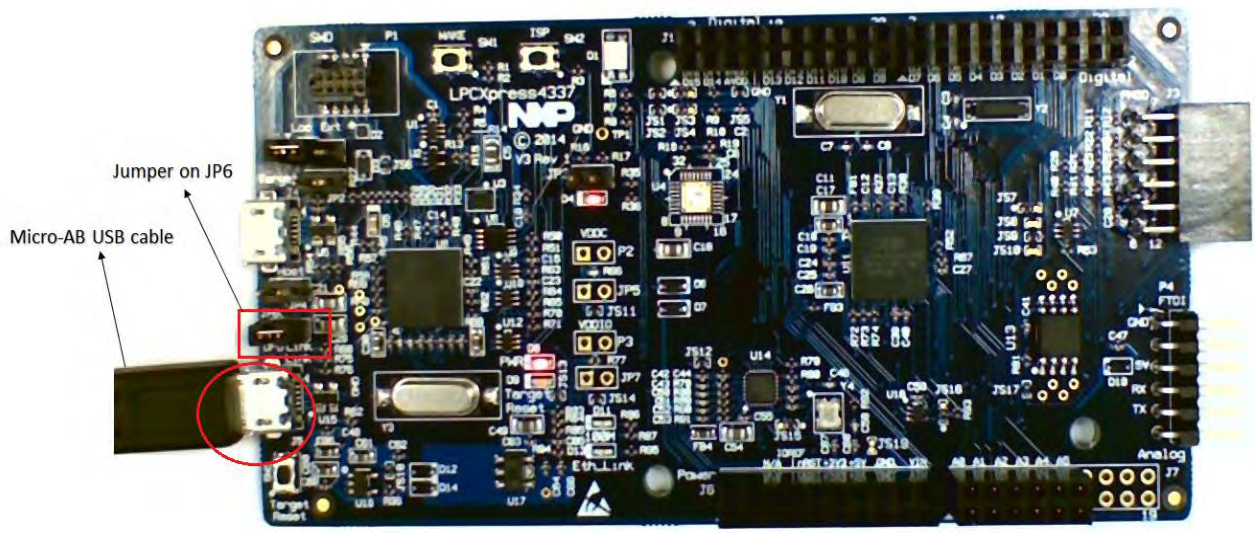

Fig 2. Board setup for installing CMSIS DAP with bridges firmware

Start the LCT tool and select the image “LPCXpresso V2/V3 CMSIS DAP debugger with bridges”. Program the selected image and then remove the jumper on JP6 and power cycle the board.

