Increasing Side-Channel Resistance by Netlist Randomization and FPGA-based Reconfiguration

Ali Asghar, Benjamin Hettwer, Emil Karimov, and Daniel Ziener

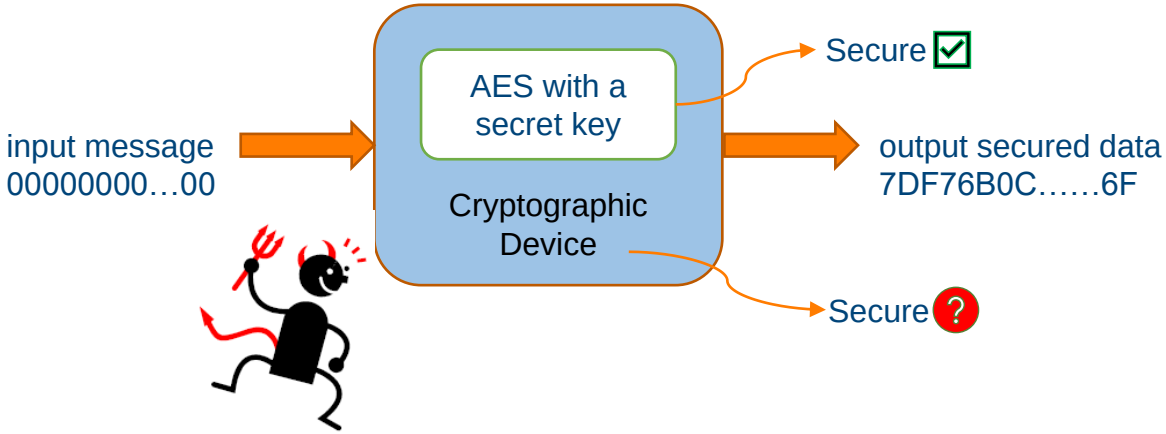
Overview

- Background
- Proposed Approach
- Results
- Conclusion

Background

Encryption

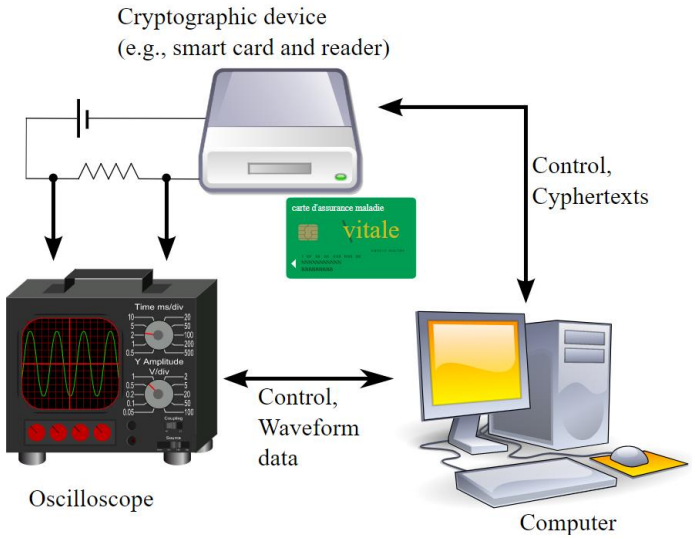
- Modern security systems rely on encryption algorithms
- Encryption algorithms transform a Message (Plaintext) into a Ciphertext using a Key
- AES is one of the most popular encryption algorithms. Computationally secure and efficient realization on hardware/software



