



# eXtended eXternal Benchmarking eXtension – XXBX

XXBX User Guide v1.0

Matthew R. Carter

Raghurama R. Velegala  
Jens-Peter Kaps  
jkaps@gmu.edu

John Pham

March 26, 2018  
George Mason University  
Fairfax, Virginia



[cryptography.gmu.edu](http://cryptography.gmu.edu)



[www.gmu.edu](http://www.gmu.edu)

**Cryptographic Engineering Research Group**

Department of Electrical and Computer Engineering      George Mason University  
3100 Engineering Building, 4400 University Drive, Fairfax, VA 22030-4444, USA  
Voice: (703) 993-1561, Fax: (703) 993-1601

# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Benchmarking . . . . .	3
1.2	Metrics . . . . .	3
1.2.1	Throughput . . . . .	3
1.2.2	ROM . . . . .	3
1.2.3	RAM . . . . .	3
1.2.4	Power . . . . .	3
<b>2</b>	<b>Previous Work</b>	<b>4</b>
2.1	SUPERCOP . . . . .	4
2.2	XXB . . . . .	4
<b>3</b>	<b>XXBX System</b>	<b>5</b>
3.1	Overview . . . . .	5
3.2	XXBX Software – XBS . . . . .	5
3.3	XXBX Harness – XBH . . . . .	5
3.4	XXBX Power Shim – XBP . . . . .	5
3.5	XXBX Device Under Test – XBD . . . . .	5
<b>4</b>	<b>Getting Started</b>	<b>6</b>
4.1	Requirements . . . . .	6
4.2	Installation . . . . .	6
4.3	Example Run . . . . .	6
4.4	Results . . . . .	6
<b>A</b>	<b>Maybe Something</b>	<b>7</b>

# 1 Introduction

## 1.1 Benchmarking

## 1.2 Metrics

### 1.2.1 Throughput

### 1.2.2 ROM

### 1.2.3 RAM

### 1.2.4 Power

## 2 Previous Work

### 2.1 SUPERCOP

### 2.2 XBX

## 3 XXBX System

### 3.1 Overview

### 3.2 XXBX Software – XBS

### 3.3 XXBX Harness – XBH

### 3.4 XXBX Power Shim – XBP

### 3.5 XXBX Device Under Test – XBD

# 4 Getting Started

4.1 Requirements

4.2 Installation

4.3 Example Run

4.4 Results

# A Maybe Something