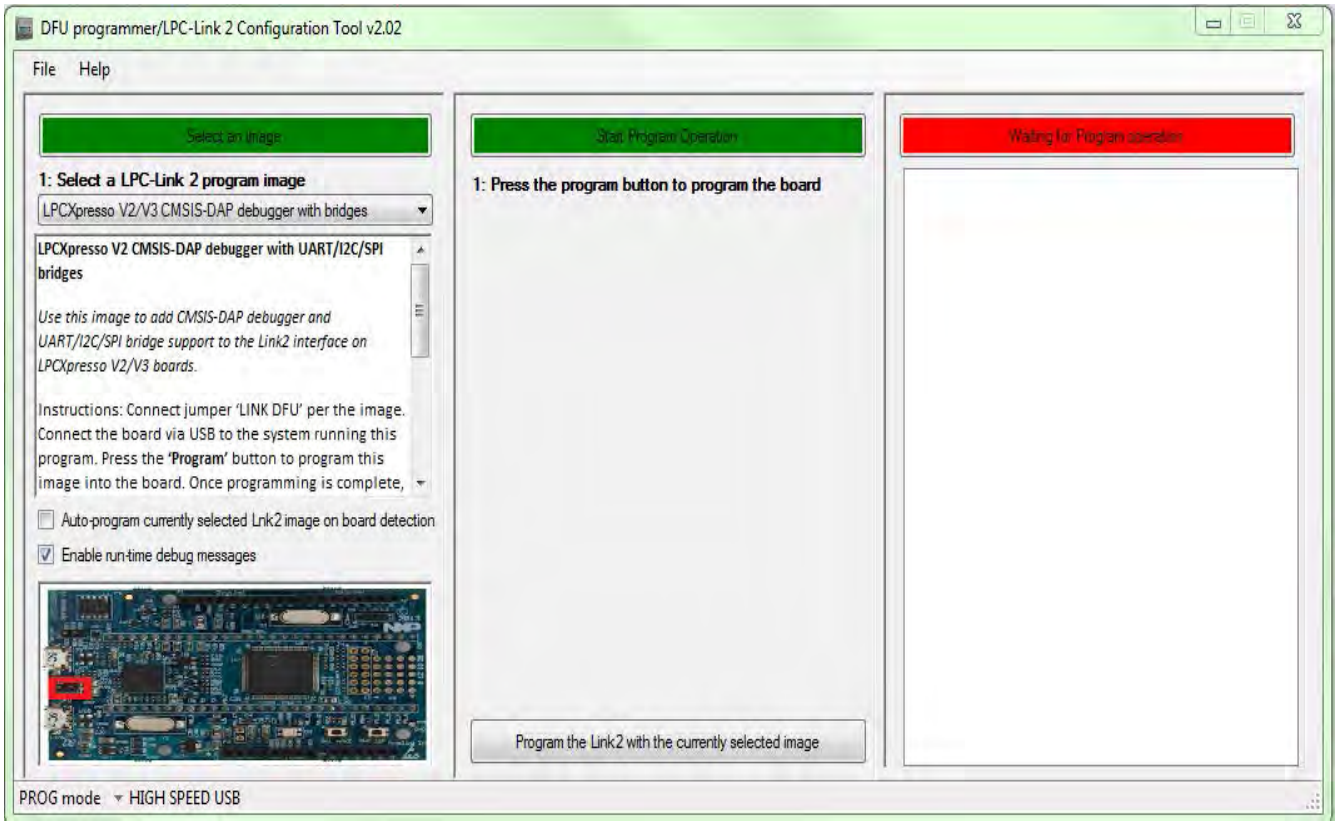

Fig 3. LPC Link-2 Configuration Tool

5. Software setup

The application note associated software is implemented on three tool chains: LPCXpresso IDE, Keil MDK and IAR Embedded Workbench.

Connect the Micro USB cable to the J5 connector.

5.1 LPCXpresso IDE

Open LPCXpresso IDE and import the project using Import Projects. See Fig 4.

The latest version of the LPCXpresso IDE can be found here:

http://www.lpcware.com/lpcxpresso/download

Connect the Micro-AB USB cable into J5 connector and click Debug 'periph_aes'.

The software is downloaded into flash bank A of LPC43S37 via CMSIS DAP debug interface.

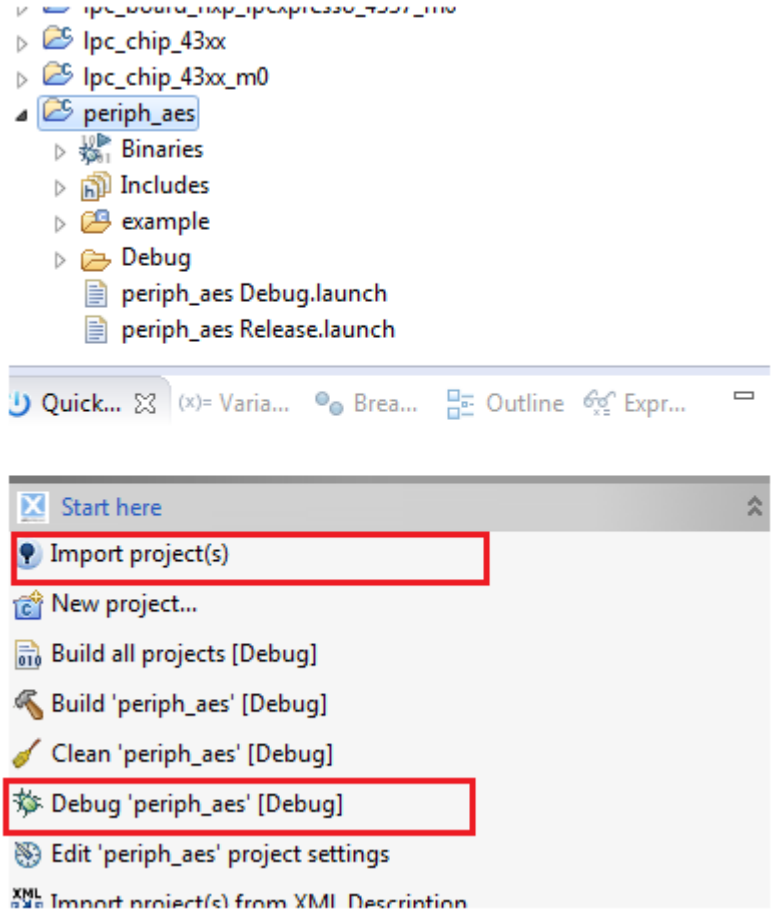

Fig 4. Import and Debug project options in LPCXpresso IDE

5.2 Keil MDK IDE

Open the project from:
'applications\lpc18xx_43xx\keil\nxp_lpcxpresso_4337\periph_examples.uvmpw'.

