Flexible, Opensource workBench fOr Side-channel analysis (FOBOS)

Rajesh Velegalati, Panasayya Yalla, Jens-Peter Kaps
Department of Electrical and Computer Engineering, George Mason University, Fairfax, Virginia 22030, USA

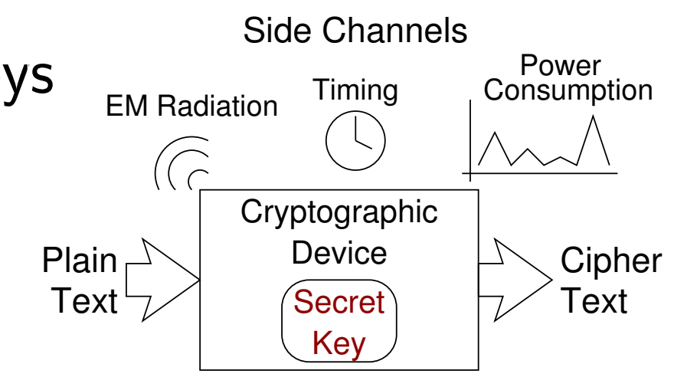
Cryptographic Engineering Research Group

Abstract

Side-channel analysis (SCA) attacks pose a growing threat to implementations of cryptographic algorithms implemented in software as well as in hardware. Current standard side-channel evaluation boards with Field Programmable Gate Arrays (FPGAs), that allow for exploring the vulnerability of cryptographic implementations on FPGAs, are expensive and available only for a few FPGA devices. Furthermore, a complete open source software package that includes drivers that run test cases on the board, control the measurement equipment, and contain several side-channel analysis techniques is not readily available. Each user has to assemble their own setup based on software packages from multiple sources, written in multiple languages and write parts themselves. Additionally, this complexity and cost makes it very difficult, if not impossible, to educate students on side-channel analysis through hands-on laboratory exercises. FOBOS is an open-source framework for conducting side-channel attacks on FPGAs which supports multiple FPGA devices and includes all necessary software to run differential power analysis attacks, which are the most prominent kind of side-channel attacks. Through its completeness and support for educational FPGA boards it is an ideal teaching tool.

Side Channel Analysis (SCA)

- Danger: Implementations are susceptible to Side Channel Analysis (SCA).
  - Key space 256-bit, $2^{256} = 1.2 \cdot 10^{77}$keys
  - Atoms in Universe (wikipedia) $9.4 \cdot 10^{79}$
  - SCA allows to attack 8-bit at a time
  - SCA complexity $\frac{256}{8} \cdot 2^8 = 8192$



- These are passive, non invasive attacks.
- They are difficult to detect.
- The measurement setup is not very expensive.
- Applies to Software as well as Hardware implementations.

Current SCA Evaluation Solutions

AES

- NIST standard for block ciphers.
- Based on Rijndael block cipher.
- 128-bit block size.
- 128/192/256-bit key size.

Keccak-$p[1600, n_r]$

- Permutation based on Keccak, winner of competition for next Secure Hash Algorithm (SHA-3).
- 1600-bit state size.

Drawbacks of Current Solutions

- IA Meter only performs acquisition using Python.
- OpenSCA Toolbox performs only analysis using Matlab.
- SASEBO has very limited FPGA support und uses C#.
  - DPA resistance depends on FPGA family.
  - DPA resistance depends on FPGA packaging (e.g., w/ or w/o capacitances).
- Currently only a patchwork of scripts and tools exist.
- No complete, free, and open-source solution is available.
- No inexpensive out-of-the-box solution for education.

Modes of Operation Summary

AES / Rijndael* and Keccak Modes (Rd. = Number of rounds)

	Operation	Mode	Block	Key	Rd.	ρ	Inputs	Outputs
AES	Hash*	AES-Hash	256	N/A	14		$\lvert M\rvert, M$	H
	MAC	CMAC	128	128	10		$\lvert M\rvert, M, K, IV$	T
	AEAD	GCM	128	128	10		$\lvert M\rvert, M, K, IV, \lvert AD\rvert, AD$	T, C
	PRNG	Fortuna	128	N/A	14		S	R
Keccak	Hash	Sponge	1600	N/A	24	1088	$\lvert M\rvert, M$	H
	MAC	Sponge	1600	128	24	1088	$\lvert M\rvert, M, K, IV$	T
	AEAD	Duplex	1600	128	12	1344	$\lvert M\rvert, M, K, IV, \lvert AD\rvert, AD$	T, C
	PRNG	Duplex	1600	N/A	12	1344	S	R

M–Message, K–Key, AD–Associated Data, S–Seed, IV–Initialization Value, H–Hash, T–Tag,

