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

Text

Motivation

IOT

Benchmarking Tools

- SUPERCOP
- XBX

Missing Features
- ROM Usage
- RAM Usage
- Power Consumption

Metrics

Throughput
- Item

RAM Usage
- Item

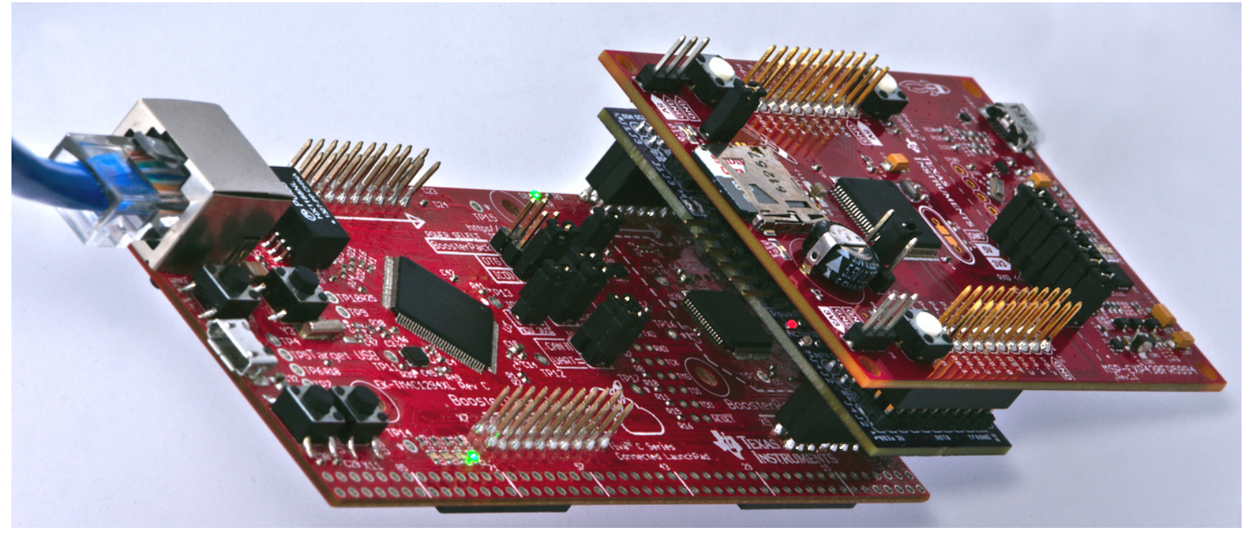
ROM Usage
- Item

Power Consumption
- Item

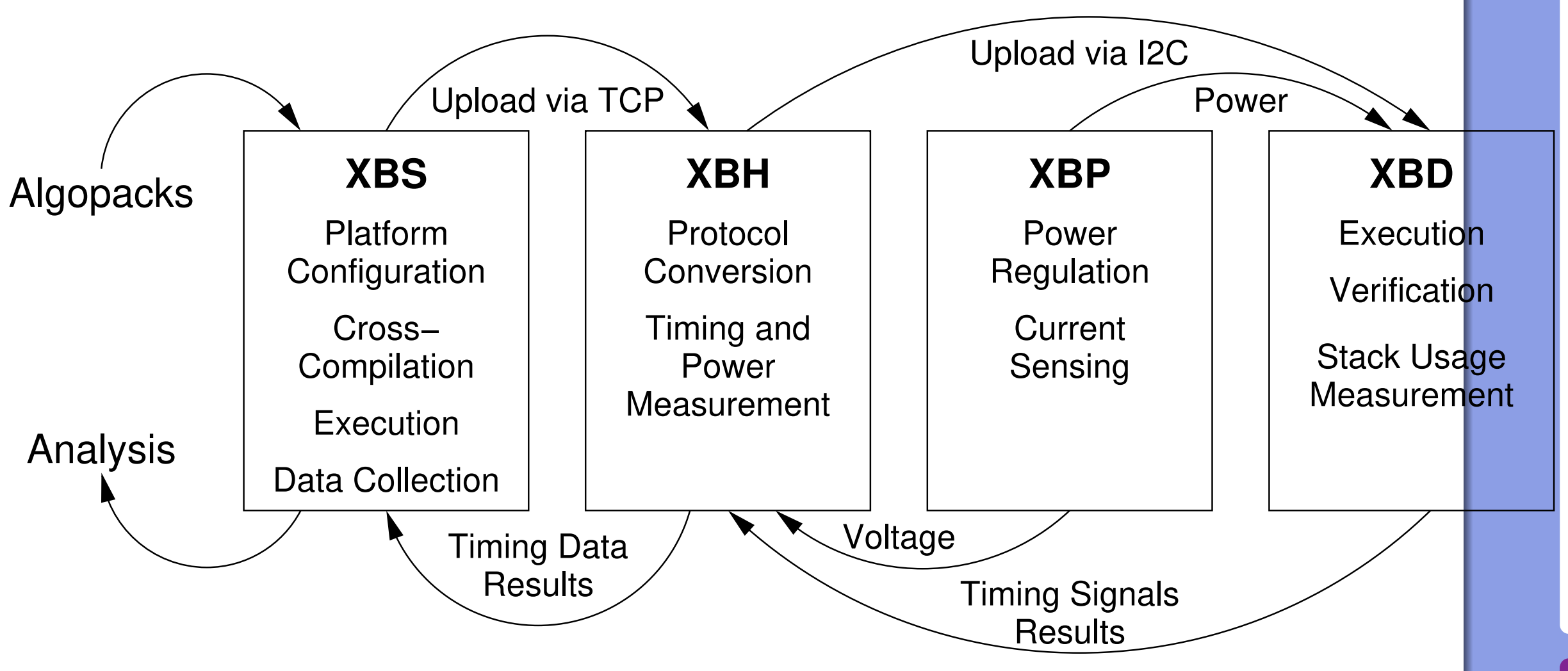
XXBX

xXtended eXternal Benchmarking eXtention, is extends the XBX by

- List of differences to XBX



Main Components of XXBX



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

Supported XBDs

Board	Manuf.	CPU	ISA	Bus
MSP-EXP430F5529	TI	MSP430F	MSP430X	16-bit
MSP-EXP430FR5994	TI	MSP430FR	MSP430X	16-bit
MSP-EXP432P401R	TI	ARM Cortex M4F	ARMv7E-M	32-bit
EK-TM4C123GXL	TI	ARM Cortex M4F	ARMv7E-M	32-bit
EK-TM4C129EXL	TI	ARM Cortex M4F	ARMv7E-M	32-bit
NUCLEO-F091RC	STM	ARM Cortex M0	ARMv6-M	32-bit
NUCLEO-F103RB	STM	ARM Cortex M3	ARMv7-M	32-bit

- FOBOS Acquisition Hardware contains
  - VHDL for the **Control Board** to interface with DUT,
  - VHDL-wrapper for the **DUT board** to instantiate a user provided algorithm, and
  - Connector description.
- FOBOS Acquisition Software is written in Python and
  - Controls FOBOS Acquisition Hardware,
  - Controls measurement equipment, and
  - Stores measurements and setup information.

