eXtended eXternal Benchmarking eXtension (XXBX)

Matthew R. Carter Raghurama R. Velegala Snehal Patil John Pham Jens-Peter Kaps
Department of Electrical and Computer Engineering, George Mason University, Fairfax, Virginia 22030, USA

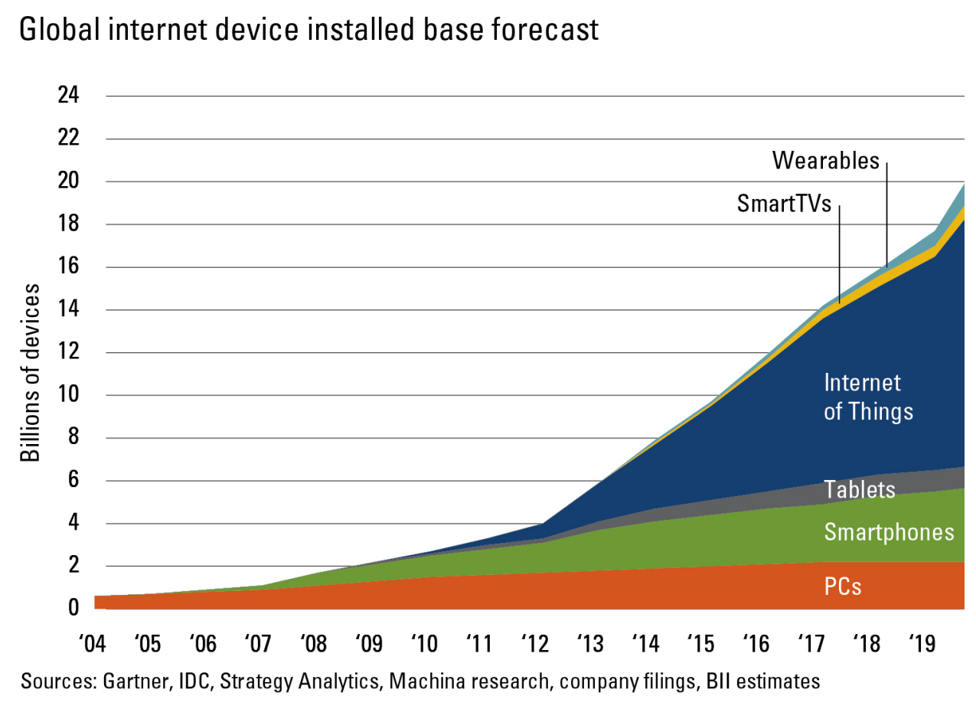
Cryptographic Engineering Research Group

Abstract

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 latest such competition is the Lightweight Cryptography Standardization Process by NIST. It targets in particular resource-constrained devices such as microcontrollers. The eXtended eXternal Benchmarking eXtension (XXBX) is a tool for benchmarking the performance, memory usage, and power / energy consumption of cryptographic software on microcontrollers. It is an extension to the System for Unified Performance Evaluation Related to Cryptographic Operations and Primitives (SUPERCOP) which benchmarks a large variety of cryptographic primitives on general purpose computers. XXBX extends it in the sense that it allows for benchmarking on embedded platforms and adds metrics for RAM and ROM usage as well as power / energy consumption.

Motivation

- The move to the Internet of Things (IoT) leads to formerly "dumb" devices being connected to the Internet.
- They require some level of security ⇒ cryptographic algorithms.
- IoT promises a dramatic increase in devices, many will be microcontrollers or System on Chips (SOCs).
- 32-bit microcontrollers are projected to take lead over 8/16-bit.
- 51% of all 32-bit microcontrollers were ARM based in 2012.



©2015 AlixPartners, LLP

Benchmarking Tools

- SUPERCOP
  - System for Unified Performance Evaluation Related to Cryptographic Operations and Primitives
  - Benchmarks many implementations of many primitives across multiple operations on multiple hardware platforms.
  - Supports environments capable of running Linux and hosting a compiler.
  - Series of shell scripts and C test harnesses, and comprehensive collection of algorithm primitive implementations.
  - Verifies correct execution of implementations and times cycles required per byte processed.

`http://bench.cr.yp.to/supercop.html`

Missing Features

- Does not measure ROM usage, RAM usage, power consumption.
- Does not support cross-compilation.
- Does not support microcontrollers.

- XBX
  - eXternal Benchmarking eXtension (XBX) to SUPERCOP
  - Automated testing on real microcontrollers.
  - Compatibility with SUPERCOP algorithm collection ("algopacks") and output format.
  - Low cost hardware and software.
  - Our contribution to original XBX was to port it to the MSP430 platform and provide results for SHA-3 finalists..
  - Measures ROM and RAM usage.

