eXtended eXternal Benchmarking eXtension (XXBX)

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

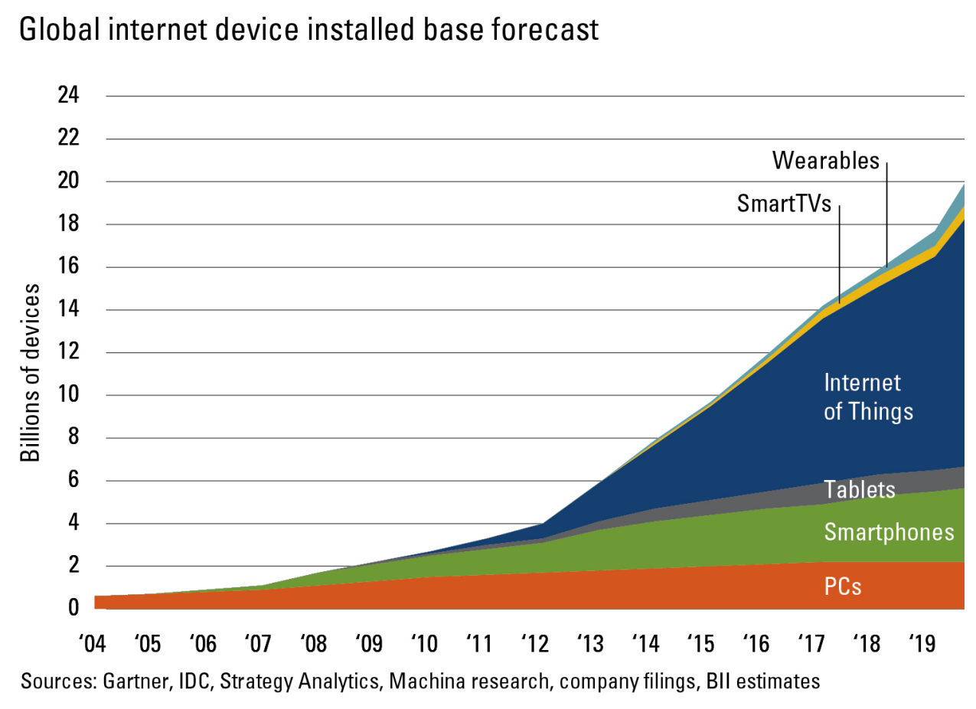
Cryptographic Engineering Research Group

Abstract

This text has abstract, motivation and previous work mixed! 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 [?].

Motivation

- IoT promises a dramatic increase in devices, many will be microcontrollers or SOCs.
- 32-bit microcontrollers are projected to take lead over 8/16-bit by 2018.
- 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`

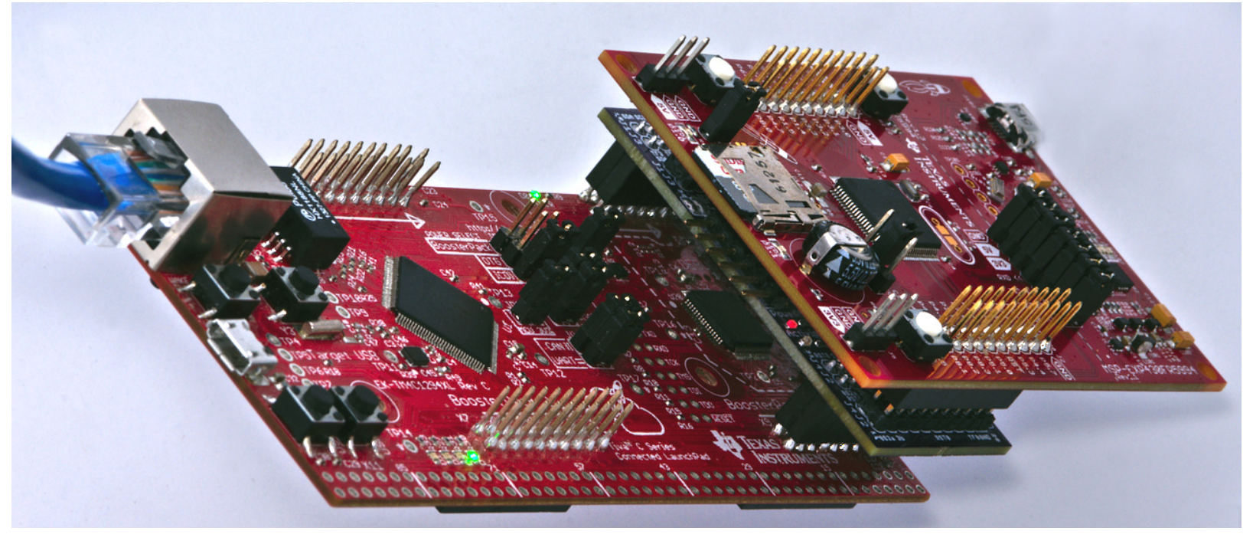
  Missing Features
  - Does not measure ROM usage, RAM usage, power consumption
  - Does not support cross-compilation
  - Does not support microcontrollers
- XBX
  - eXternal Benchmarking eXtension (XBX) to SUPERCOP
  - Automated testing on real microcontrollers
  - Compatibility with SUPERCOP algorithm 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

