Flexible Opensource workBench fOr Side-channel analysis

*FOBOS User Guide v*1.0

Rajesh Velegalati, Panasayya Yalla

&

Jens-Peter Kaps

{rvelegal,pyalla,jkaps}'at'gmu.edu

George Mason University

Fairfax, Virginia

Monday 9th May, 2016

Contents

Contents . . . i
List of Figures . . . iii
List of Tables . . . 0
1 Side Channel Analysis . . . 1
1.1 Introduction . . . 1
1.2 Power Analysis . . . 2
1.2.1 Simple Power Analysis (SPA) . . . 2
1.2.2 Differential/Correlation Power Analysis (DPA/CPA) . . . 2
1.2.3 Power Model . . . 2
1 FOBOS Overview . . . 1
1.1 Introduction . . . 1
1.2 Setup . . . 1
1.2.1 Acquisition . . . 1
1.2.2 Analysis . . . 1
1.3 Download & Install . . . 1
1.3.1 Windows Requirements . . . 1
1.3.2 Linux Requirements . . . 1
1.3.3 File Structure . . . 2
2 FOBOS Acquisition . . . 3
2.1 FOBOS Acquisition . . . 5
2.1.1 Requirements . . . 5
2.1.2 Oscilloscope Interface . . . 5
2.1.3 Control Board Programming . . . 5
2.1.4 DUT Board Programming . . . 5
2.2 FOBOS Acquisition Configuration . . . 5
2.2.1 Multi/Single Capture . . . 5
2.2.2 Trigger Start/Width . . . 5
2.2.3 Reset . . . 5
2.2.4 Plot Waveform . . . 5
2.2.5 FOBOS Oscilloscope Configuration . . . 5
2.3 Example . . . 5
3 FOBOS Analysis . . . 7
3.1 Power Model . . . 7
3.2 Trace Alignment . . . 7

3.3 Sample Window . . . 7
3.4 Compression . . . 7
3.5 Example . . . 7
3.6 Files . . . 7
Contents . . . iii
List of Figures . . . v
List of Tables . . . 0
1 FOBOS Overview . . . 1
1.1 Introduction . . . 1
1.2 Setup . . . 1
1.2.1 Acquisition . . . 1
1.2.2 Analysis . . . 1
1.3 Download & Install . . . 1
1.3.1 Windows Requirements . . . 1
1.3.2 Linux Requirements . . . 1
1.3.3 File Structure . . . 2
2 FOBOS Acquisition . . . 3
2.1 FOBOS Acquisition . . . 5
2.1.1 Requirements . . . 5
2.1.2 Oscilloscope Interface . . . 5
2.1.3 Control Board Programming . . . 5
2.1.4 DUT Board Programming . . . 5
2.2 FOBOS Acquisition Configuration . . . 5
2.2.1 Multi/Single Capture . . . 5
2.2.2 Trigger Start/Width . . . 5
2.2.3 Reset . . . 5
2.2.4 Plot Waveform . . . 5
2.2.5 FOBOS Oscilloscope Configuration . . . 5
2.3 Example . . . 5
3 FOBOS Analysis . . . 7
3.1 Power Model . . . 7
3.2 Trace Alignment . . . 7
3.3 Sample Window . . . 7
3.4 Compression . . . 7
3.5 Example . . . 7
3.6 Files . . . 7

List of Figures

List of Tables

Chapter 1: Side Channel Analysis

1.1 Introduction

Recent years have seen a dramatic increase of market adoption and utility of so called "smart" devices by people from all walks of life. These devices play a central role in how people are entertained, communicate, network, work, bank and shop. Yet for every positive outcome from these devices, there is often a corollary risk. For example, let us consider a smart phone. On one hand, there are billions of applications which provide unprecedented ease of access to a plethora of applications or simply termed *apps* to meet any user requirements. On the other hands, they are also are providing a fertile environment for the distribution of hostile apps or malware. Also, the increased power of these smart phones makes them more suitable for a host of business purposes, which can also result in the exposure and compromise of corporate data and systems. Finally, the very portability of mobile devices means that they are highly susceptible to loss and theft. Thus there is great need in protecting information accessed by these devices and this information is usually secured using cryptographic algorithms.