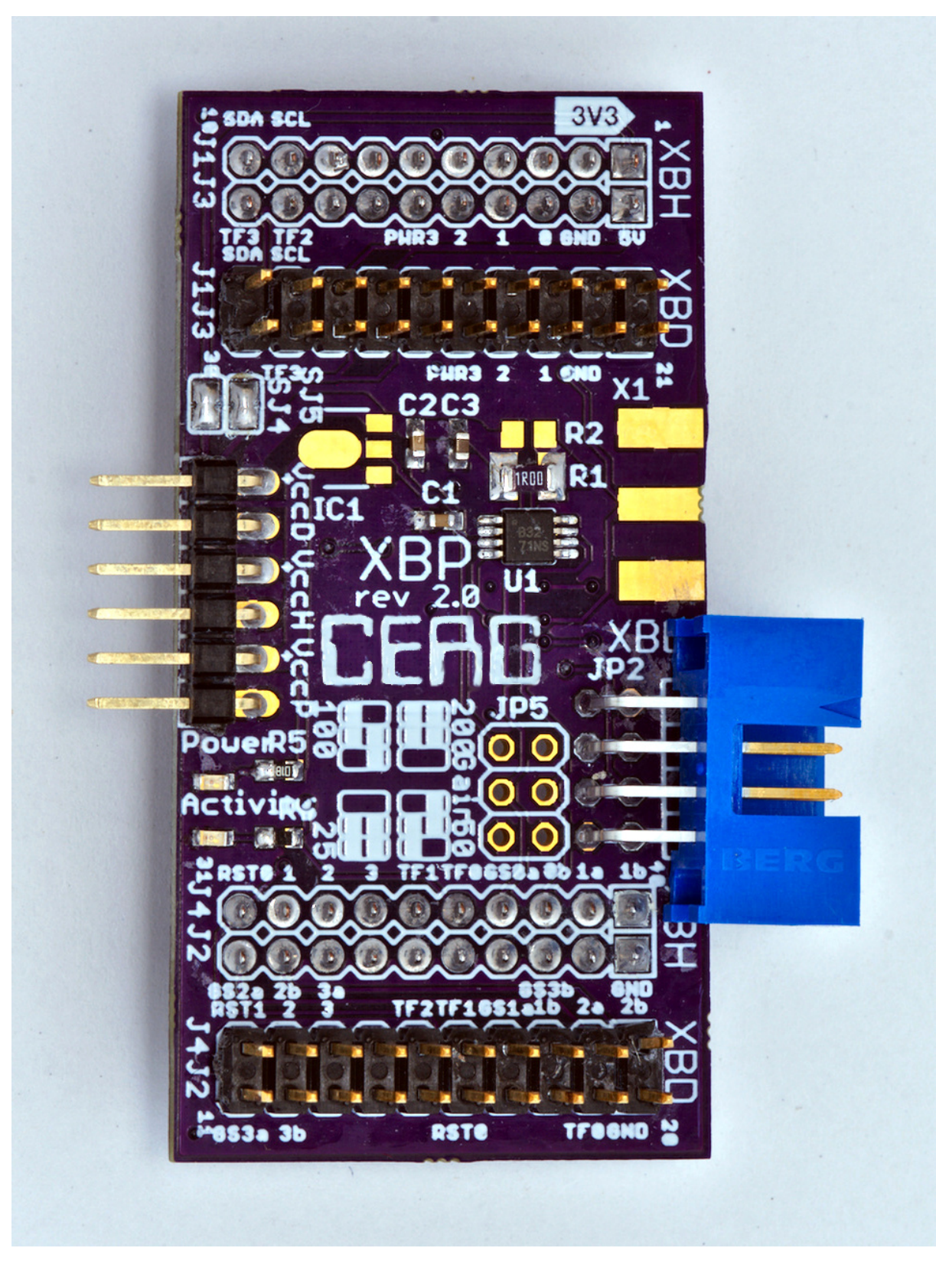
FOBOS Hardware

- FOBOS Control can be Digilent Nexys2 or Nexys3, soon Nexys4.

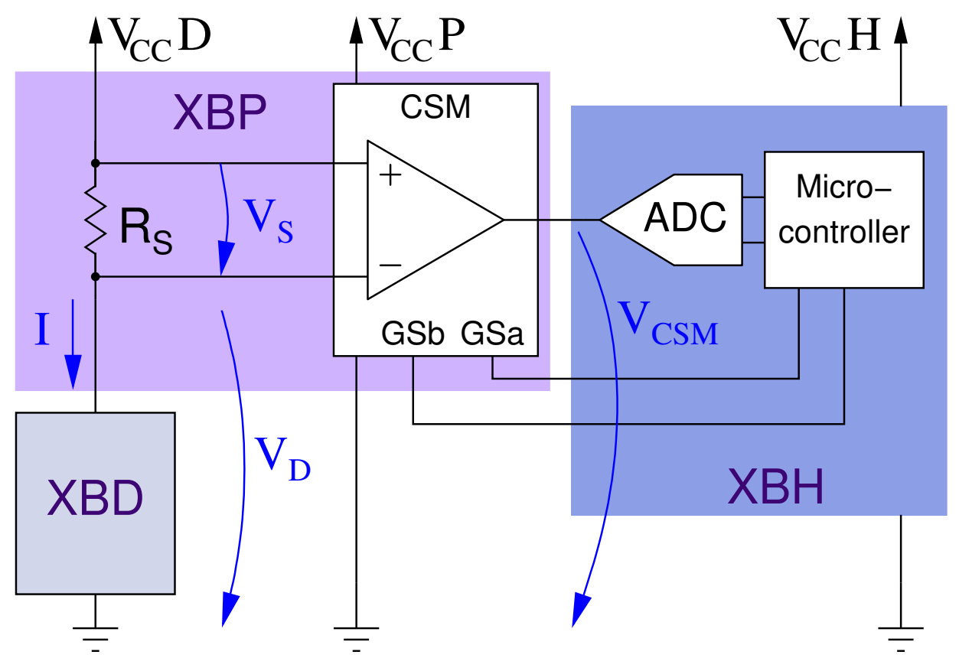
Acquisition Control

- Control Board sends Key and Plaintext to the DUT.
- After DUT receives all data, the Control Board generates the trigger.
- The trigger indicates that the cryptographic algorithm has started and initiates capture of data by the oscilloscope.

Power Measurement



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



Analysis Workflow

1. Statistics Module
   - Statistics can identify outliers in traces and samples across traces.
2. Post-Processing Module
   - The main goal of these modules is to reduce the amount of data that has to be analyzed by the SCA Module.
3. SCA Module
   - User can test his/her own power model using a library of state-of-the art side channel distinguishers.
   - FOBOS supports CPA using Spearman, Pearson, ANOVA & MIA.

Signal Alignment

- User can select any part of the trace for further analysis.
- Reduces computation time.
- The recorded trigger signal is used by FOBOS Analysis to align the power traces.

```
WINDOW_START_POINT = 100
SAMPLE_WINDOW = 1000
```

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