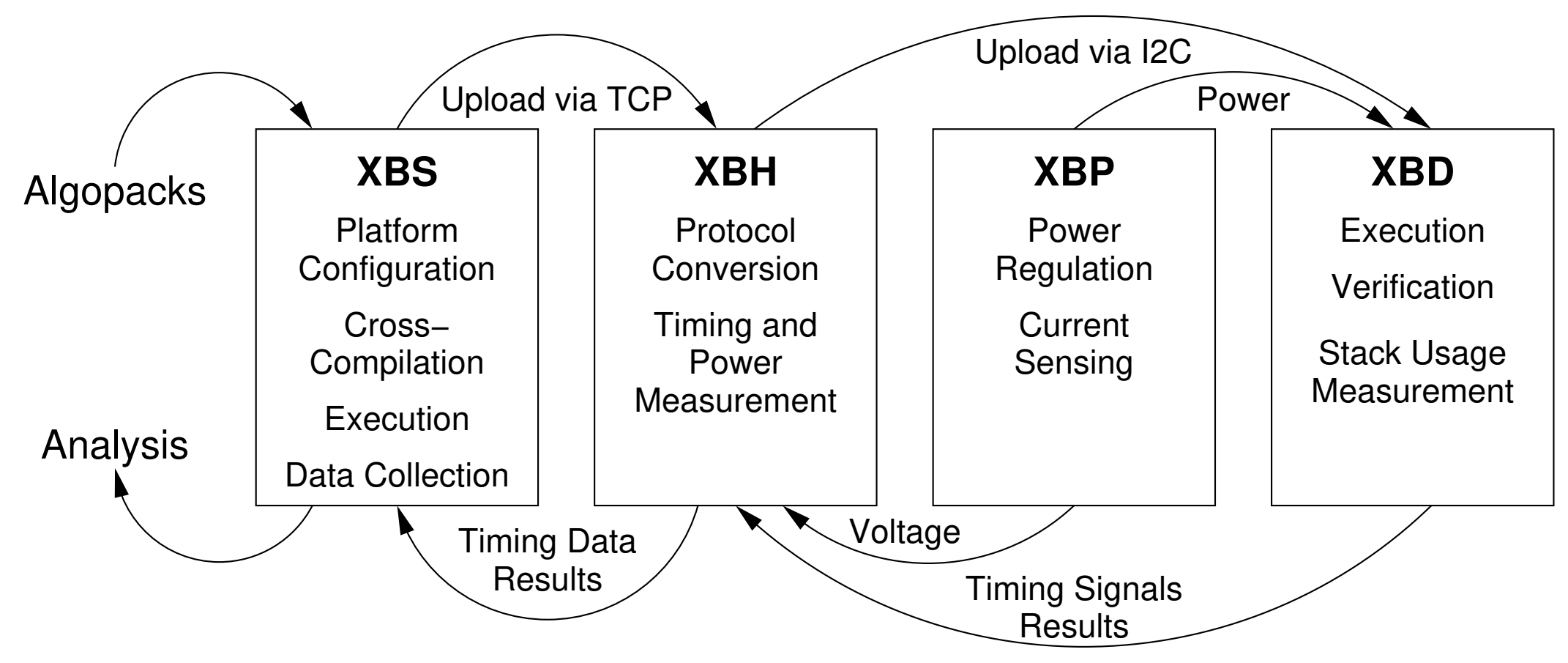
XXBX

eXtended eXternal Benchmarking eXtention extends the XBX by:

- Added power measurement
- Added support for Authenticated Encryption with Associated Data (AEAD) functions
- Replaced harness with more powerful device running FreeRTOS
- Rewrote software in Python 3 (was bash and perl)
- Result storage now in SQLite database



Main Components of XXBX



- XXBX Software – XBS
  - item
- XXBX Harness – XBH
  - item
- XXBX Power Shim – XBP
  - item
- XXBX Device Under Test – XBD
  - item