According to Kerchoff's Law (or Shannon's Maxim) [**?**],
a cryptosystem's security must be solely based on the secret key even if everything about the underlying encryption algorithm is public knowledge.
However, physical implementations in hardware as well as in software of such encryption algorithms have been shown to leak secret information in the form of so called side-channels and also during sudden change in operational characteristics of the crypto-device i.e. via *Fault Injection*. The side-channel leakage could be in the form of power consumption [**?**], electro magnetic radiation [**?**] or timing [**?**] of the device. The side-channels leak sensitive information whenever the device performs an operation using the secret data. Attacks which make use of such inhAnalysiserent physical leakage are called side-channel attacks SCA. SCA is a new research area of applied cryptanalysis that has gained popularity since mid nineties. The research in this area shows that SCA pose a major threat because the physical implementations of the cryptographic devices are difficult to control and often result in unintended leakage of information. Generally, all hardware implementations of cryptographic algorithms are assumed to be vulnerable to side channel cryptanalysis, if there are no special precautions in the implementation.

1.2 Power Analysis

1.2.1 Simple Power Analysis (SPA)

1.2.2 Differential/Correlation Power Analysis (DPA/CPA)

Difference of Means

Spearman Rank Coefficient

Pearson's r

1.2.3 Power Model

Hamming Distance (HD)

Hamming Distance HD

Hamming Weight (HW)