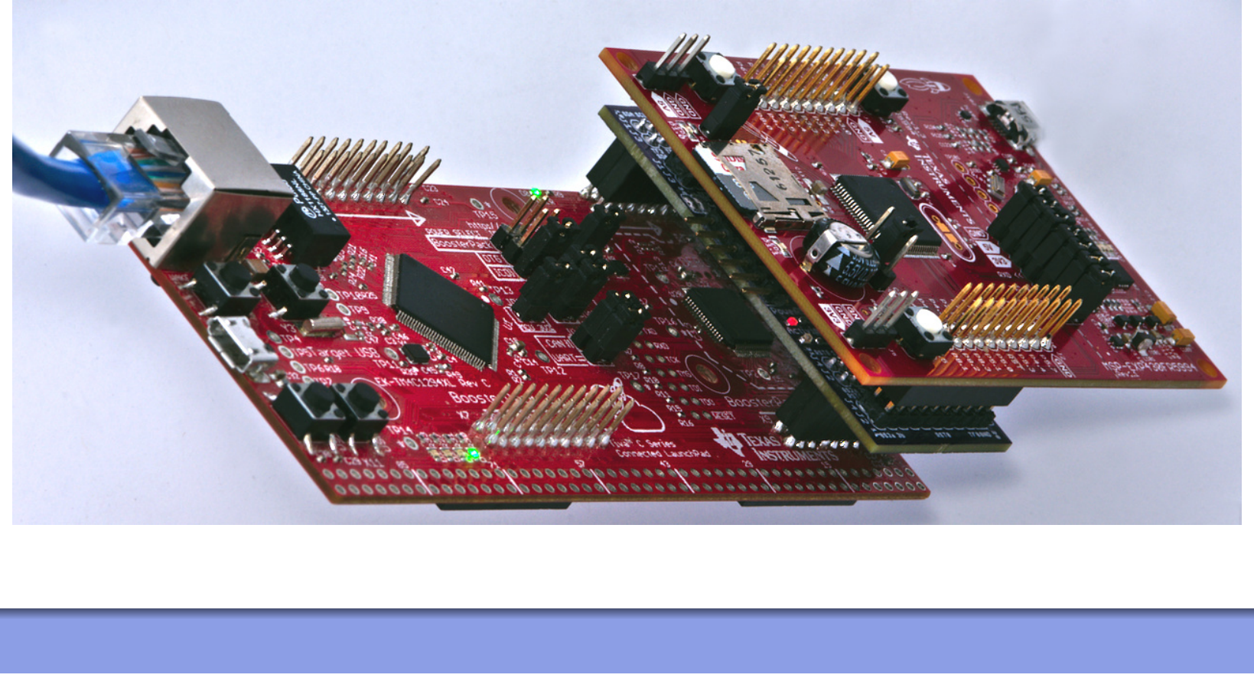
Missing Features

- Does not measure power consumption.
- Harness device (ATmega32) limits future expansion.