Benchmarking Flow

Text

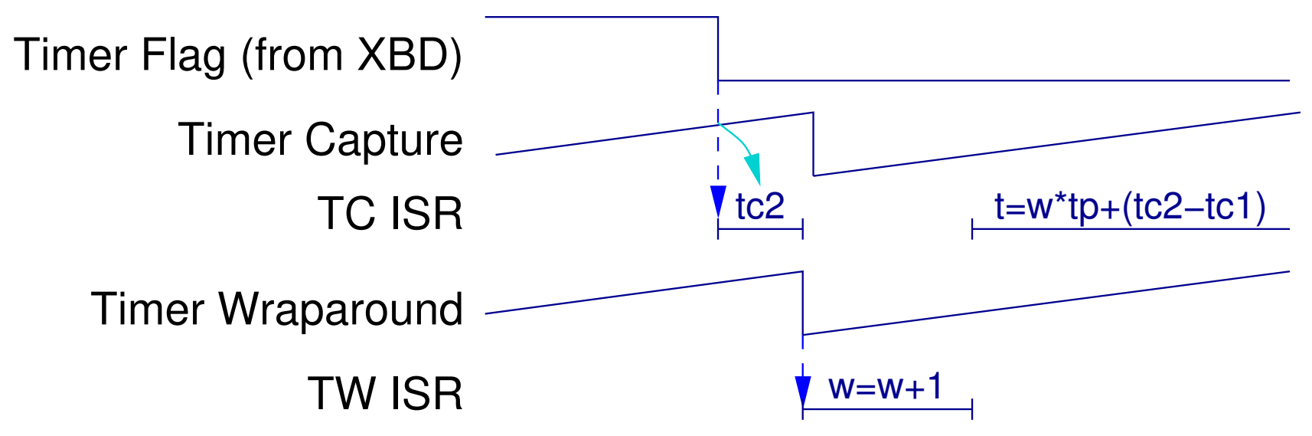
```
[hardware]
platform = msp430fr5994_16mhz
[algorithm]
operation = crypto_aead
primitives =  0cipher
              aes128n12t8silcv3
[implementation]
whitelist =  0cipher/empty
             aes128n12t8silcv3/ref
```

RAM and ROM Usage Measurement

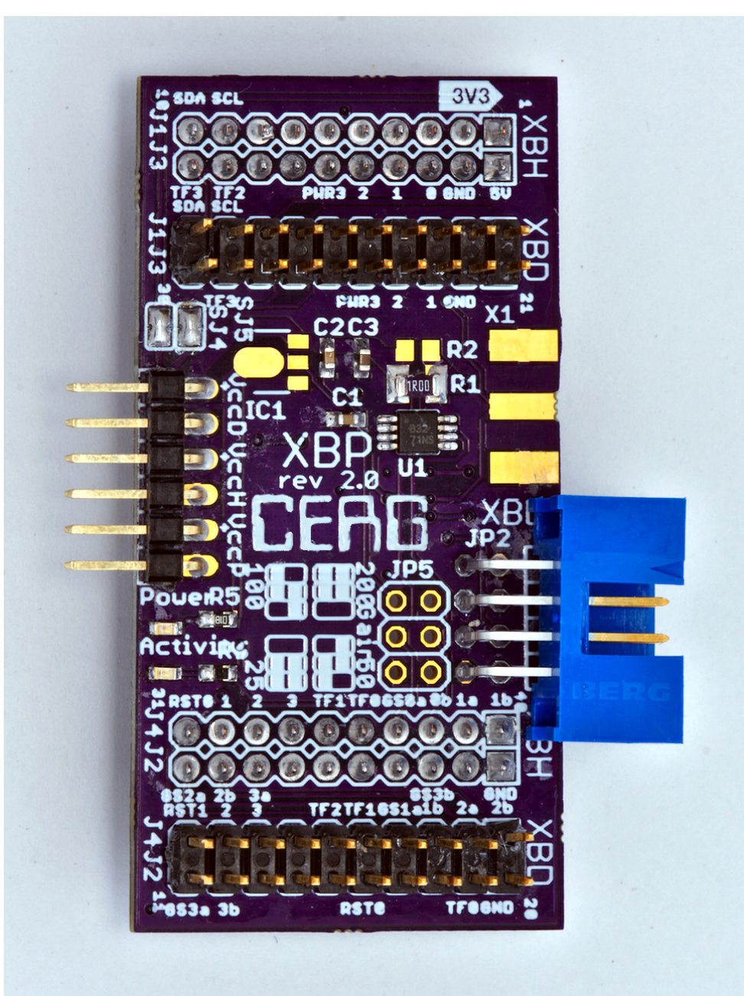
- RAM Usage
  - Bootloader??? paints memory with canary values
  - After execution of application it checks the number of addresses not containing canary values
  - This is the amount of stack memory used
- ROM Usage
  - UNIX size command is run on generated application which reports sizes of .bss, .data, and .text
  - The sum??? is the amount of ROM that is used