Go to Project->Options for Target-> Debug. Choose CMSIS DAP debugger option.

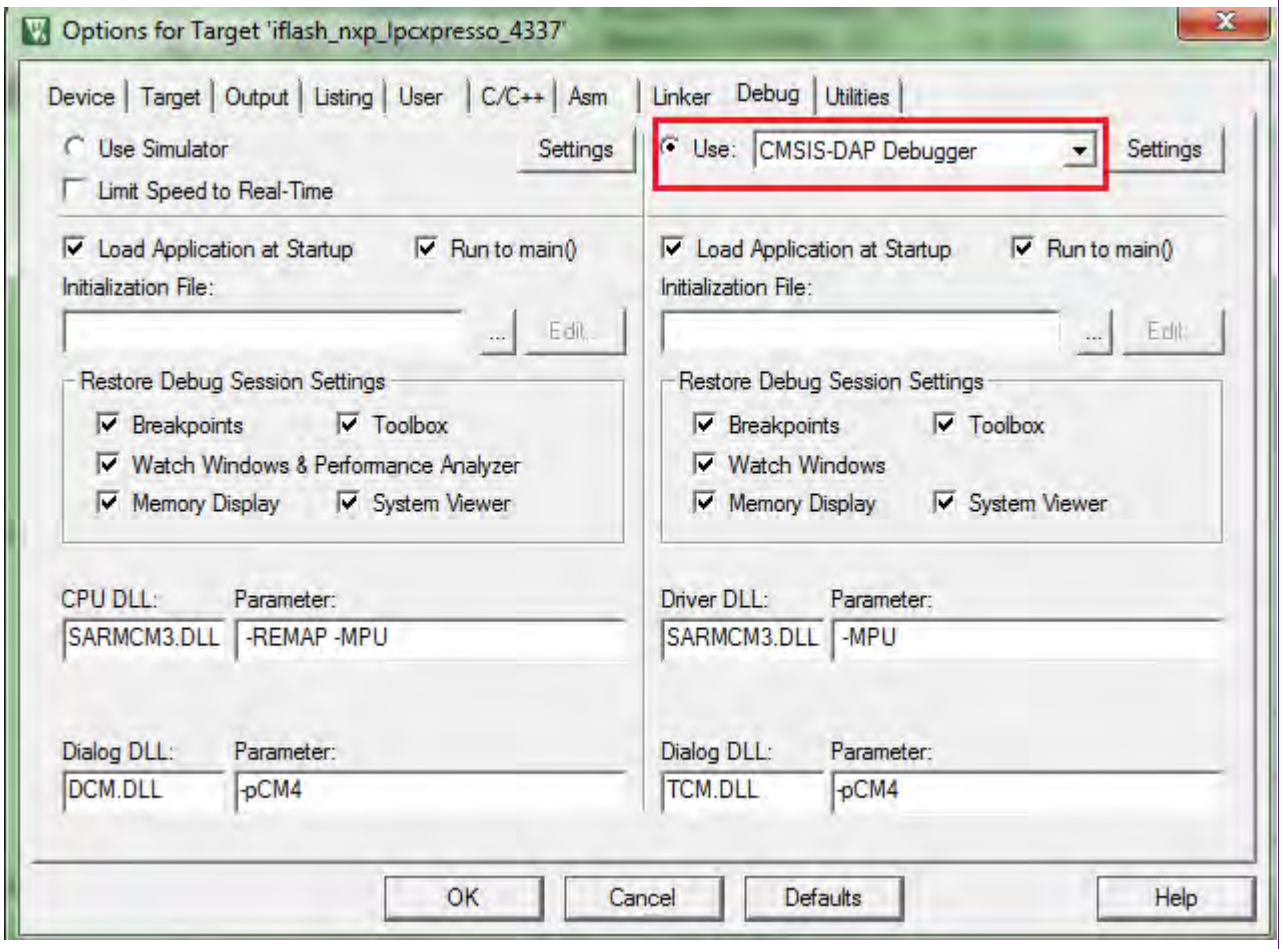

Fig 5. CMSIS DAP Debugger option in Options Window

To build the project go to Project -> Rebuild. Build the chip library 'lib_lpc_chip_43xx' and board library 'lib_lpc_board_nxp_lpcxpresso_4337' before building the project. To download the code into the target go to Flash -> Download.