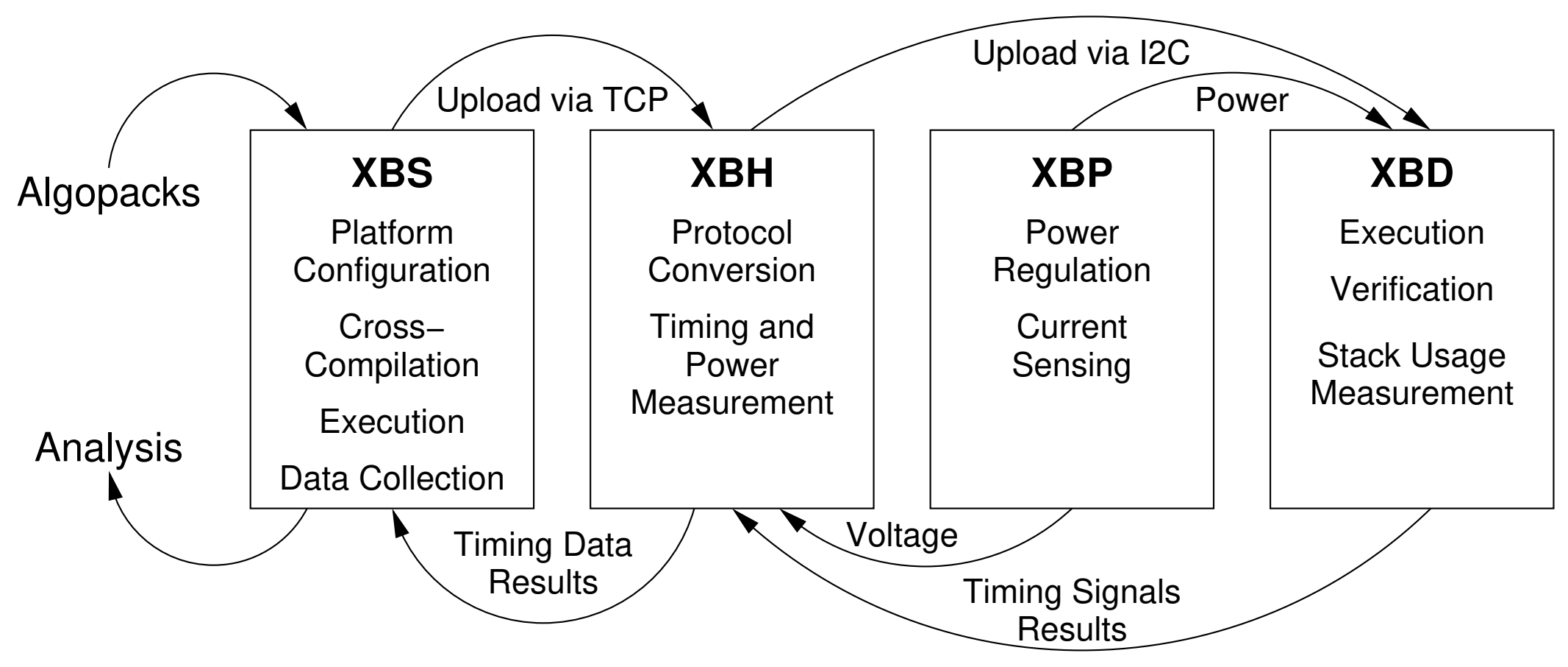
XXBX

eXtended eXternal Benchmarking eXtention extends the XBX by:

- Support for power and energy measurement.
- Support for Authenticated Encryption with Associated Data (AEAD) and hash functions to support NIST Lightweight Cryptography competition.
- Usage of a new harness with a powerful microcontroller running FreeRTOS.
- Rewritten software in Python 3 (was bash and perl).
- Storage of results in SQLite database.