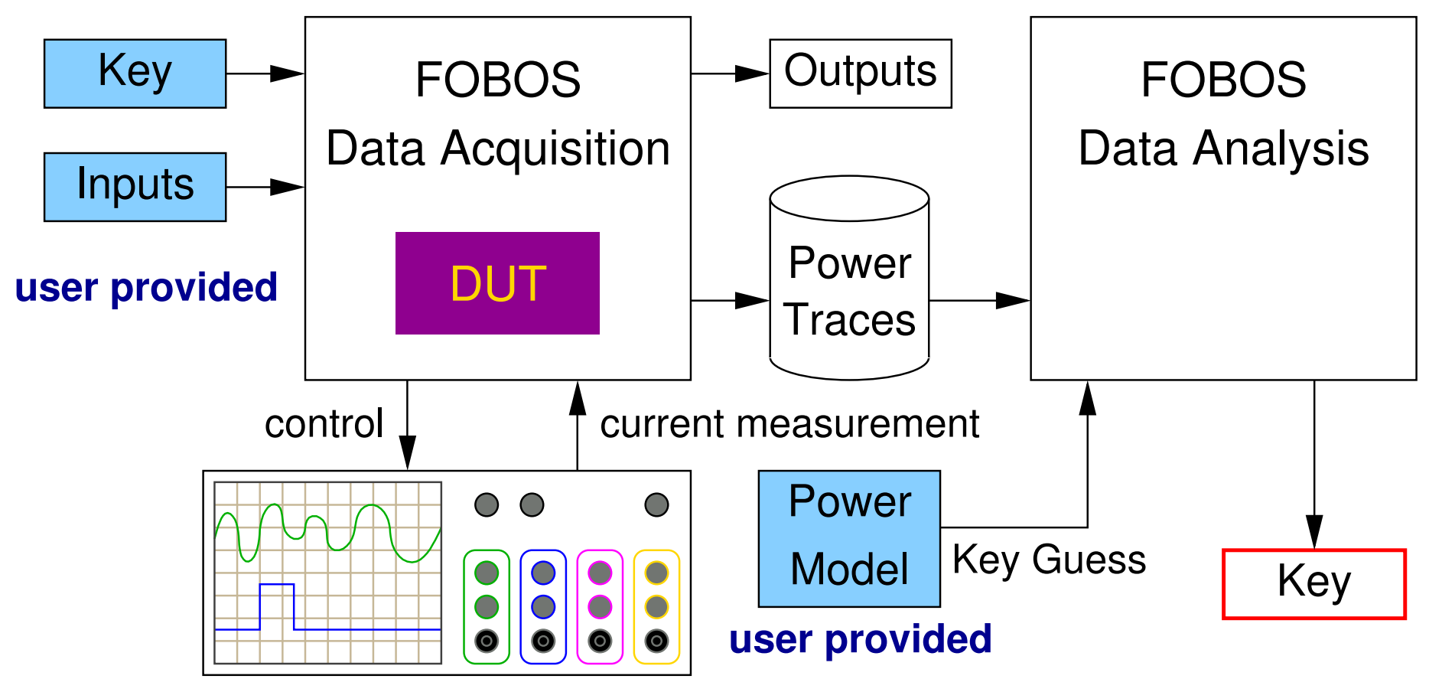
C–Cipher-text, R–Random Number, $|X|$–Length of X