Hamming Weight HW

Chapter 2: FOBOS Overview

2.1 Introduction

2.2 Setup

2.2.1 Acquisition

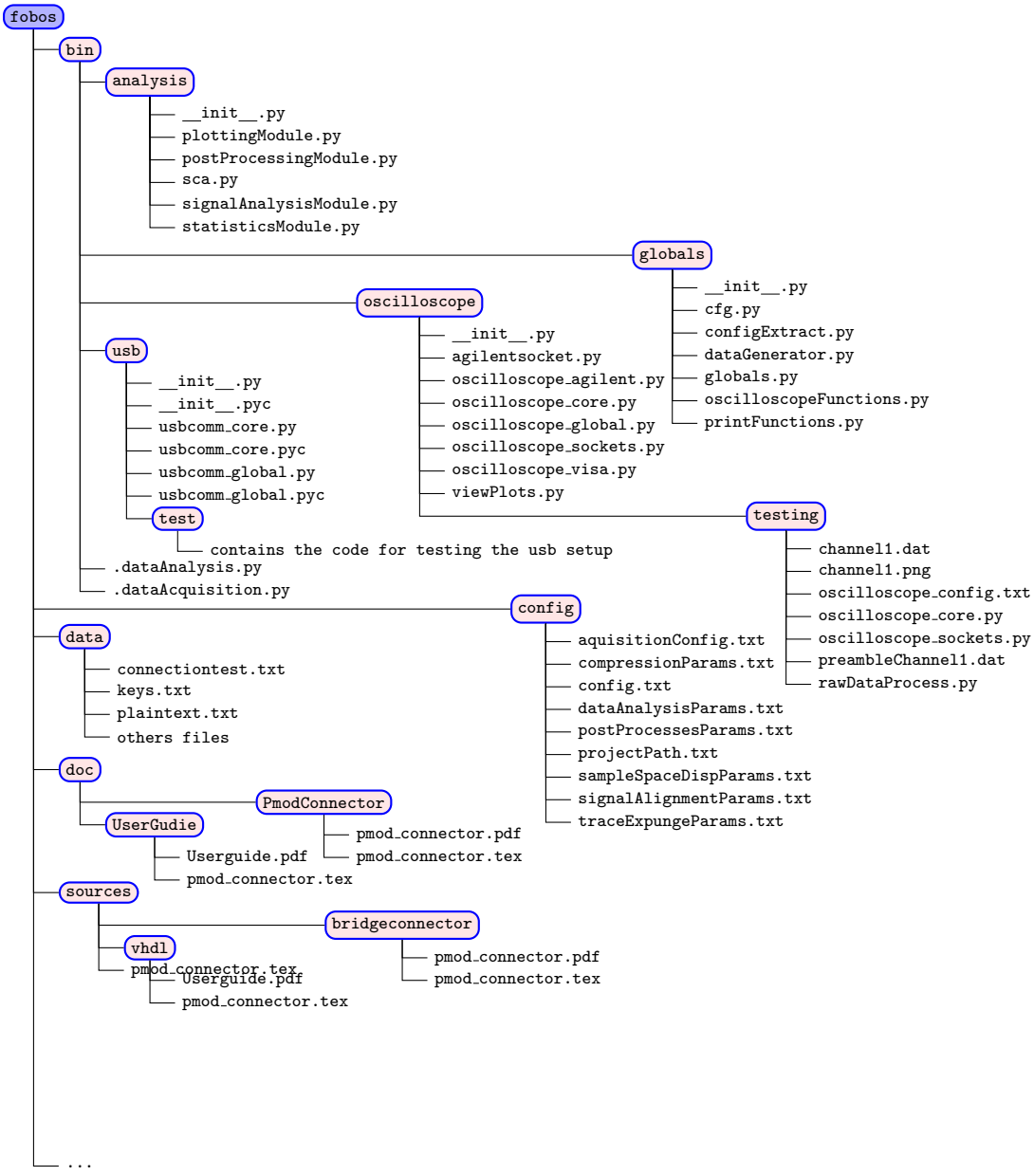
2.2.2 Analysis

2.3 Download & Install

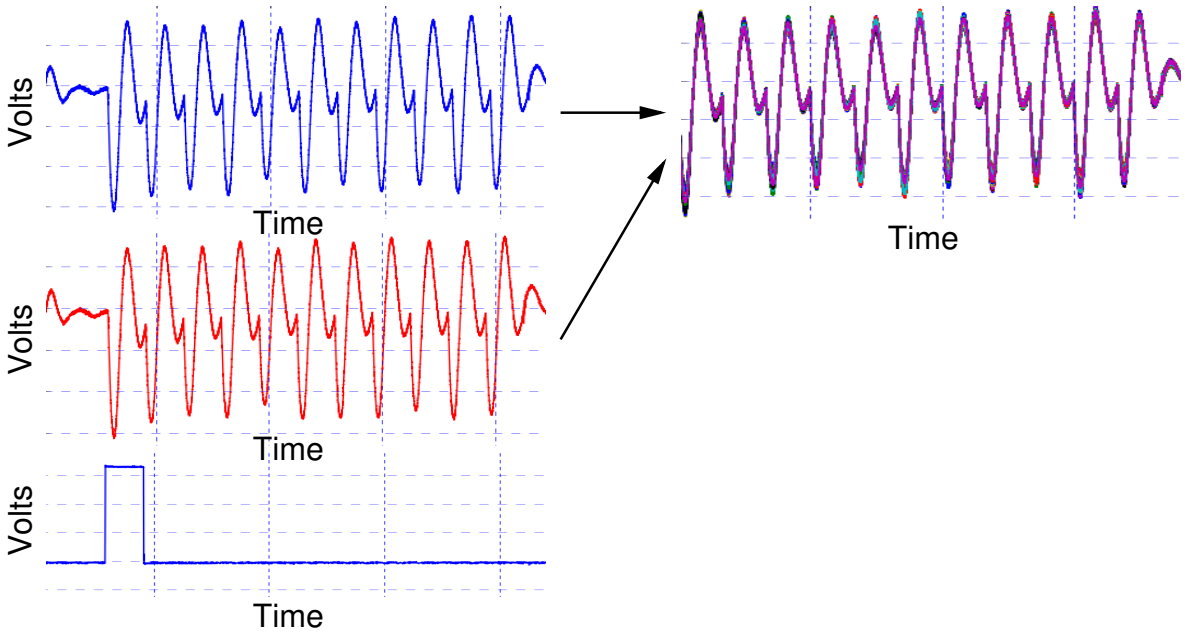
2.3.1 Windows Requirements

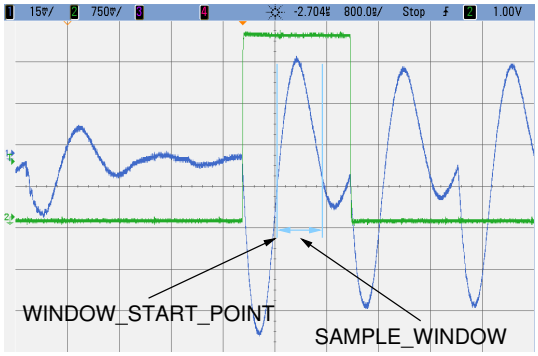
2.3.2 Linux Requirements

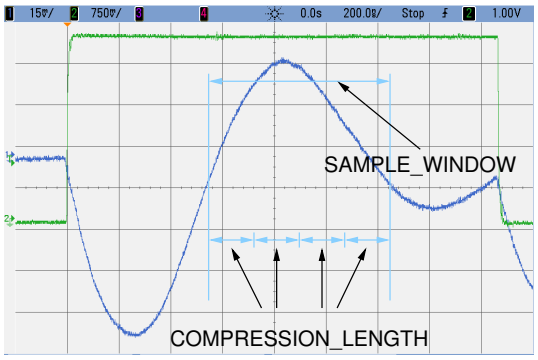
2.3.3 File Structure



Chapter 3: FOBOS Acquisition


Volts
Time
Volts
Time
Volts
Time
Time


WINDOW_START_POINT
SAMPLE_WINDOW


SAMPLE_WINDOW
COMPRESSION_LENGTH

3.1 FOBOS Acquisition

3.1.1 Requirements

3.1.2 Oscilloscope Interface

3.1.3 Control Board Programming

Connections to DUT

Bus width

UCF

3.1.4 DUT Board Programming

Crypto Algorithm Wrapper

3.2 FOBOS Acquisition Configuration

3.2.1 Multi/Single Capture

3.2.2 Trigger Start/Width

Signal Alignment

Signal Space Disposition

Signal compression

3.2.3 Reset

3.2.4 Plot Waveform

3.2.5 FOBOS Oscilloscope Configuration

3.3 Example

Chapter 4: FOBOS Analysis

4.1 Power Model

4.2 Trace Alignment

4.3 Sample Window

4.4 Compression

4.5 Example

4.6 Files

dataAnalysisParams.txt

Location:fobos/bin/config/dataAnalysisParams.txt

```
WORK_DIR = FOBOSAnalysis
MEASUREMENT_WORK_DIR = FOBOSWorkspace
TAG = counter
```

compressionParams.txt

Location:fobos/bin/config/compressionParams.txt

```
#####################################################
######## Compression Module Parameters #############
#####################################################
COMPRESSION_LENGTH = 40
COMPRESSION_TYPE = MAX   # MAX|MIN|MEAN
```

postProcessesParams.txt

Location:fobos/bin/config/postProcessesParams.txt

```
#####################################################
######## Post Processing Flow ######################
#####################################################
SAMPLE_SPACE_DISPOSITION = 2 # 1-3|NO
COMPRESS_DATA = 3 #1-3|NO
TRACE_EXPUNGE = 1 #1-3|NO
TRACE_EXPUNGE_PARAMS = VAR-0.0000110:0.0000139 #STD|VAR-BELOW:ABOVE|NO
```