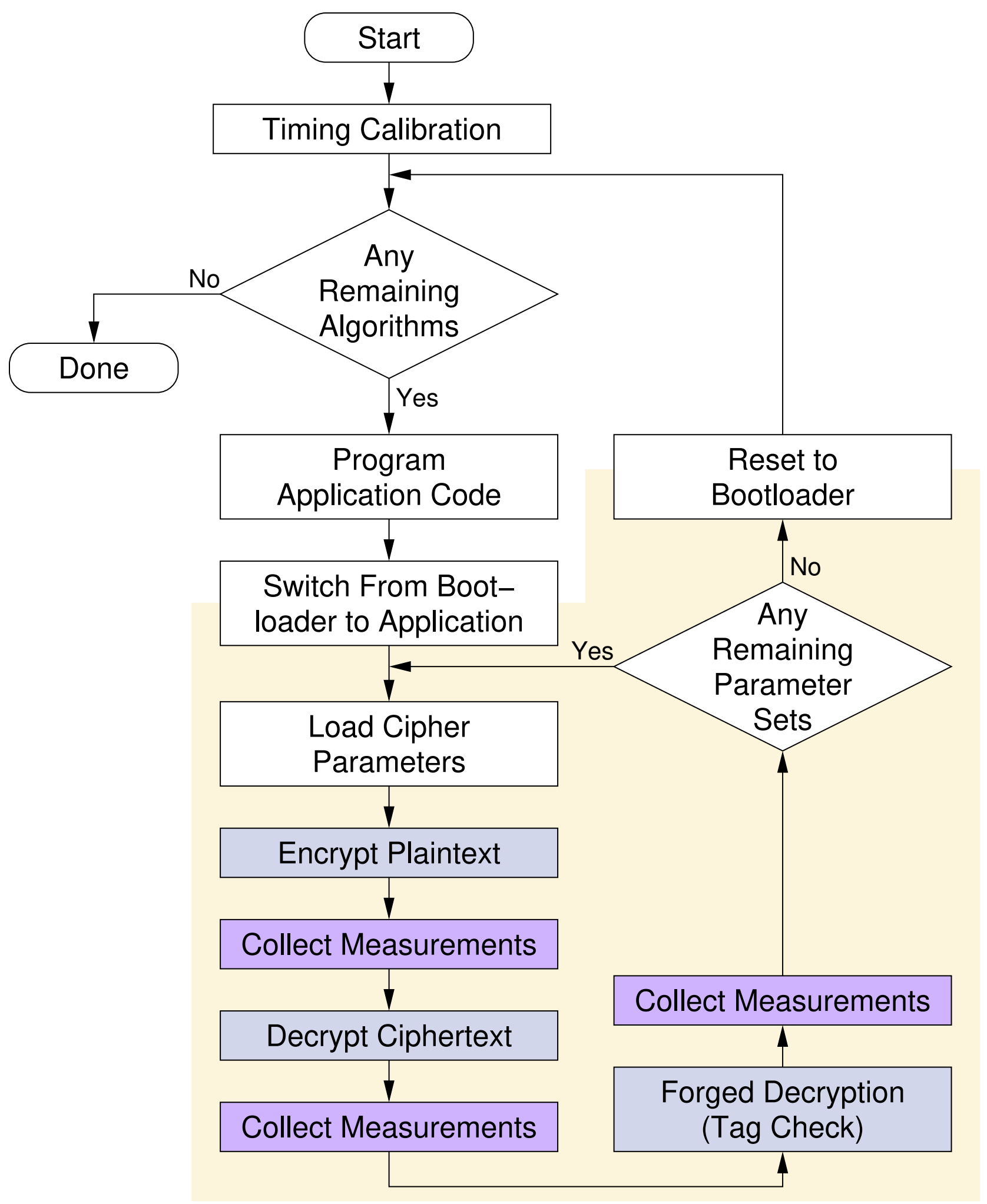


Main Components of XXBX



- XXBX benchmarking System – XBS
  - Software written in Python and runs on Linux.
  - Cross-compiles cryptographic algorithms from SUPERCOP.
  - Orchestrates benchmarking flow.
  - Collects results and stores them into SQLite database.
- XXBX Harness – XBH
  - Passes applications, test data, and instructions to XBD.
  - Measures timing and power consumption.
- XXBX Power Shim – XBP
  - Senses and amplifies power consumption.
- XXBX Device Under Test – XBD
  - Bootloader accepts commands and waits for application.
  - Executes application with cryptographic algorithms.