FOBOS

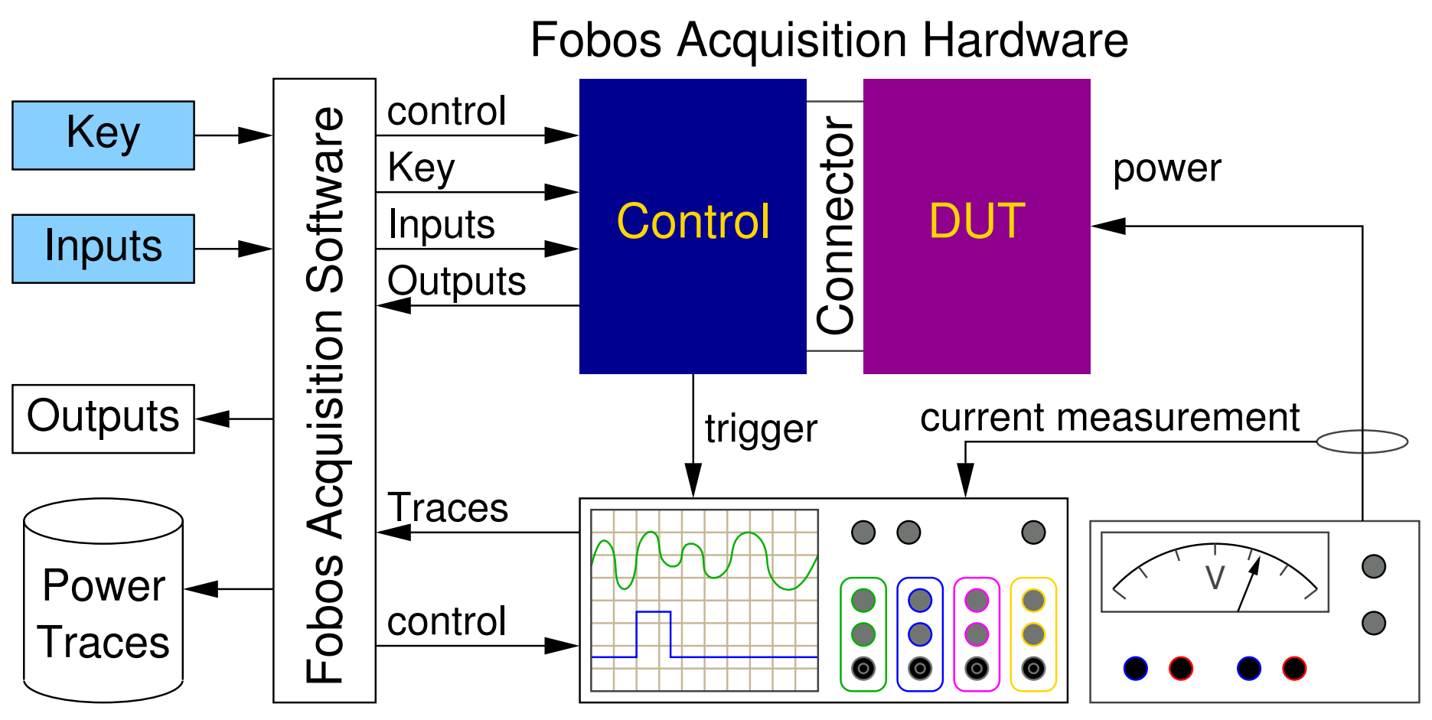
Flexible Open-source workBench fOr Side-channel analysis, loosely named after the Greek god Phobos ($\phi\acute{o}\beta o\varsigma$) is an open-source framework for DPA with the following goals:

- Complete solution useful for education.
- De-couples Control from Device under Test (DUT).
- Allows use of inexpensive FPGA boards.
- Modular software, allows for easy adaptation for new boards, oscilloscopes.
- Extensible by the user to include
  - new attack scenarios and
  - new attack models.