projectPath.txt

Location:fobos/bin/config/projectPath.txt

```
/home/pyalla/projects/fobos/FOBOSWorkspace/testing/16-testing
```

sampleSpaceDispParams.txt

Location:fobos/bin/config/sampleSpaceDispParams.txt

```
#####################################################
#### Sample Space Disposition Module Parameters ####
#####################################################
SAMPLE_WINDOW = 3300
WINDOW_START_POINT = 500
```

signalAlignmentParams.txt

Location:fobos/bin/config/signalAlignmentParams.txt

```
#####################################################
######## Signal Alignment Module Parameters ########
#####################################################
CAPTURE_MODE = SINGLE # MULTI|SINGLE
TRIGGER_THRESHOLD = 1.0
```

traceExpungeParams.txt

Location:fobos/bin/config/traceExpungeParams.txt

```
#####################################################
######## Trace Expunge Module Parameters ############
#####################################################
TRACE_EXPUNGE_PARAMS = VAR:0.0000109:0.0000137 #STD|VAR:BELOW:ABOVE|NO
```

config.txt

Location:fobos/bin/config/config.txt

```
################################################################################
#                                                                              #
#   Copyright 2014 CERG                                                        #
#                                                                              #
#   Licensed under the Apache License, Version 2.0 (the "License");           #
#   you may not use this file except in compliance with the License.           #
#   You may obtain a copy of the License at                                    #
#                                                                              #
#       http://www.apache.org/licenses/LICENSE-2.0                             #
#                                                                              #
#   Unless required by applicable law or agreed to in writing, software        #
#   distributed under the License is distributed on an "AS IS" BASIS,          #
#   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.#
#   See the License for the specific language governing permissions and        #
#   limitations under the License.                                             #
#                                                                              #
################################################################################
# ================================================
# ================================================
# Global Settings
# ================================================
# ================================================
WORK_DIR      = FOBOSWorkspace
SOURCE_DIR    = sources
PROJECT_NAME = testing
TAG = counter
# ================================================
# ================================================
# Plot Generator Settings
# ================================================
# ================================================
PLOT_LABELS_FONT_FAMILY = sans-serif
PLOT_LABELS_FONT_WEIGHT = normal
PLOT_LABELS_FONT_SIZE = 12
PLOT_SIZE_LENGTH = 34.5 #In Inches
PLOT_SIZE_BREADTH = 15.5 #In Inches
GENERATE_EPS_PDF_GRAPHS = NO #YES|NO
DISPLAY_THREE_SIGMAS = 3 # 1|2|3
```