Benchmarking Flow

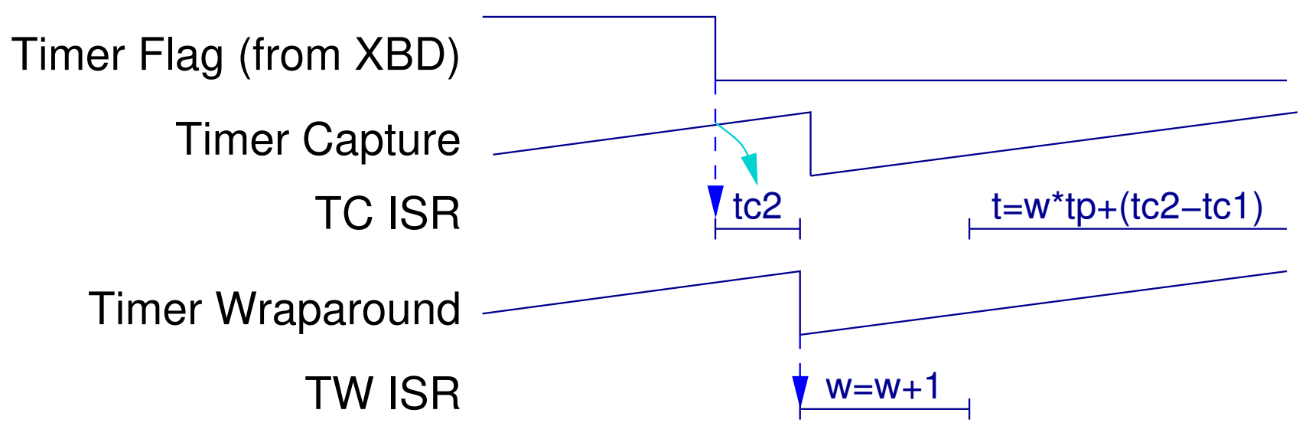


RAM and ROM Usage Measurement

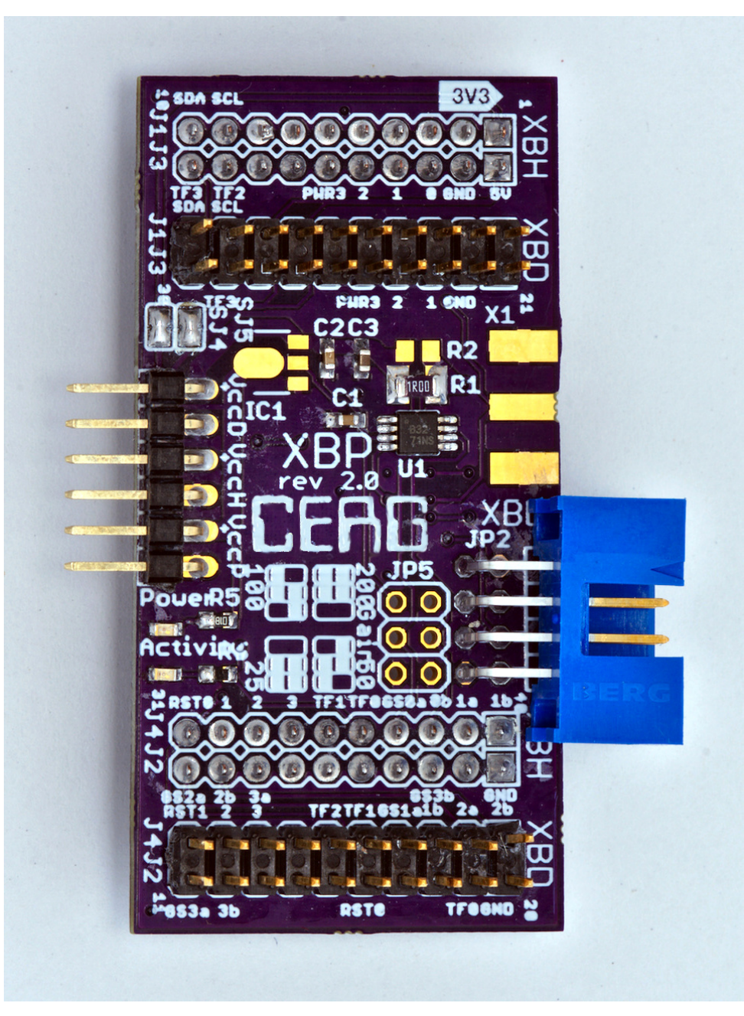
- ROM Usage
  - UNIX size command is run on generated application which reports sizes of executable sections: `.bss`, `.data`, and `.text`.
  - The sum of the `.text` and `.data` sections is the amount of ROM that is used.
- RAM Usage
  - Application paints memory with canary values.
  - After execution of cipher operation, application checks the number of addresses not containing canary values.
  - This is the amount of stack memory used.
  - The sum of the stack usage, `.data` section, and `.bss` section is the amount of RAM that is used.

Timing Measurements

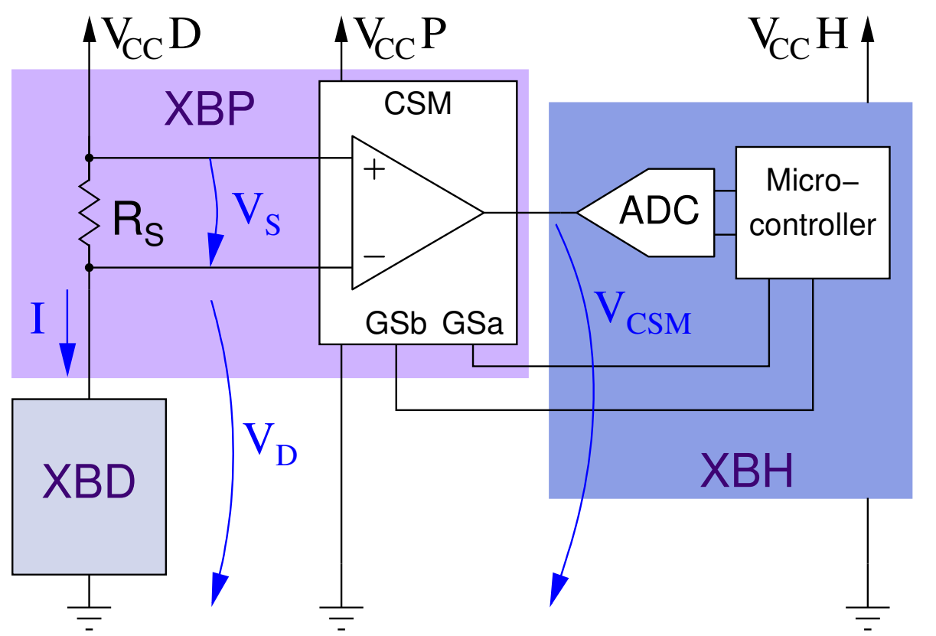
- 16-bit timer TC to capture timing flag from XBD.
- Need additional timer TW at same rate to get interrupts when timer wraps around.
- Higher priority TW counts wraps (w).
- TW can interrupt processing of TC ISR!
- Maximum time (t) is 35.8 seconds (64-bit value) at 120 MHz.