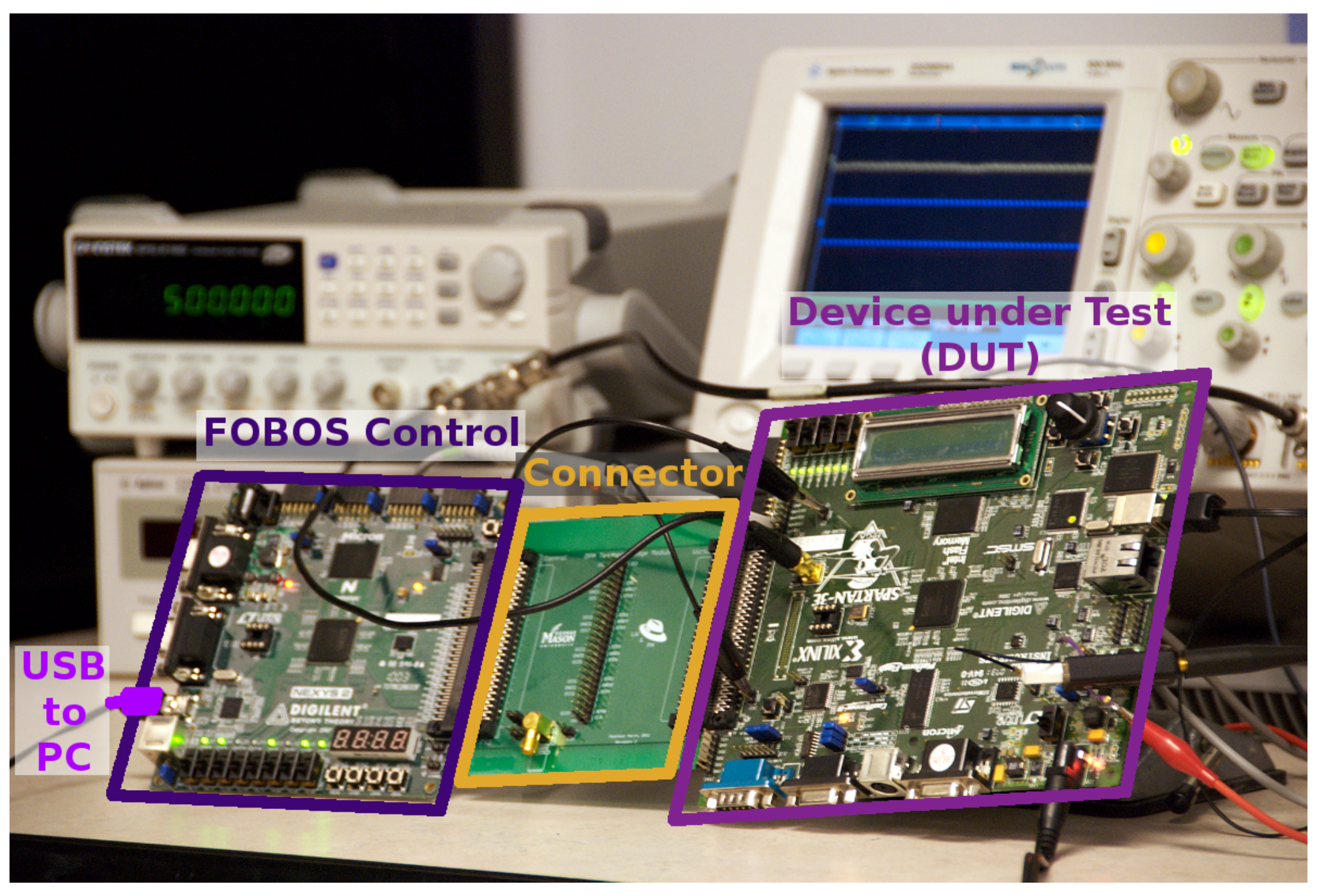
Top Level Diagram



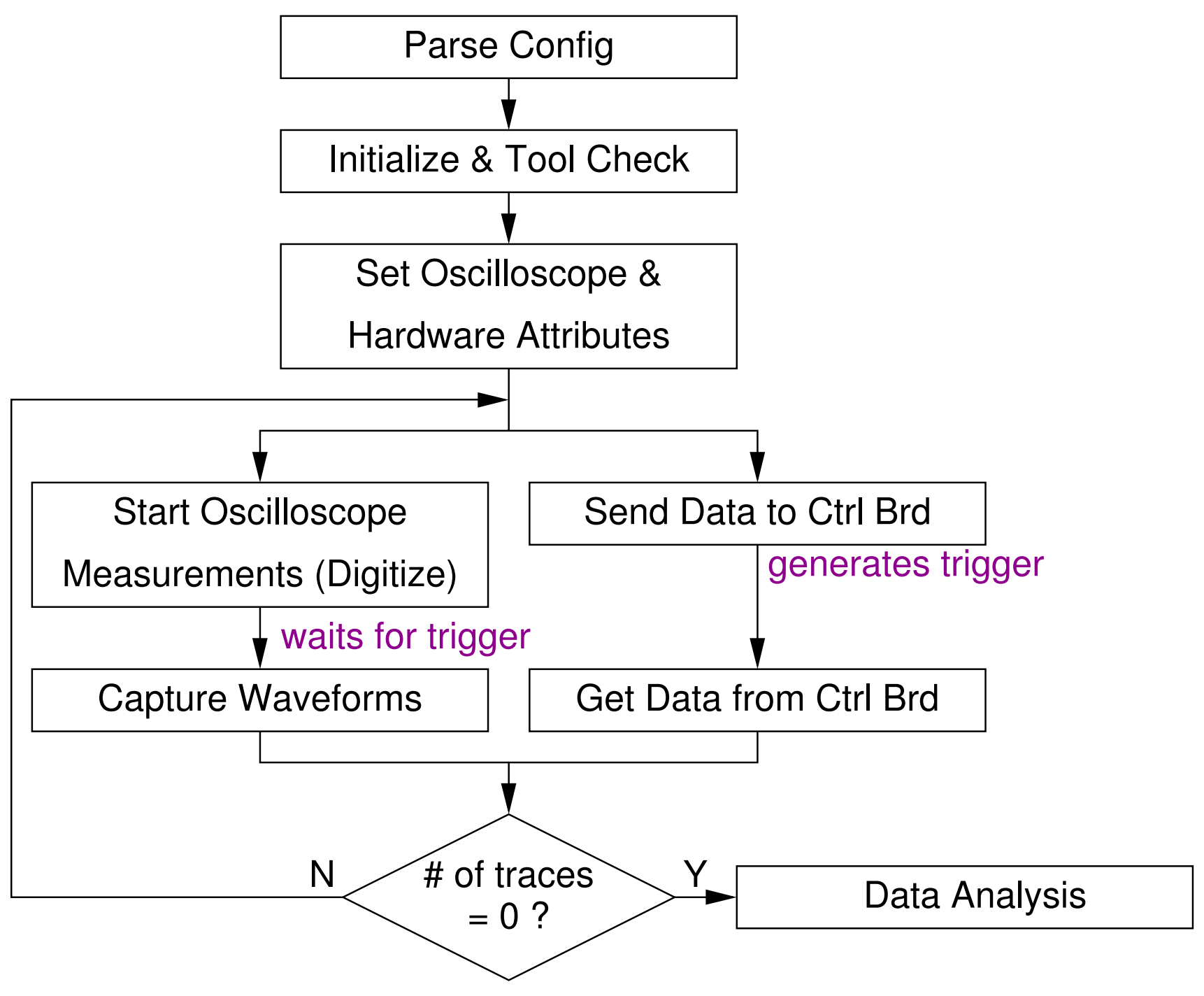
FOBOS Acquisition



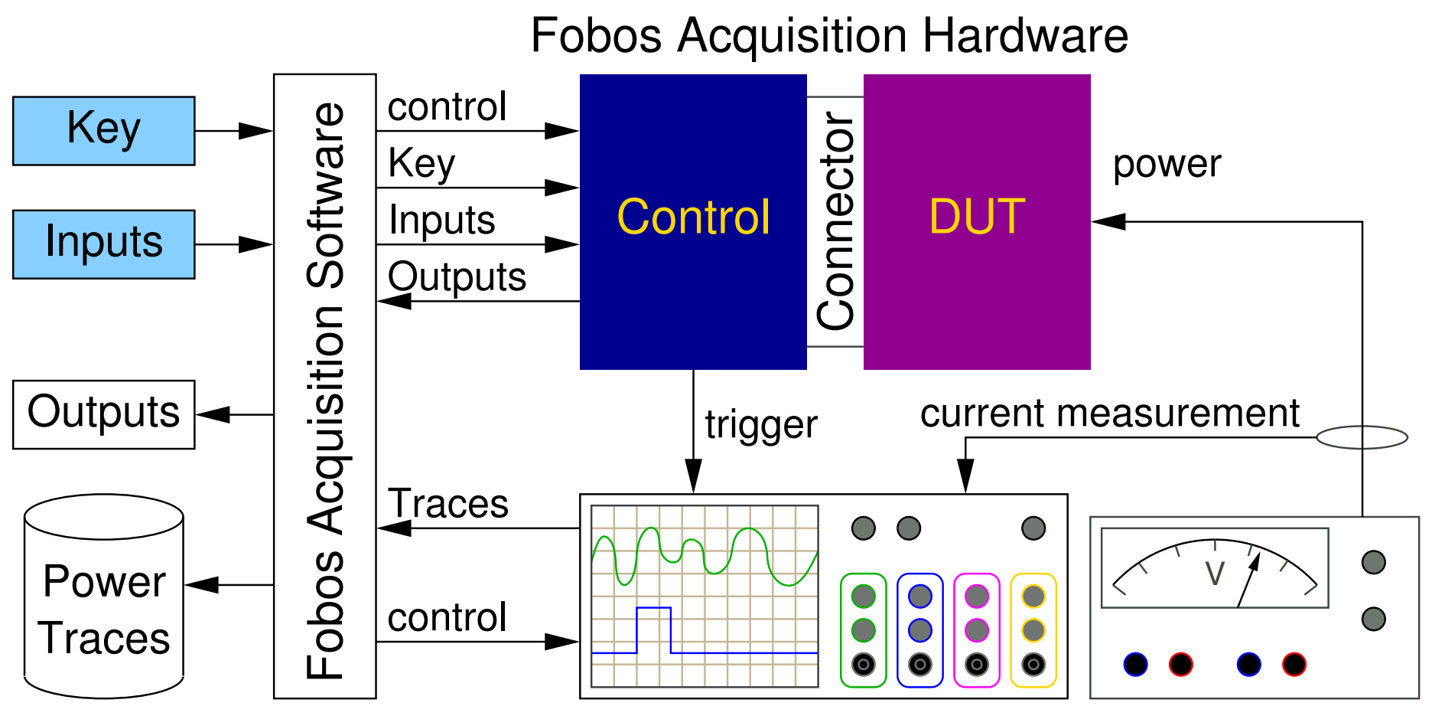