5.3 IAR embedded workbench

Open the project from:
'applications\lpc18xx_43xx\iar\nxp_lpcxpresso_4337\periph_examples.eww'.

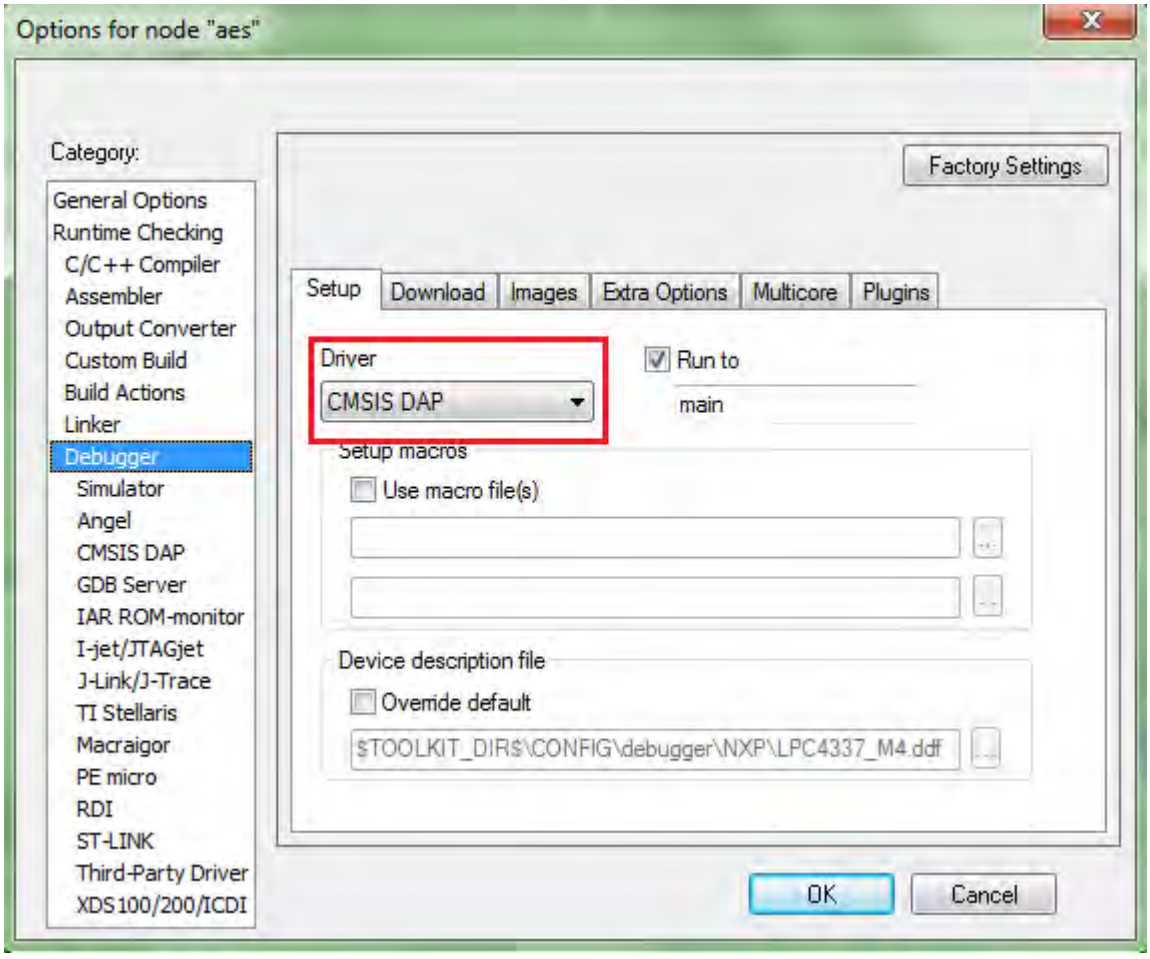

Fig 6. CMSIS DAP Debugger option in Options Window

To build the project go to Project - > Rebuild All. Build the chip library 'lib_lpc_chip_43xx' and board library 'lib_lpc_board_nxp_lpcxpresso_4337' before building the project. To download the code into the target, go to Project -> Download and Debug.