Timing Measurements

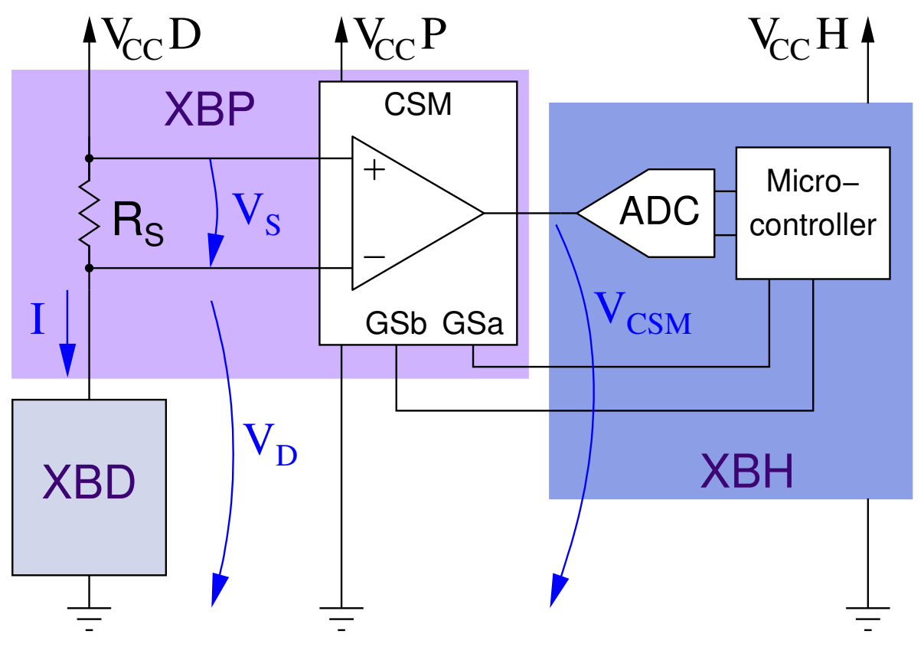
- 16-bit timer TC to capture timing flag from XBD.
- Need additional timer TW at same rate to get interrupts when timer wraps around.
- Higher priority TW counts wraps (w).
- TW can interrupt processing of TC ISR!
- Maximum time (t) is 35.8 seconds (64-bit value) at 120 MHz.



Power Measurement



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



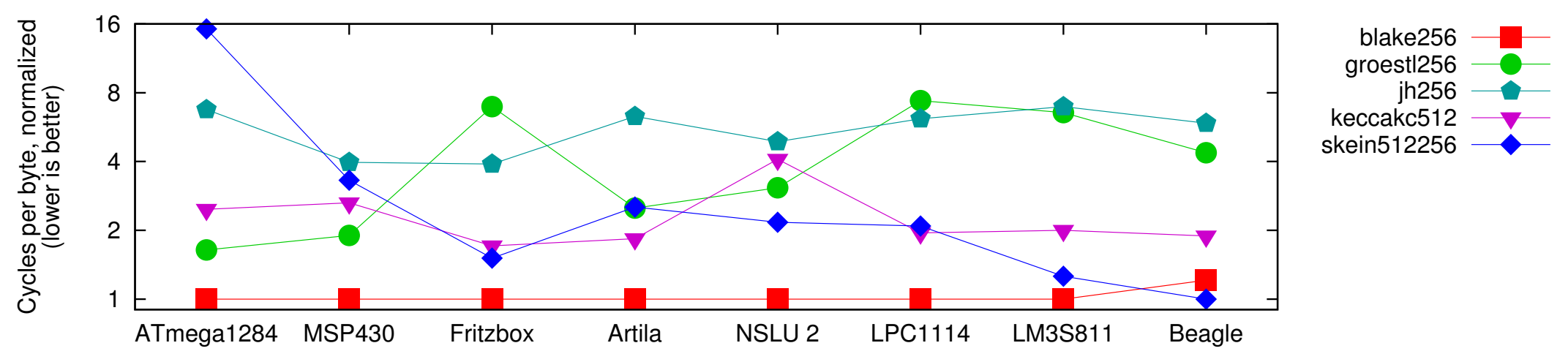
CAESAR

1. Item

CAESAR Results

Board	SASEBO				SAKURA	
		G	GII	B	X	G
Control FPGA	Virtex-2 Pro	Virtex-2 Pro	Spartan-3A	Stratix-2	Spartan-6	Spartan-6
DUT FPGA	Virtex-2 Pro	Virtex-2 Pro	Virtex-5	Stratix-2	Kintex-7	Spartan-6
Techn.	130 nm	130 nm	65 nm	90 nm	28 nm	45 nm
PC Data Comms.	RS232	RS232, FT245RL (USB)	FT2232D (USB)	RS232, FT245RL (USB)	USB	USB
Status	Discon-tinued	Discon-tinued	Discon-tinued			

Throughput of CAESAR Candidates



Caption

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