FOBOS Hardware



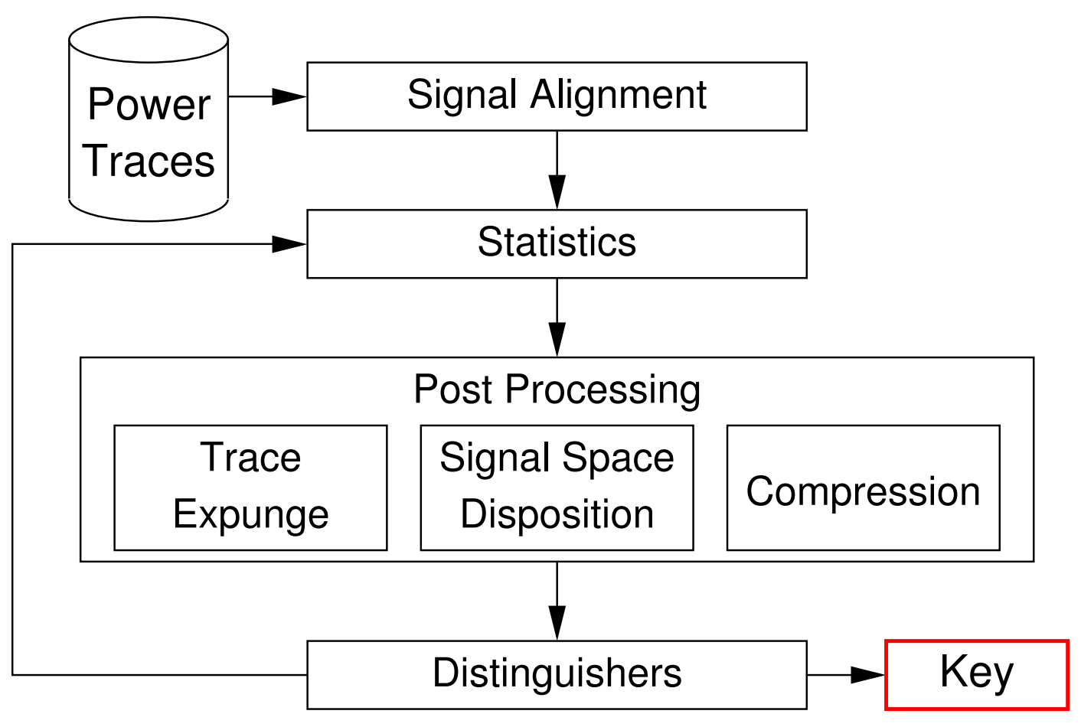
Acquisition Control



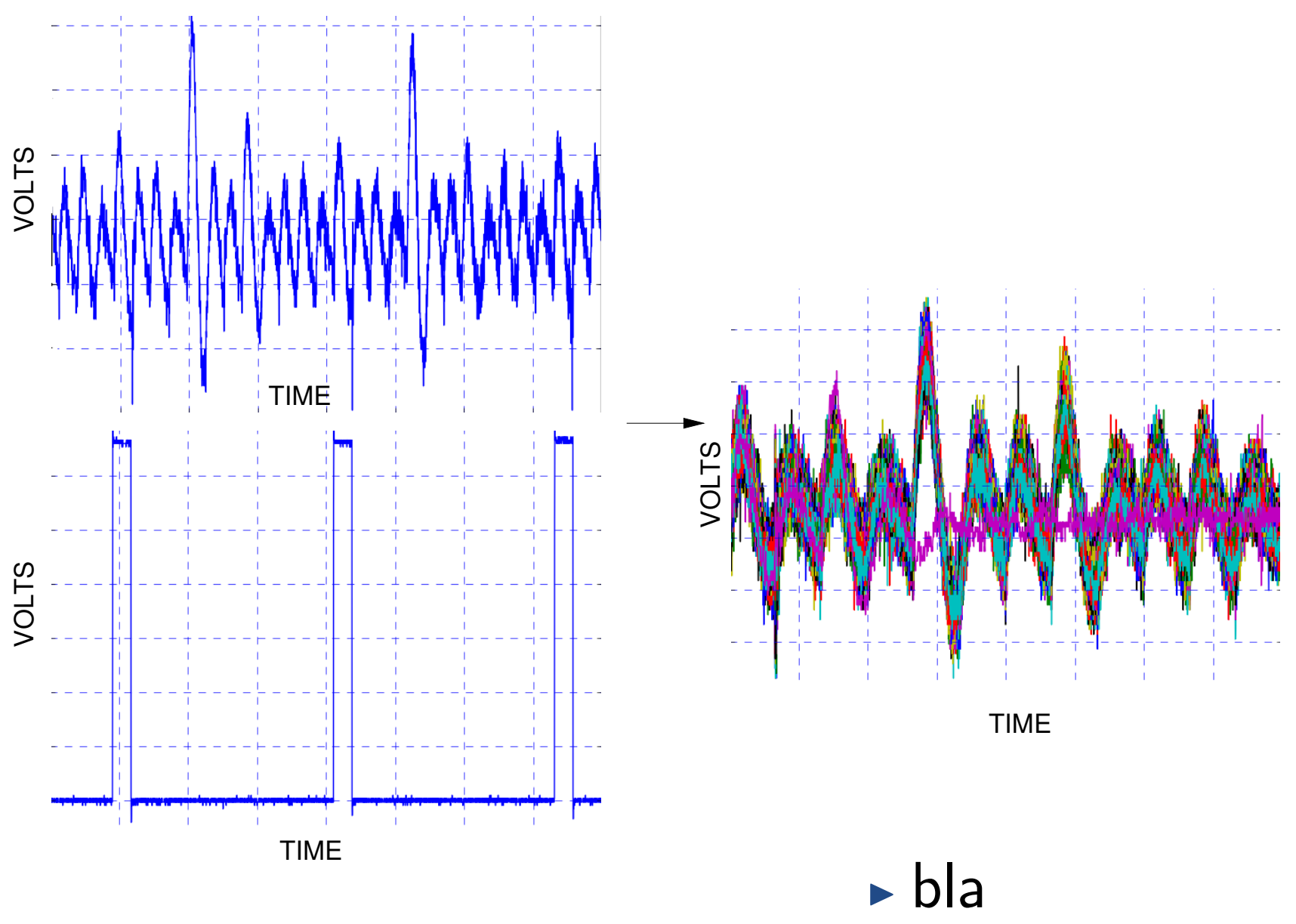
FOBOS Analysis