6. Application setup

After downloading the code into the target, open a terminal console, such as Tera Term, and establish a new connection with LPC-LinkII UCom Port.

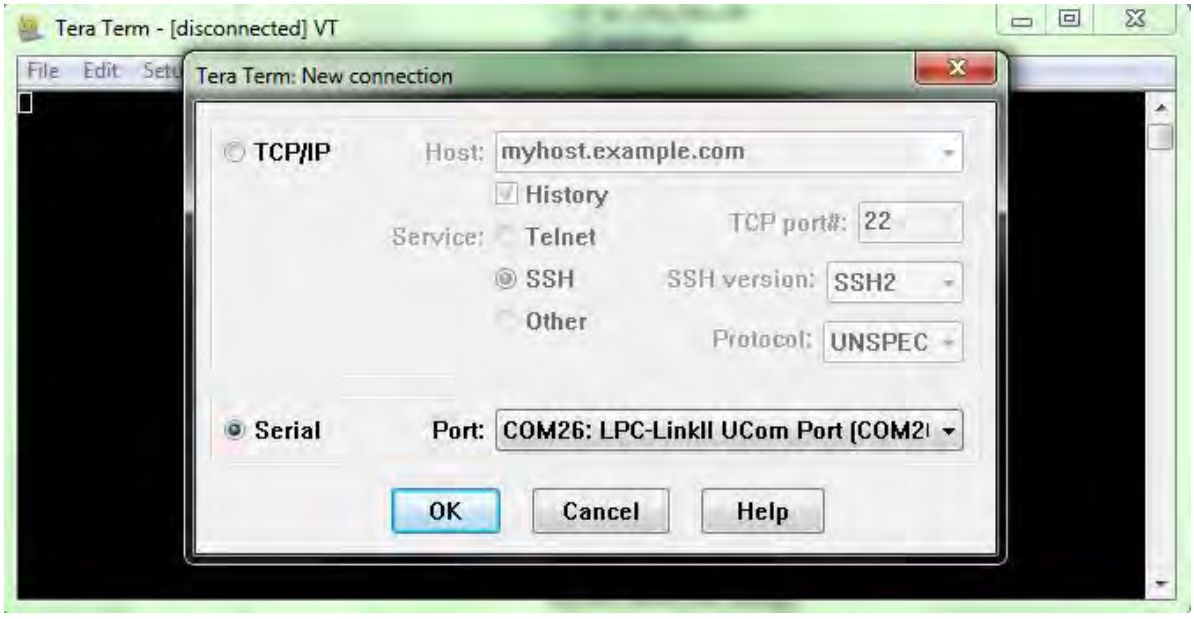

Fig 7. New connection in Tera Term Console

Go to Setup -> Serial Port. Select Baud rate: 115200, Data: 8 bit, Parity: none, Stop: 1 bit and Flow control: none.

Press SW3 button on the LPCXpresso board and information about software and hardware AES encryption/decryption speed is displayed on the terminal.

