Flexible Opensource BOard for Sidechannel analysis

FOBOS Version 0.1

Table of Contents

1 FOBOS - Capture Module 3
2 FOBOS - Analysis Module 3

1 FOBOS - Capture Module

2 FOBOS - Analysis Module

FOBOS's analysis module uses a set of python scripts to post process the raw measurement data obtained from the oscilloscope and perform analysis on the obtained data Various functions implemented in the Analysis module is described below:

Table 1. Config Extract Functions

configExtract.extractAnalysisConfigAttributes()	
Usage	`$configExtract.extractAnalysisConfigAttributes(filename)`
Description	Loads the configuration attributes required for various analysis sub-modules
Inputs	file-name
Outputs	None

Table 2. Signal Alignment Functions

signalAlignmentModule.getAlignedMeasuredPowerData()	
Usage	`$signalAlignmentModule.getAlignedMeasuredPowerData()`
Inputs	None
Outputs	An M x N numpy array matrix
Description	Aligns all the raw measured data obtained from the oscilloscope with respect to trigger signal. This function returns a M x N numpy array matrix where there are M encryptions/decryptions and N oscilloscope sample points per measurement

Table 3. Signal Alignment Functions

signalAlignmentModule.acquireHypotheticalValues()	
Usage	`$signalAlignmentModule.acquireHypotheticalValues(filename)`
Inputs	filename
Outputs	An M x N numpy array matrix
Description	Loads the hypothetical power model into an M x N numpy array where there are M secret key guesses and N encryptions. This file is to be placed in `$fobos\powermodels` directory.