Flexible Opensource BOard for Side-channel analysis

*FOBOS Reference Manual v*1.0

Rajesh Velegalati, Panasayya Yalla

&

Jens-Peter Kaps

{rvelegal,pyalla,jkaps}'at'gmu.edu

George Mason University

Fairfax, Virginia

Monday 9th May, 2016

www.gmu.edu

Contents

List of Figures

List of Tables

Chapter 1: FOBOS Overview

1.1 Introduction

1.2 Setup

1.2.1 Acquisition

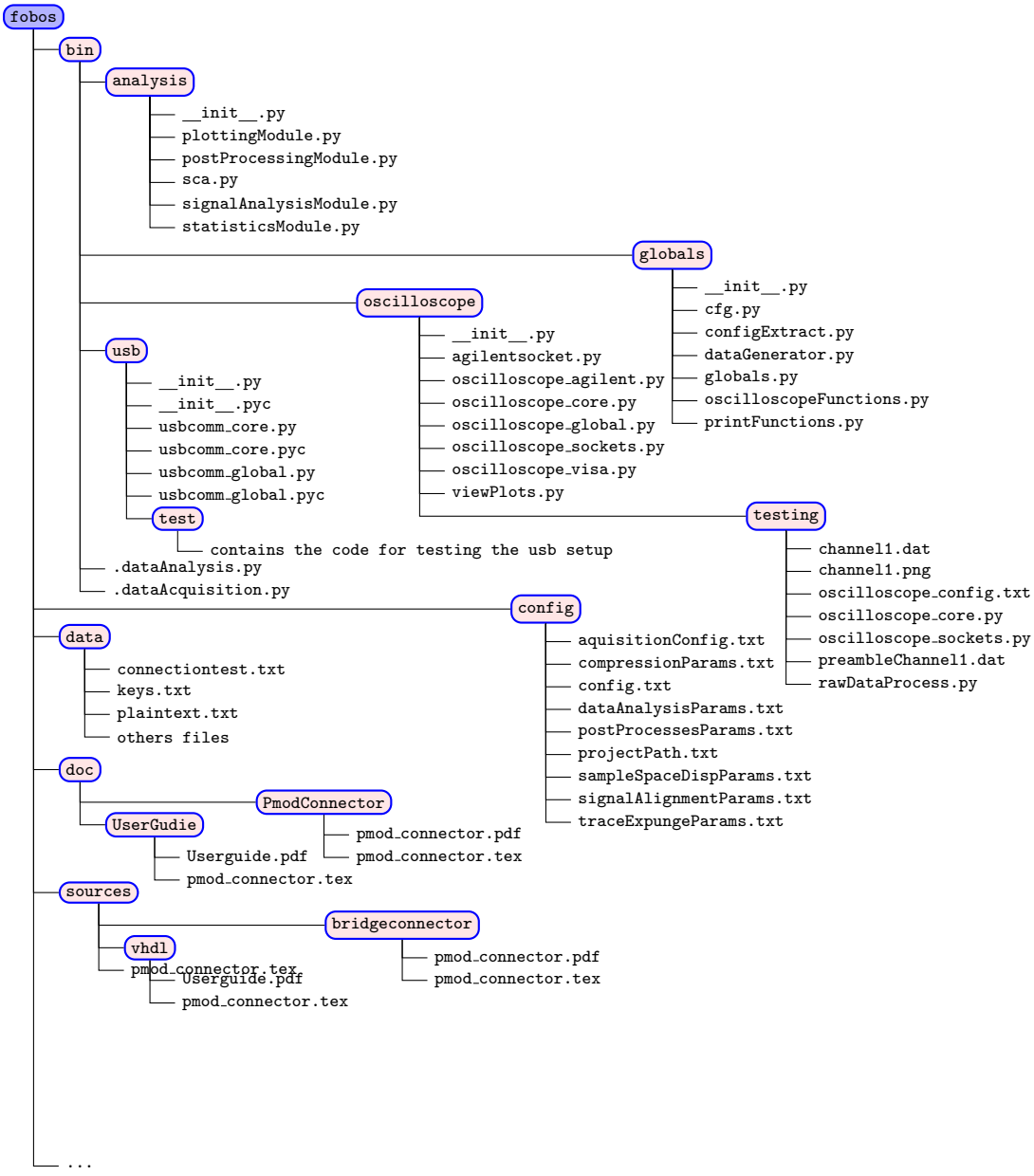
1.2.2 Analysis

1.3 Download & Install

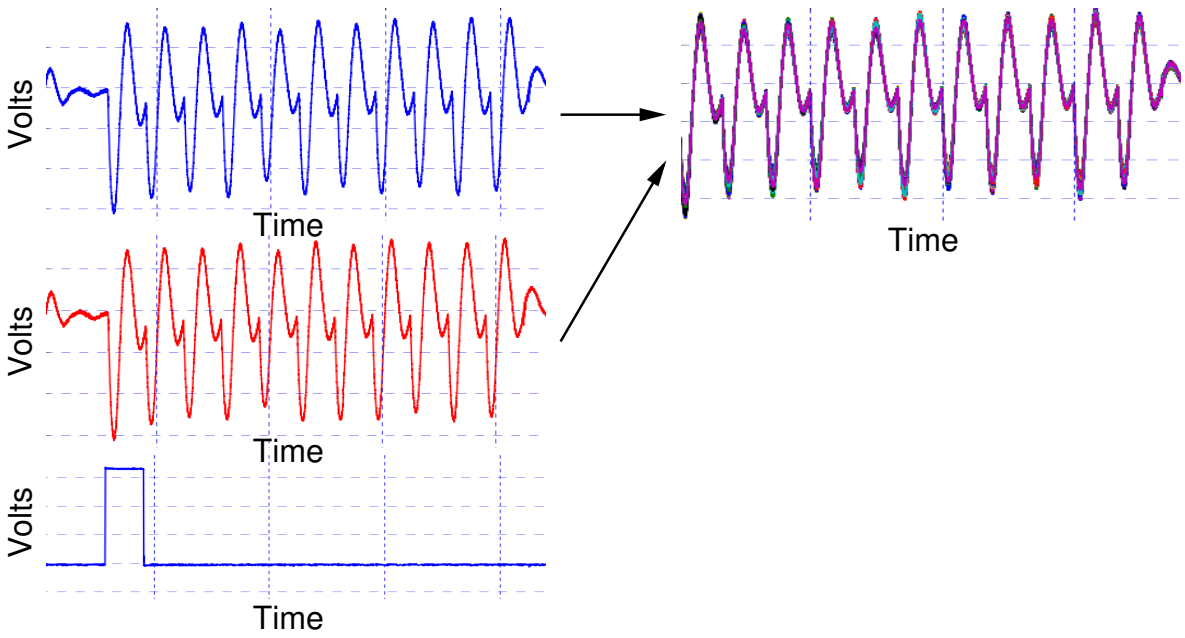
1.3.1 Windows Requirements

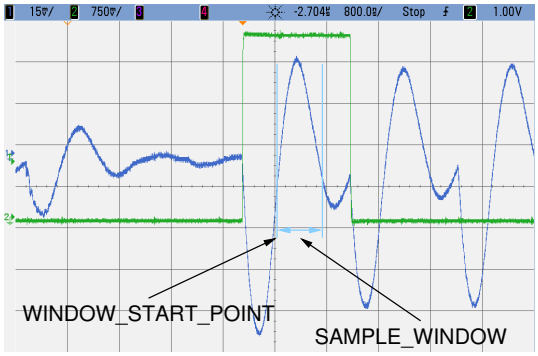
1.3.2 Linux Requirements

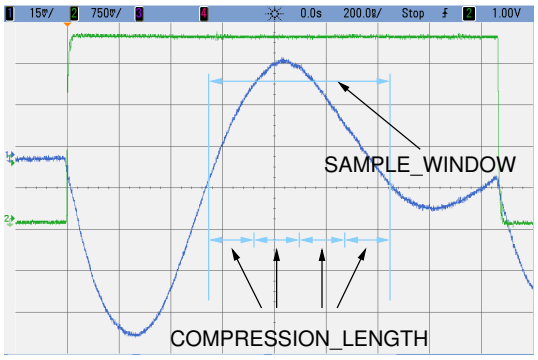
1.3.3 File Structure



Chapter 2: FOBOS Acquisition


Volts
Time
Volts
Time
Volts
Time
Time


WINDOW_START_POINT
SAMPLE_WINDOW


SAMPLE_WINDOW
COMPRESSION_LENGTH

2.1 FOBOS Acquisition

2.1.1 Requirements

2.1.2 Oscilloscope Interface

2.1.3 Control Board Programming

Connections to DUT

Bus width

UCF

2.1.4 DUT Board Programming

Crypto Algorithm Wrapper

2.2 FOBOS Acquisition Configuration

2.2.1 Multi/Single Capture

2.2.2 Trigger Start/Width

Signal Alignment

Signal Space Disposition

Signal compression

2.2.3 Reset

2.2.4 Plot Waveform

2.2.5 FOBOS Oscilloscope Configuration

2.3 Example

Chapter 3: FOBOS Analysis

3.1 Power Model

3.2 Trace Alignment

3.3 Sample Window

3.4 Compression

3.5 Example

3.6 Files

dataAnalysisParams.txt

Location:fobos/bin/config/dataAnalysisParams.txt

```
WORK_DIR = FOBOSAnalysis
MEASUREMENT_WORK_DIR = FOBOSWorkspace
TAG = counter
```