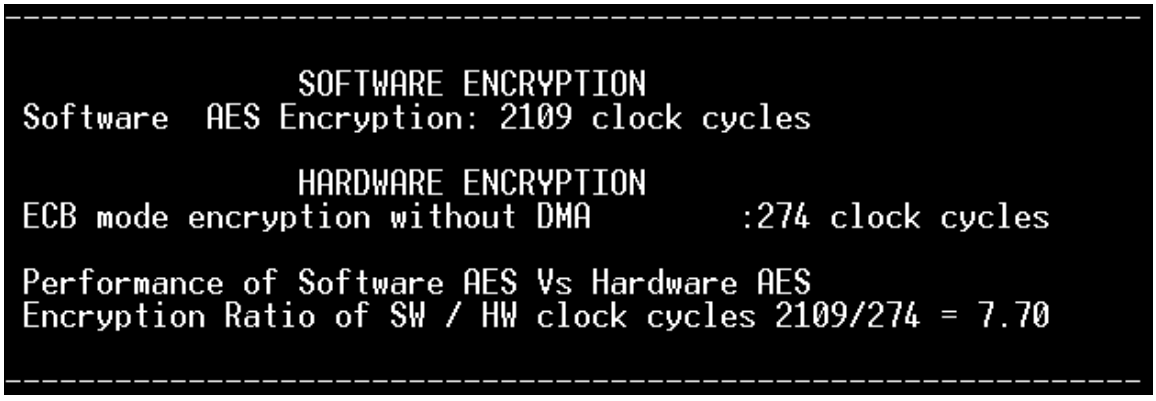

Fig 8. Tera Term Console

Encryption or decryption options can be defined with macros at the top of “aes.c” file. See Fig 9.

```
/* Encryption/Decryption options */
#define SW_ENCRYPT              1
#define SW_DECRYPT              0
#define HW_ECB_ENCRYPT          1
#define HW_ECB_DECRYPT          0
#define HW_CBC_ENCRYPT          0
#define HW_CBC_DECRYPT          0
#define HW_ECB_ENCRYPT_DMA      0
#define HW_ECB_DECRYPT_DMA      0
#define HW_CBC_ENCRYPT_DMA      0
#define HW_CBC_DECRYPT_DMA      0
```

Fig 9. Macro definitions for Encryption/Decryption choices

Based on optimization settings used in the compiler, the time taken for encryption/decryption may vary. On an average, when optimized for time, the performance boost of hardware encryption is 7.6x and when optimized for size, the performance boost is about 8x that of software encryption. This is a major advantage of hardware encryption.

7. Power measurement for software vs. hardware encryption

Fig 10 shows the power consumption of the MCU with software and hardware encryptions. The software encryption is run in a while loop and it consumes 211 mA compared to the hardware encryption, shown in Fig 11, which consumes 189 mA. Thus, hardware encryption consumes less power compared to software encryption.

