Project Proposal

Group Number: 3

Project Members:

1. Jay Raval
2. Snehal Sanjay Patil
3. Matthew Carter

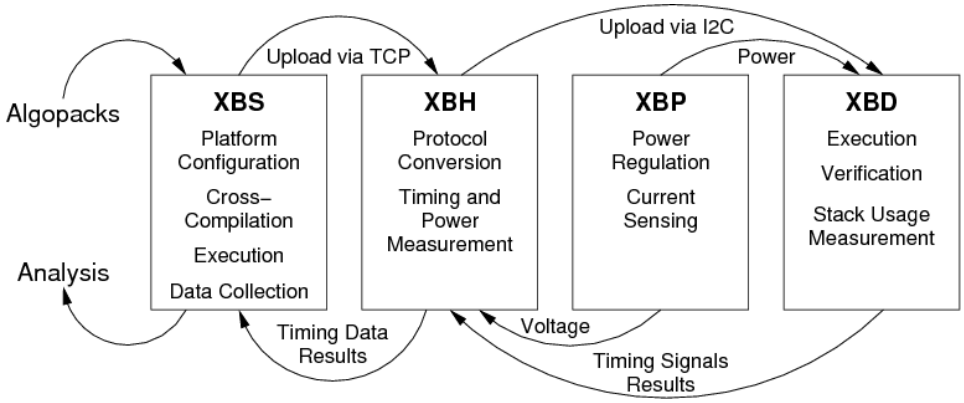
Project Title: Benchmarking of lightweight cryptographic algorithm on MSP432P401R.

Project Goals:

The main objective of this project is to add the Texas Instruments MSP432P401R microcontroller to the eXtended eXternal Benchmarking eXtension (XXBX), a system to evaluate cryptographic algorithms competing in the CAESAR competition on embedded devices. In this project we will measure ROM, RAM, throughput, and power to attain an understanding of the performance of algorithms in those metrics on MSP432P401R. We need to ensure the portability of MSP432P401R which will acts as the XBD or the device under test with the XXBX platform. The goals involved are establishing a connection between XBH and XBD using I2C communication, Designing the software code for the bootloader of MSP432P401R, collecting the metrics from MSP432P401R using XBH and power shim.

Components of the project:

The XXBX platform consists of four main components:



- XBX Benchmarking System (XBS): It runs on an Ubuntu PC and uses Python 3 code that compiles the primitives of the cryptographic implementation and sends them to the XBH and collects the measured metrics.
- XBX Harness (XBH): It is a microcontroller that facilitates communication between the XBS and XBD. It is termed as a "harness" device since the various testing devices are connected on it. It uses its internal 12-bit ADC for power measurement and its timer for measuring the throughput. The XBH supported is EK-TM4C1294XL based on ARM M4F.
- XBX Power shim (XBP): Power is measured using a shunt resistor circuit. It is placed above the XBH and below the XBD.
- XBX Device under test (XBD): It is the microcontroller under test which uses its bootloader to communicate with the XBH and the algorithm is implemented on it. The device to be tested is MSP432P401R.

Hardware Component to be used:

- Harness Device: We plan to use a harness device called XBH which is supported by EK-TM4C1294XL based on ARM M4F. It will communicate to XBS through Ethernet (UART) and will be interfaced to MSP432P401R through I2C communication. The harness device will help us to collect the metrics like power, throughput and RAM usage on MSP432P401R for implementation of cryptographic algorithm.
- Power Shim: We plan to use a power shim to measure the power metric. It is a board that sits between the XBH and the XBD, captures and amplifies the current drawn by MSP432P401R so that the ADC on the XBH can measure it. Power will be measured in milliwatts by the XBH ADC measuring the voltage over time

Interfaces of MSP432P401R to be used:

In this project MSP432P401R is the device under test, where it has to perform all the operations that the XBD has in XXBX project.

- Timer: The timer flags of MSP432P401R will be monitored by XBH to measure the cycle/ byte. The cycles are measured using a timer running on the XBH triggered by a pin that XBD controls. The pin idles HIGH, before execution the pin is pulled LOW and after execution the pin is pulled HIGH by the XBD.
- Bootloader: The XBD code will consists of a small bootloader that is flashed once to XBD that performs basic calibration and self- programming of the primitive implementations over the communications channel. It contains the Hardware Abstraction Layer and can perform rudimentary functions such as initializing the I2C module, Clocks module, GPIO ports, Universal Serial Communication Interface (USCI), etc. and also be able to report timing measurements for calibration and receive the Application over I2C.

- I2C: We will use the I2C communication as an interface between the harness device and the device under test i.e. MSP432P401R.
- AES accelerator: On board AES accelerator present in MSP432P401R will be used to benchmark the cryptographic algorithm against software AES algorithm.

References:

[1] Kinnera Chintamaneni, Raghurama Velagala, Clinton Dias, Ashish Kokare, Vaibhav Chittampalli, "Adaptation of Software Implementations of CAESAR Candidates to Run on Microcontrollers and Benchmark them using XBXX," George Mason University, Fairfax, VA, December 18th, 2016.

[2] Kinnera Chintamaneni, Raghurama Velagala, "Addition of an Hardware Supported AES MCU to the XBXX Cryptographic Benchmarking Platform," George Mason University, Fairfax, VA, May 15th, 2017.

[3] M. Carter, "Extending XBXX Support to STM32 Microcontrollers," George Mason University, Fairfax, VA.

[4] Girmay Weldemichael, "Behavior of Software Implementations of CAESAR Candidates on XBXX," George Mason University, Fairfax, VA, March 27th, 2017.

[5] "eBACS: ECRYPT Benchmarking of Cryptographic Systems: SUPERCOP". Available: https://bench.cr.yp.to/supercop.html Accessed Sep. 11, 2017

[6] CAESAR Competition. CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness. http://competitions.cr.yp.to/caesar.html. [7] "eBACS: ECRYPT Benchmarking of Cryptographic Systems". Available: http://bench.cr.yp.to Accessed Sep. 11, 2017.

[8] Christian Wenzel-Benner and Jens Gräf. "XBX: eXternal Benchmarking eXtension for the SUPERCOP crypto benchmarking framework". In: Cryptographic Hardware and Embedded Systems, CHES 2010. Springer, 2010, pp. 294–305. URL: http://link.springer.com/chapter/10.1007/978-3-642-15031-9_20

[9] J. Pham, "Development and Benchmarking of Cryptographic Implementations on Embedded Platforms," M.S. thesis, ECE Dept., GMU, Fairfax, VA, USA, 2015. [10] J. Pham and J.-P. Kaps, EXtended eXternal Benchmarking eXtension (XXBX), Sep., 2015 [pdf] [Bibtex] DIAC 2015: Directions in Authenticated Ciphers, Singapore. [11] Elio Andia, Fletcher Ta, and Margaux McGivern, "Benchmarking Hash Functions on the MSP430," GMU, Fairfax, VA, Rep. ECE493 Final Report, May 2011.

[12] Farzaneh Abed, Christian Forler, and Stefan Lucks, "Overview of the Candidates in the CAESAR Competition for Authenticated Encryption", Accessed Sep. 11, 2017.