Power Measurement



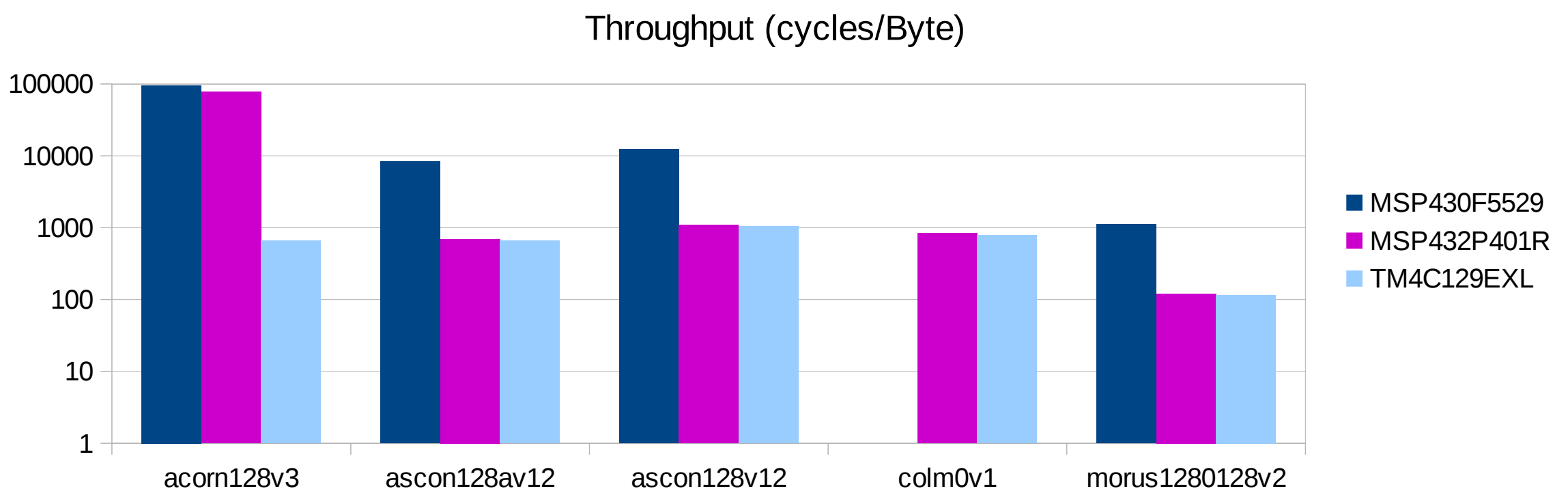
- Fits between XBH and XBD
- Contains I^2C pull-ups
- Space for power regulator
- Supports XBDs with 1.2 V–5 V