Analysis Workflow

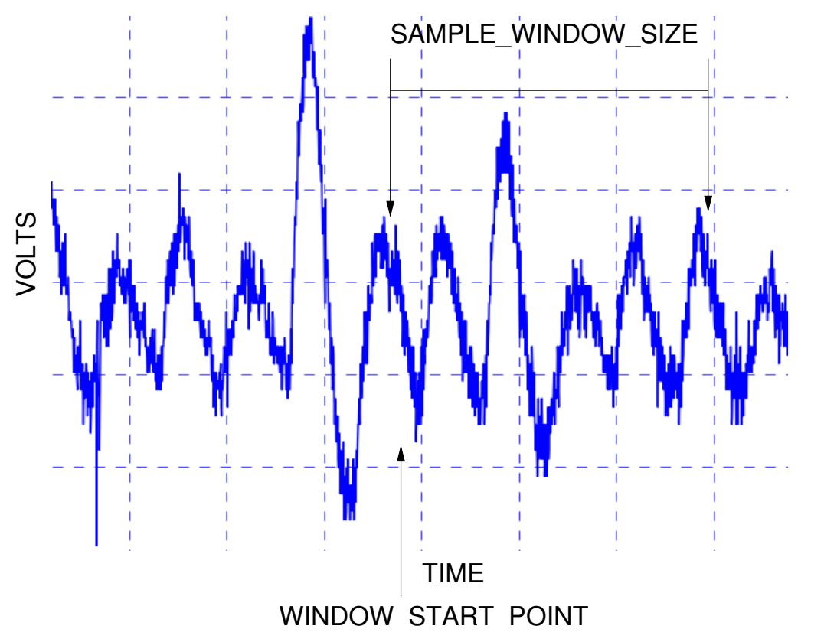


Signal Alignment



- bla
- bla

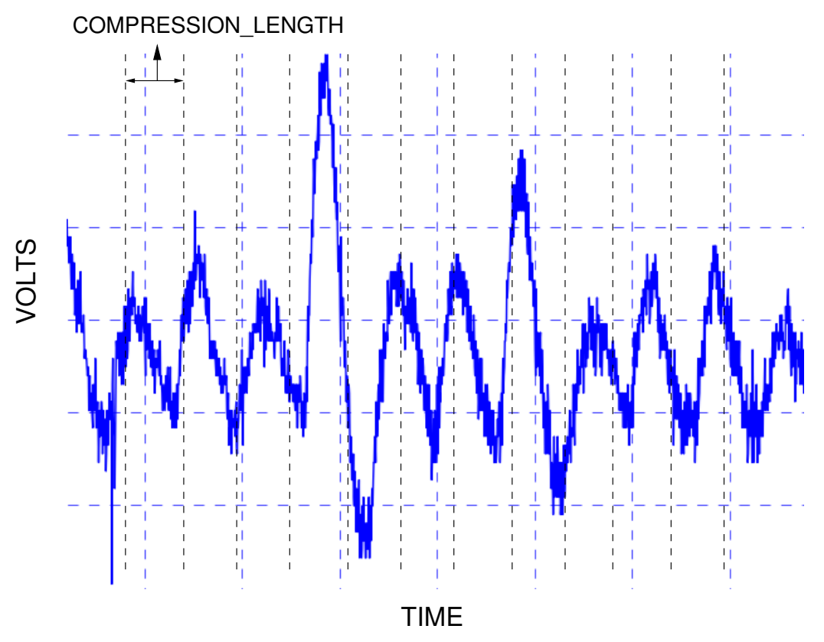
Sample Space Disposition



- User can select any part of the trace for further analysis.
- Reduces computation time.

```
WINDOW_START_POINT = 100
SAMPLE_WINDOW = 1000
```