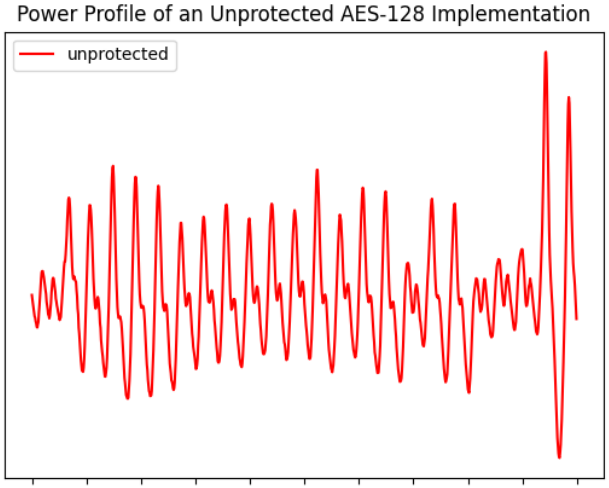
Background

Side Channel Attacks

- Cryptographic devices implementing encryption algorithms can be attacked [Kocher-99]
- Side channels like: timing, power, and EM radiations can leak useful information related to the encryption algorithm



Source: Wikipedia



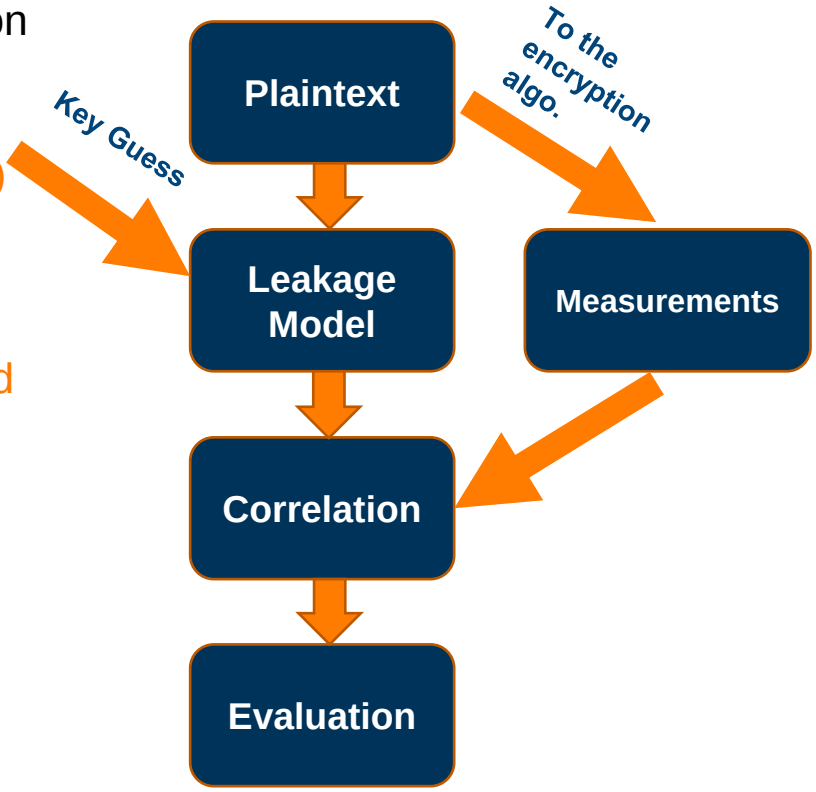
Distincive power profile with low variance and std.deviation

[Kocher-99]P. C. Kocher, J. Jae, B. Jun, M. J. Wiener, “Differential power analysis" Advances in Cryptology-CRYPTO '99 19th Annual International Cryptology Conference, LNCS, vol. 1666, pp. 388-397, 1999.

Background

Side Channel Attacks

- Adversary takes advantage of the correlation between the processed data and some physical observations
  - e.g., Correlation Power Analysis (CPA)
- Create an effective leakage model
  - Generally Hamming Weight (HW) or Hamming Distance (HD) model is used