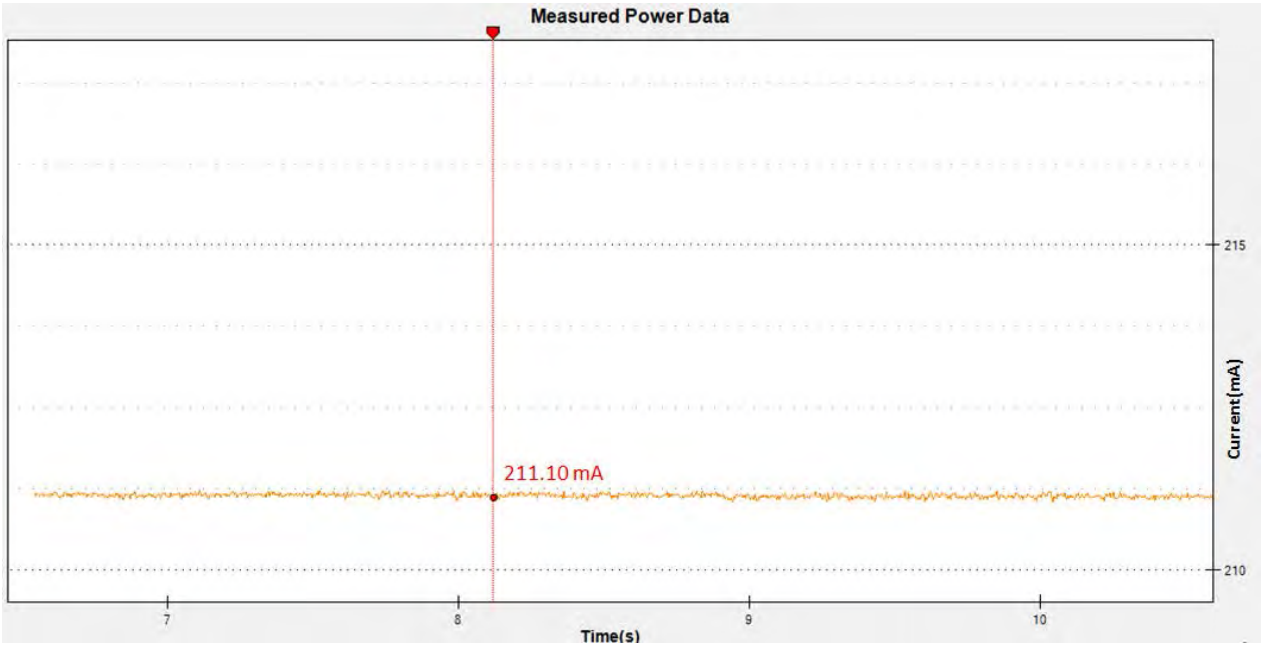

Fig 10. Power consumption with Software Encryption

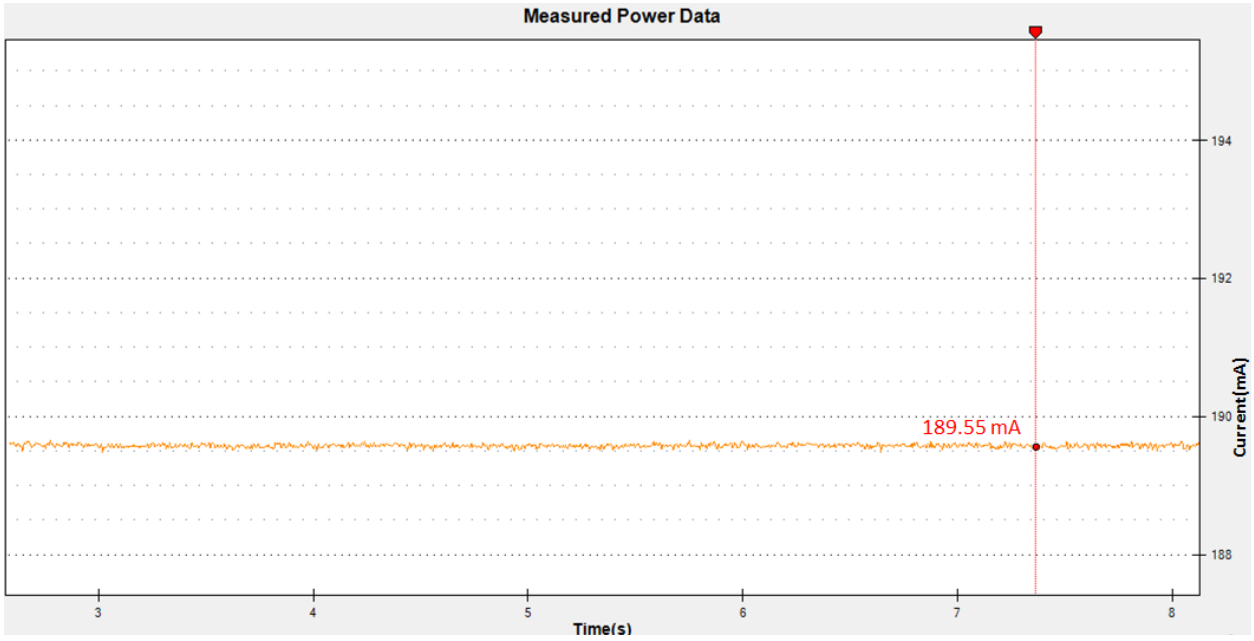

Fig 11. Power consumption with Hardware Encryption

8. Conclusion

Hardware encryption is performed by an on-chip AES engine without CPU. This saves CPU bandwidth to perform other tasks and is significantly faster than software encryption, which uses CPU resources for its operation. Less power is consumed when the hardware AES block is used. With encryption keys stored in the OTP memory and encryption done in hardware, attacks like brute force and malicious code attacks are curtailed. Thus, hardware based encryption is faster and safer.

9. Legal information

9.1 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.

9.2 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 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 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.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on a weakness or default in the customer application/use or the application/use of customer's third party customer(s) (hereinafter both referred to as "Application"). It is customer's sole responsibility to check whether the NXP Semiconductors product is suitable and fit for the Application planned. Customer has to do all necessary testing for the Application in order to avoid a default of the Application and the product. NXP Semiconductors 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 national authorities.

9.3 Trademarks

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

10. Contents

1. Introduction 3
2. Software encryption vs hardware encryption ... 3
3. Hardware setup 3
4. Installation of CMSIS DAP debugger firmware . 4
5. Software setup 6
5.1 LPCXpresso IDE 6
5.2 Keil MDK IDE 7
5.3 IAR embedded workbench 8
6. Application setup 9
7. Power measurement for software vs hardware encryption 11
8. Conclusion 12
9. Legal information 13
9.1 Definitions 13
9.2 Disclaimers 13
9.3 Trademarks 13
10. Contents 14

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

Date of release: 18 February 2015
Document identifier: AN11649