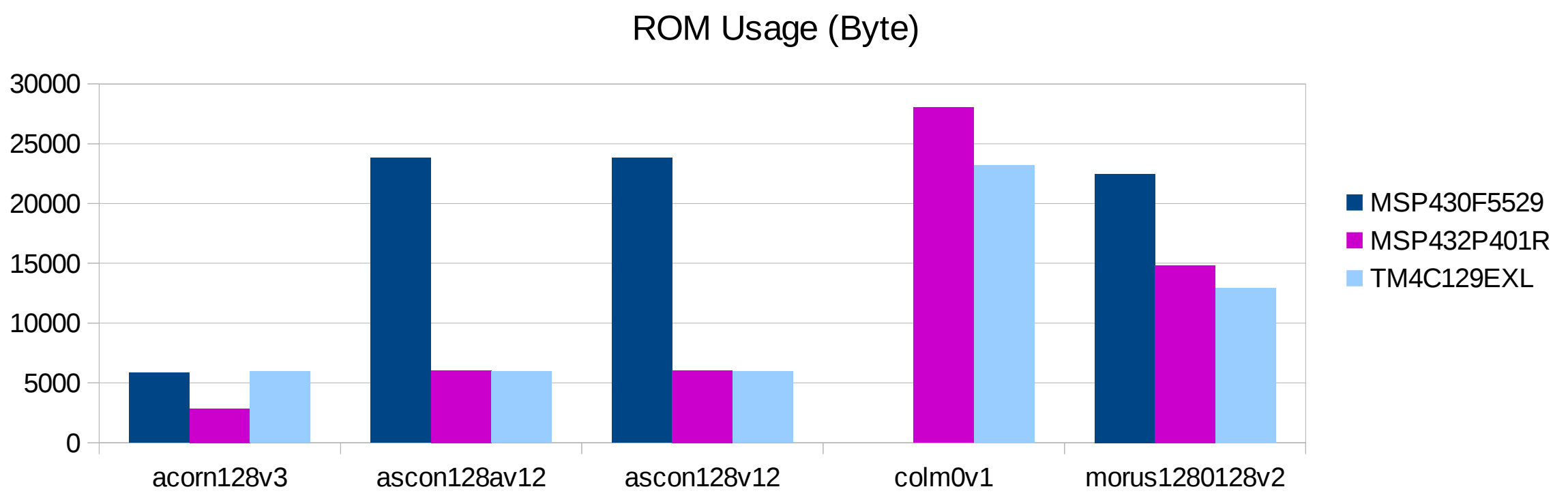


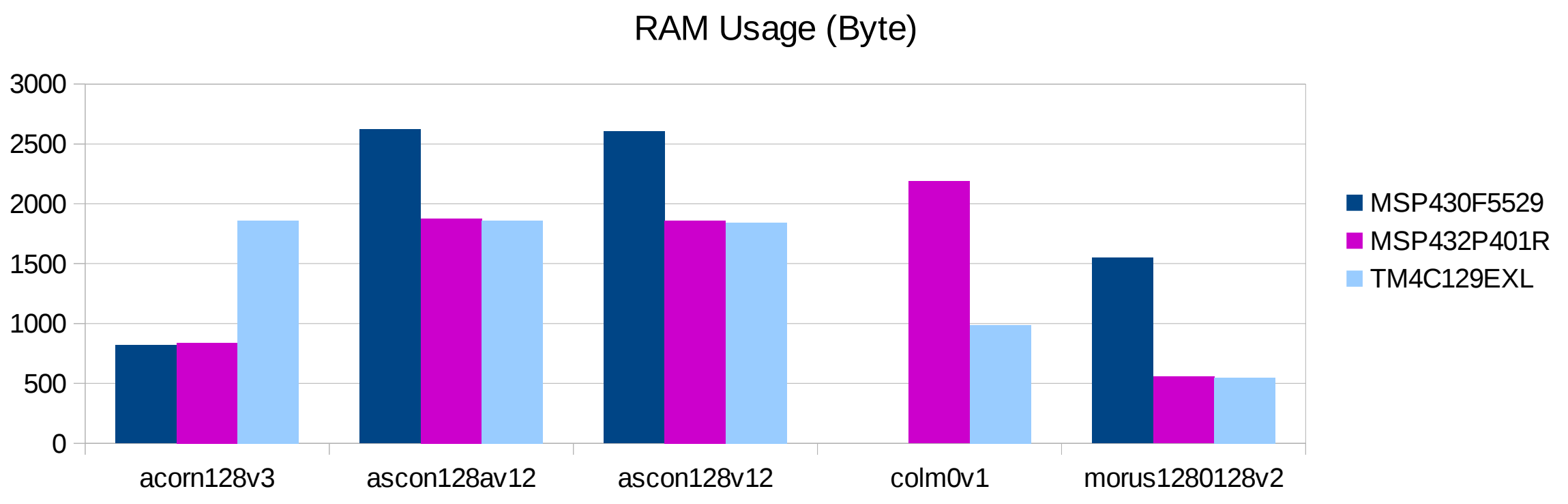
CAESAR

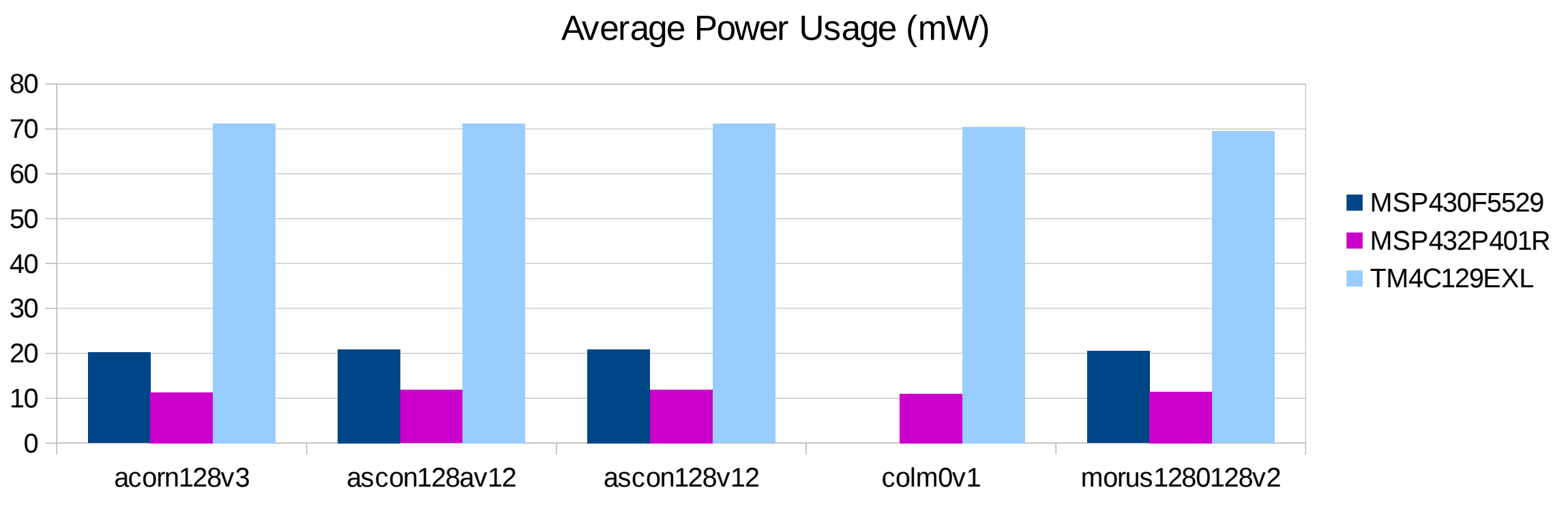
- Competition for Authenticated Encryption: Security, Applicability and Robustness
- Announced in 2013, finalists announced in March 2018.
- Round 3 had 16 algorithms with several variations.
- We tried to benchmark all 7 finalists and their variations on the microcontrollers supported by XXBX.
- Unfortunately only few could be compiled for microcontrollers.