compressionParams.txt

Location:fobos/bin/config/compressionParams.txt

```
#####################################################
######## Compression Module Parameters #############
#####################################################
COMPRESSION_LENGTH = 40
COMPRESSION_TYPE = MAX   # MAX|MIN|MEAN
```

postProcessesParams.txt

Location:fobos/bin/config/postProcessesParams.txt

```
#####################################################
######## Post Processing Flow ######################
#####################################################
SAMPLE_SPACE_DISPOSITION = 2 # 1-3|NO
COMPRESS_DATA = 3 #1-3|NO
TRACE_EXPUNGE = 1 #1-3|NO
TRACE_EXPUNGE_PARAMS = VAR-0.0000110:0.0000139 #STD|VAR-BELOW:ABOVE|NO
```

projectPath.txt

Location:fobos/bin/config/projectPath.txt

```
/home/pyalla/projects/fobos/FOBOSWorkspace/testing/16-testing
```

sampleSpaceDispParams.txt

Location:fobos/bin/config/sampleSpaceDispParams.txt

```
#####################################################
#### Sample Space Disposition Module Parameters ####
#####################################################
SAMPLE_WINDOW = 3300
WINDOW_START_POINT = 500
```

signalAlignmentParams.txt

Location:fobos/bin/config/signalAlignmentParams.txt

```
#####################################################
######## Signal Alignment Module Parameters ########
#####################################################
CAPTURE_MODE = SINGLE # MULTI|SINGLE
TRIGGER_THRESHOLD = 1.0
```

traceExpungeParams.txt

Location:fobos/bin/config/traceExpungeParams.txt

```
#####################################################
######## Trace Expunge Module Parameters ############
#####################################################
TRACE_EXPUNGE_PARAMS = VAR:0.0000109:0.0000137 #STD|VAR:BELOW:ABOVE|NO
```

config.txt

Location:fobos/bin/config/config.txt

```
################################################################################
#                                                                              #
#   Copyright 2014 CERG                                                        #
#                                                                              #
#   Licensed under the Apache License, Version 2.0 (the "License");           #
#   you may not use this file except in compliance with the License.           #
#   You may obtain a copy of the License at                                    #
#                                                                              #
#       http://www.apache.org/licenses/LICENSE-2.0                             #
#                                                                              #
#   Unless required by applicable law or agreed to in writing, software        #
#   distributed under the License is distributed on an "AS IS" BASIS,          #
#   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.#
#   See the License for the specific language governing permissions and        #
#   limitations under the License.                                             #
#                                                                              #
################################################################################
# ================================================
# ================================================
# Global Settings
# ================================================
# ================================================
WORK_DIR      = FOBOSWorkspace
SOURCE_DIR    = sources
PROJECT_NAME = testing
TAG = counter
# ================================================
# ================================================
# Plot Generator Settings
# ================================================
# ================================================
PLOT_LABELS_FONT_FAMILY = sans-serif
PLOT_LABELS_FONT_WEIGHT = normal
PLOT_LABELS_FONT_SIZE = 12
PLOT_SIZE_LENGTH = 34.5 #In Inches
PLOT_SIZE_BREADTH = 15.5 #In Inches
GENERATE_EPS_PDF_GRAPHS = NO #YES|NO
DISPLAY_THREE_SIGMAS = 3 # 1|2|3
```