eXtended eXternal Benchmarking eXtension (XXBX)

Matthew R. Carter, Raghurama R. Velagala, John Pham, and Jens-Peter Kaps

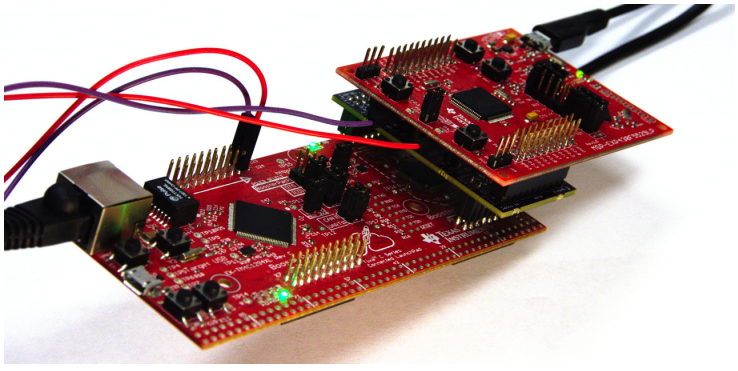
Cryptographic Engineering Research Group
George Mason University, Fairfax, VA, http://cryptography.gmu.edu

Many cryptographic standards are determined through competitions in which candidate algorithms are evaluated for their security and performance in software as well as in hardware. The move to the Internet of Things (IoT) leads to formerly "dumb" devices being connected to the Internet and hence requiring some level of security, provided by cryptographic algorithms. It became therefore necessary to benchmark cryptographic algorithms on microcontrollers. While algorithms on desktop computers and other devices capable of running an POSIX operation system and a compiler can be benchmarked using the System for Unified Performance Evaluation Related to Cryptographic Operations and Primitives (SUPERCOP), no such benchmarking was available for less powerful microcontrollers. Furthermore, these microcontrollers can impose severe restrictions on available random-access and read-only memory (RAM, ROM), which makes RAM and ROM usage metrics as important as execution time. Therefore, an eXternal Benchmarking eXtension (XBX) to SUPERCOP was developed, which supports several microcontrollers and captures execution time as well as RAM and ROM usage. It was first used during the Secure Hash Function-3 (SHA-3) competition [4].

In support of the Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) we eXtended XBX, hence XXBX. First of all, we adjusted it to handle algorithms for Authenticated Encryption with Associated Data (AEAD). The most significant change is the ability to measure the power consumption of the microcontroller Device under test (XBD). We developed a Power shim (XBP) that sits between the test Harness (XBH) and XBD and amplifies the sensed current so that the Analog to Digital Converter (ADC) on the XBH can measure the current drawn by the XBD. Due to this additional task we had to replace the original XBH with a more capable platform which is ARM based and runs RTOS. This required a complete re-write of the software. The cost of the XBH did not change. Also the software that runs the benchmarking on a desktop System (XBS) was rewritten to eliminate a mix of shell and Perl scripts by Python and a flat file result collection by a SQLite database [2, 3, 1].

Hardware Demonstration at HOST 2018

We intend to present two XXBX setups, one with a microcontroller that has an AES accelerator, and one with a microcontroller that can only run AES in software. Both setups will benchmark those CAESAR candidates which use AES as an underlying function. We will walk through the setup and execution and present the results using an IPython notebook. The picture on the right shows the harness (XBH) on the bottom, one device being benchmarked (XBD) on the top, and a power shim (XBP) in between.



The following boards with microcontrollers will be seen by visitors of our demonstration.

Table 1. Devices for Benchmarking (XBD) Supported by XXBX

Board	Manuf.	CPU	ISA	Bus	f	HW	ROM	RAM	Price
MSP-EXP430F5529	TI	MSP430F	MSP430X	16-bit	25 MHz		12kB	10kB	$12.99
MSP-EXP430FR5994	TI	MSP430FR	MSP430X	16-bit	16 MHz	AES	256kB	8kB	$15.99
MSP-EXP432P401R	TI	ARM Cortex M4F	ARMv7E-M	32-bit	48 MHz	AES	256kB	64kB	$12.99
EK-TM4C123GXL	TI	ARM Cortex M4F	ARMv7E-M	32-bit	80 MHz		256kB	32kB	$12.99
EK-TM4C129EXL	TI	ARM Cortex M4F	ARMv7E-M	32-bit	120 MHz	AES	1024kB	256kB	$24.99
NUCLEO-F091RC	STM	ARM Cortex M0	ARMv6-M	32-bit	48 MHz		256kB	32kB	$10.33
NUCLEO-F103RB	STM	ARM Cortex M3	ARMv7-M	32-bit	72 MHz		128kB	20kB	$10.33

References

1. Kaps, J.P.: eXtended eXternal Benchmarking eXtension (XXBX). SPEED-B - Software performance enhancement for encryption and decryption, and benchmarking (Oct 2016), Utrecht, Netherlands, invited talk
2. Pham, J.: Development and Benchmarking of Cryptographic Implementations on Embedded Platforms. Masters thesis, ECE Department, George Mason University, Fairfax, Virginia, USA (Aug 2015)
3. Pham, J., Kaps, J.P.: eXtended eXternal Benchmarking eXtension (XXBX) (Sep 2015), presentation at DIAC
4. Wenzel-Benner, C., Gräf, J., Pham, J., Kaps, J.P.: XBX benchmarking results January 2012 (Mar 2012), third SHA-3 candidate conference