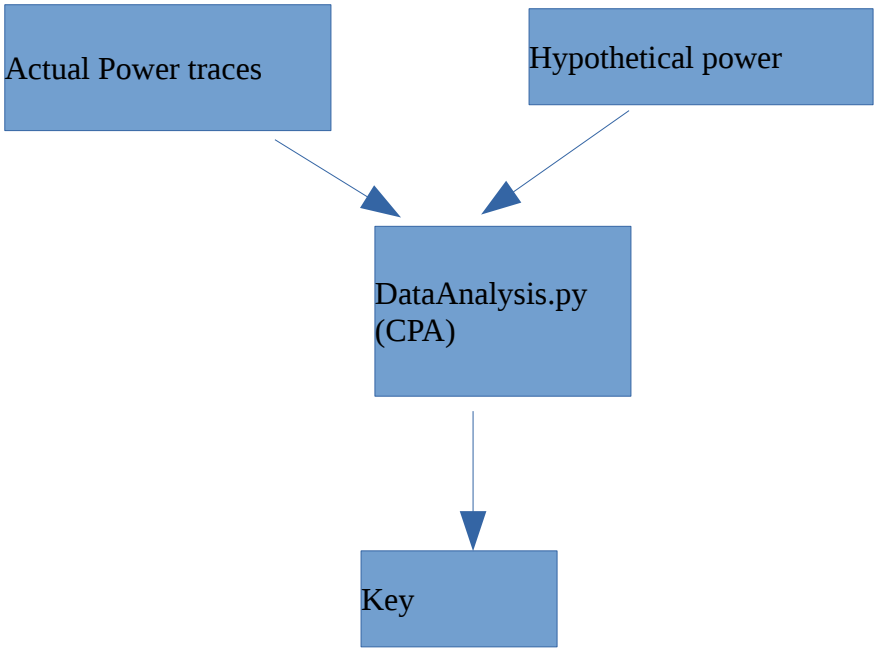
FOBOS CPA

Once acquisition is complete Correlation Power Analysis CPA can be performed.
User must provide their own power model and calculate hypothetical power for each key guess.
FOBOS takes the hypothetical power for each key guess and use a correlation method e.g. Pearson's coefficient and calculates the correlation values.
The key guess that achieves the highest correlation is a candidate for correct key.

The Analysis module is used to perform DPA attack on power traces collected by the Acquisition module. To Perform CPA, two inputs are needed, the power traces and and hypothetical power.



Steps to perform CPA using FOBOS

1- Hypothetical power calculating

Power model or hypothetical power data is user provided. FOBOS uses a text file for each key byte. This file includes a line for each key guess value (i.e. 0-255). Each line inculdes hypothetical power value for the specific key guess for all encryptions. Each value is an integer and separated from next value by a space. Fig X is an example for one key byte. The firs number is the estimated power when the byte equals zero for the frist encryption, first value in the second line is the estimated power when the key byte equals one for the first encryption and so on.
FOBOS expects to find these files at $fobos/data/. File names should be HPower_byte_< BYTE NUMBER>.txt.

Here is sample of Hpower_byte_0.txt

6 4 4 2 5 4 3 5 7 4 5 5 7 3 4 6 5 2 4 5 3 4 3 4 7 4 ….
5 3 4 5 4 2 5 7 4 4 2 4 3 2 4 4 3 4 2 4 3 6 3 2 1 5 ….
.
.
.

2- CPA configuration

There are few configuration files that controls the CPA analysis:
Here we list all the configuration parameters used in the FOBOS Analysis and description of usage:

dataAnalysisParams.txt

Parameter	Description	Example
WORK_DIR	Directory to save analysis files (Inside the measurements director)	analysis
MEASUREMENT_WORK_DIR	The name of the measurement directory	FOBOSWorkspace
TAG	The type of prefix for the directory name. Used to distinguish different runs.	counter

samplesSpacesDisp.txt

Parameter	Description	Possible Values
SAMPLE_WINDOW_SIZE	Number of samples (per trace) to be used in analysis.	Number (e.g. 2000)
SAMPLE_WINDOW_START	The number of the first sample in the window.	Number (e.g. 100)

signalAlignmentParams.txt

Parameter	Description	Possible values
COMPRESSION_LENGTH	Number of samples to be compressed into one samples.	Number (e.g. 10)
COMPRESSION_TYPE	The operation to be performed to generate the compressed sample.	MEAN | MAX | MIN

Here is a sample of configuration files above. These were used in the Example AES attack

dataAnalysisParams.txt

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

compressionParams.txt

```
#####################################################
######## Compression Module Parameters #############
#####################################################
COMPRESSION_LENGTH = 10
COMPRESSION_TYPE = MEAN # MAX|MIN|MEAN
```

sampleSpaceDispParams.txt

```
#####################################################
#### Sample Space Disposition Module Parameters ####
#####################################################
SAMPLE_WINDOW_SIZE = 3000
SAMPLE_WINDOW_START = 3000
```

3- Running Data Analysis

Data Analysis can be run as follows:
cd $fobos
python dataAnalysis.py
Once this is done, the script reads the measured and hypothetical power data, runs CPA and produces several output files. The script prompts the user for the directory that contains the traces and then uses the power data in the measurements director as input. The script will create a new directory each time it runs. This directory is created in the project directory. Output files will be save in $fobos/$workspace/$projectName/$attempt#/analysis/$analysis-attempt/. Where $analysis-attempt is a folder with a unique name created each time the script runs.