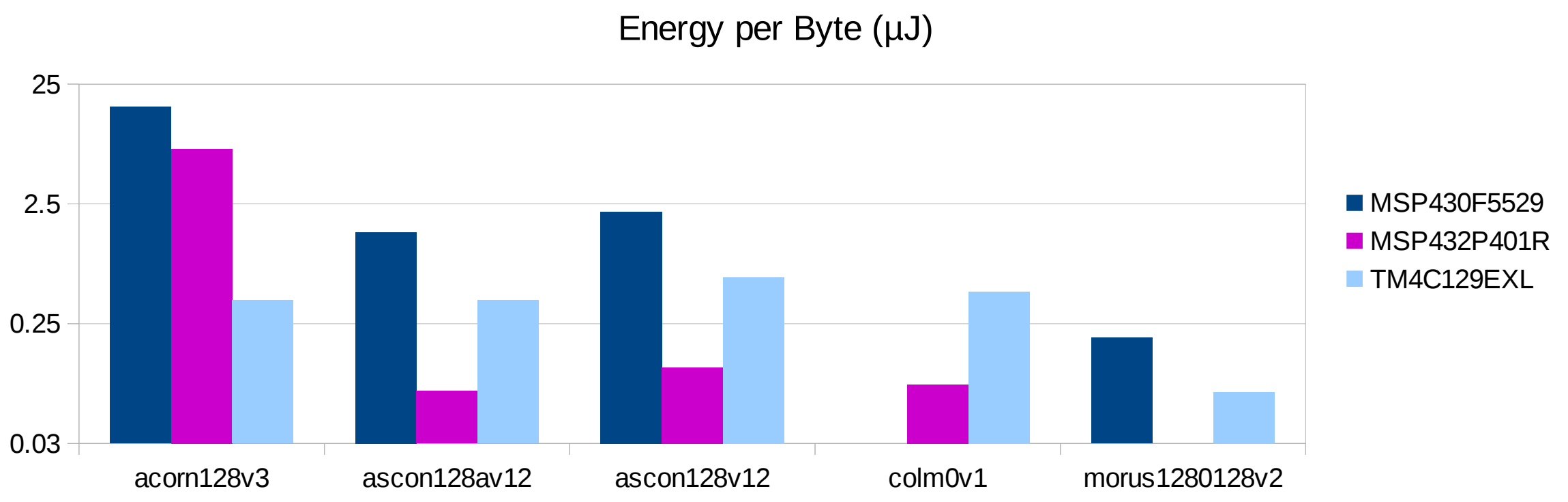
Results of CAESAR Candidates









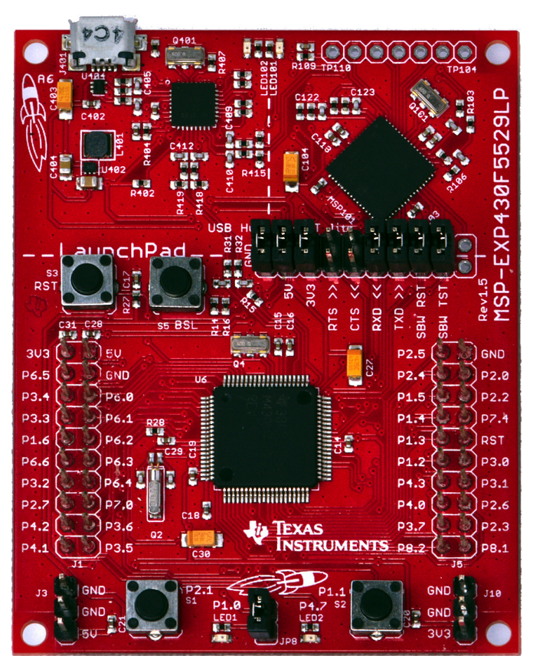


Future Research

- Adapt XXBX to support Post Quantum Crytpography
- NIST is starting a Lightweight Cryptography Standardization Process for AEAD functions and Hash functions. The draft submission requirements were published in April 2018. XXBX will support this effort.
- Expanding to other microcontrollers incl. 8-bit.
- Combine with FOBOS to allow side-channel leakage evaluation.

Supported XBDs

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



Cryptographic Engineering Research Group (CERG) Department of Electrical and Computer Engineering George Mason University http://cryptography.gmu.edu