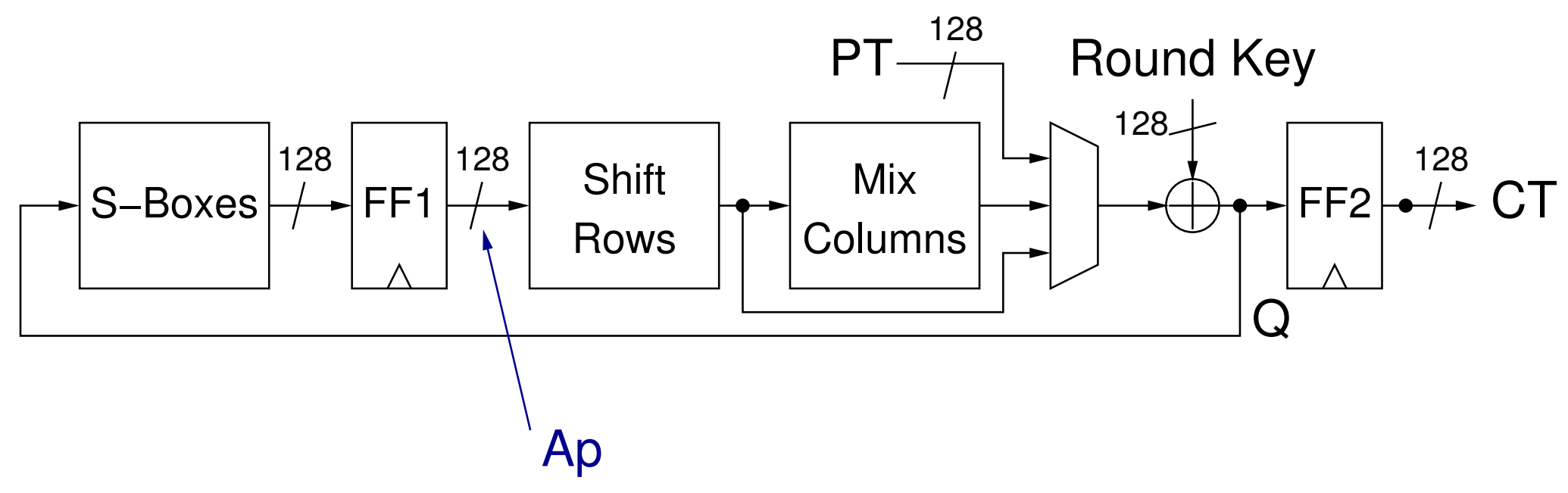
Compression



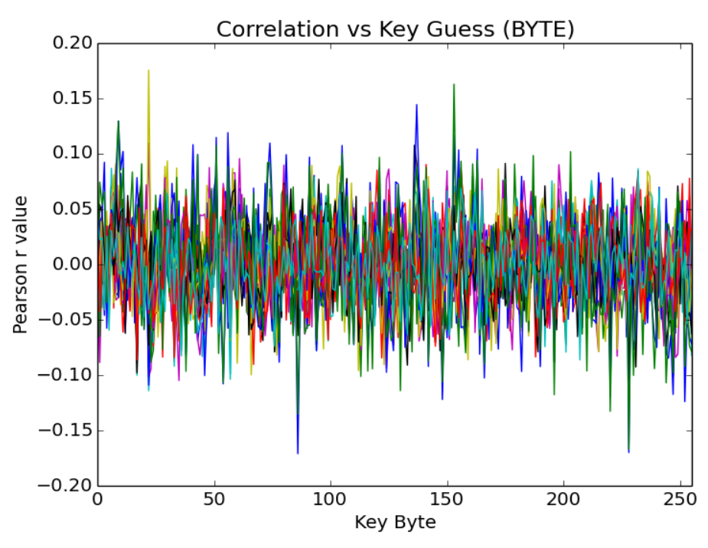
- Compress to MAXimum, MINimum, or MEAN of given sample set.
- Further reduces number of points for correlation.

```
COMPRESSION_LENGTH = 40
COMPRESSION_TYPE = MAX
```

Example: Attack on AES



- bla
- bla


Correlation vs Key Guess (BYTE)
Pearson r value
Key Byte