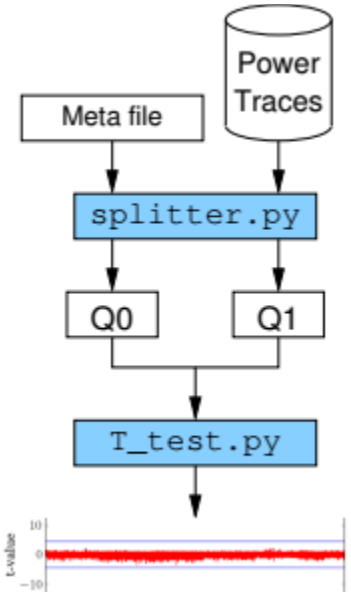
FOBOS T-test Guide

Welch’s T-test is used as a tool for leakage assessment. This guide describes using FOBOS to perform a fixed-vs-random t-test.
Test vector generation

Fixed-vs-random t-test uses interleaved fixed and random test vectors. We can select a fixed test vector D and create as set of test vectors that interleaves D and a randomly selected test vector. The interleaving is random.



For example the following test vector has been used to perform a t-test on an algorithm implemented on FOBOS DUT.

2- Reforming a t-test

Once FOBOS is used to perform acquisition and traces has been collected, scripts are used to perform the t-test.

1- Confiure the t-Test in fobos/config/analysis.ini

```
#Analysis config file
#This file follows the INI format
[tTest]
cleanTraceFile = cleanTrace.npy
cleanTraceNum  = 2000

maxTrace = 2000

tValuesFile = t_values.npy
tPlotFile = t_plot.png
stateFile = state_file.txt

Q0File = traces0.npy
Q1File = traces1.npy

fvrFile = fvrchoicefile.txt
tValuesPlotFile = t_values.png
profilerPlot = profiler_plot.png
```

Mos of the config are file names for input and output files. The most important parameter to configure is the cleanTraceNum which is the total number of traces.
<Y LIM/XLIM config>

Run the fobos/bin/tTest.py file
This will display a menu with all the measurements done in the current project.
You can select a measurement and the t-test will be performed on it.