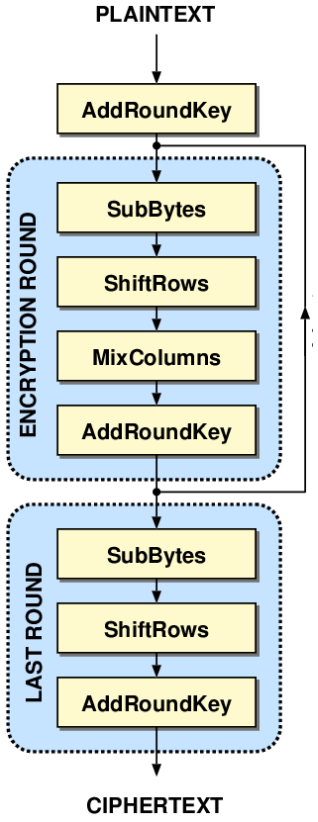


A leakage model is a mathematical function which can establish an effective relation b/w the power consumed and the data being processed by the device

Background

Advanced Encryption Standard (AES)

- Symmetrical
  - *The same key can be used for encryption and decryption*
- Block cipher
  - *Encrypts a block (of fixed size) of plaintext with a secret key in several rounds*
- Variants
  - *Depending upon the key-length (128, 192, or 256 bits), the number of rounds can vary (10,12, or 14)*



Background

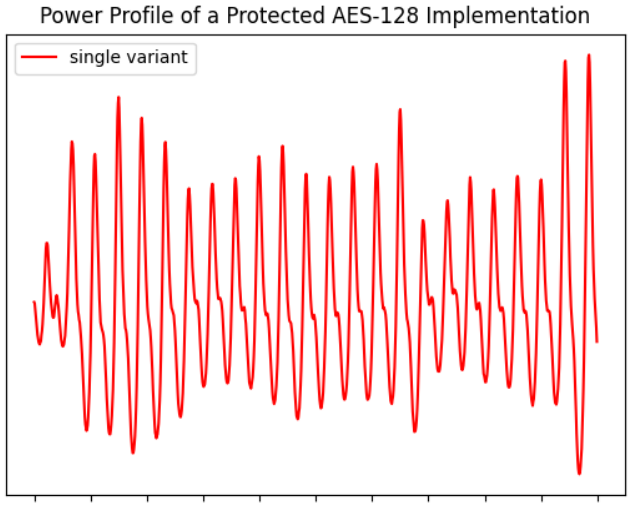
Partial Reconfiguration

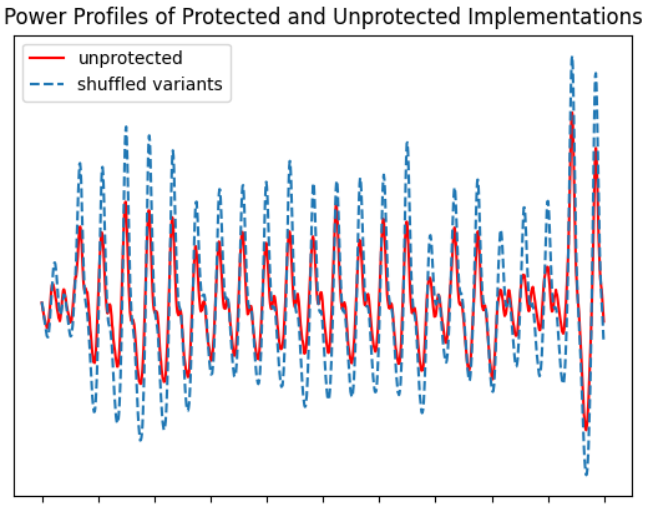
- Allows modifying parts of the design (mapped to PR region) during runtime
- The rest of the logic (mapped to static region) remains unperturbed

Proposed Approach

Concept of Dynamic Circuits

- Side channel attacks such as CPA are favored by the fact that cryptographic hardware implementations are realized as static circuits → can be measured or manipulated
    - *What if we dynamically change the hardware configuration by the means of reconfigurable technology at run time?*
- Create a set of realizations (variants) of the entire (or parts of) cryptographic algorithm which are functionally identical, but structurally different which can then be dynamically shuffled using Partial Reconfiguration
    - *Resulting in varying power profiles*





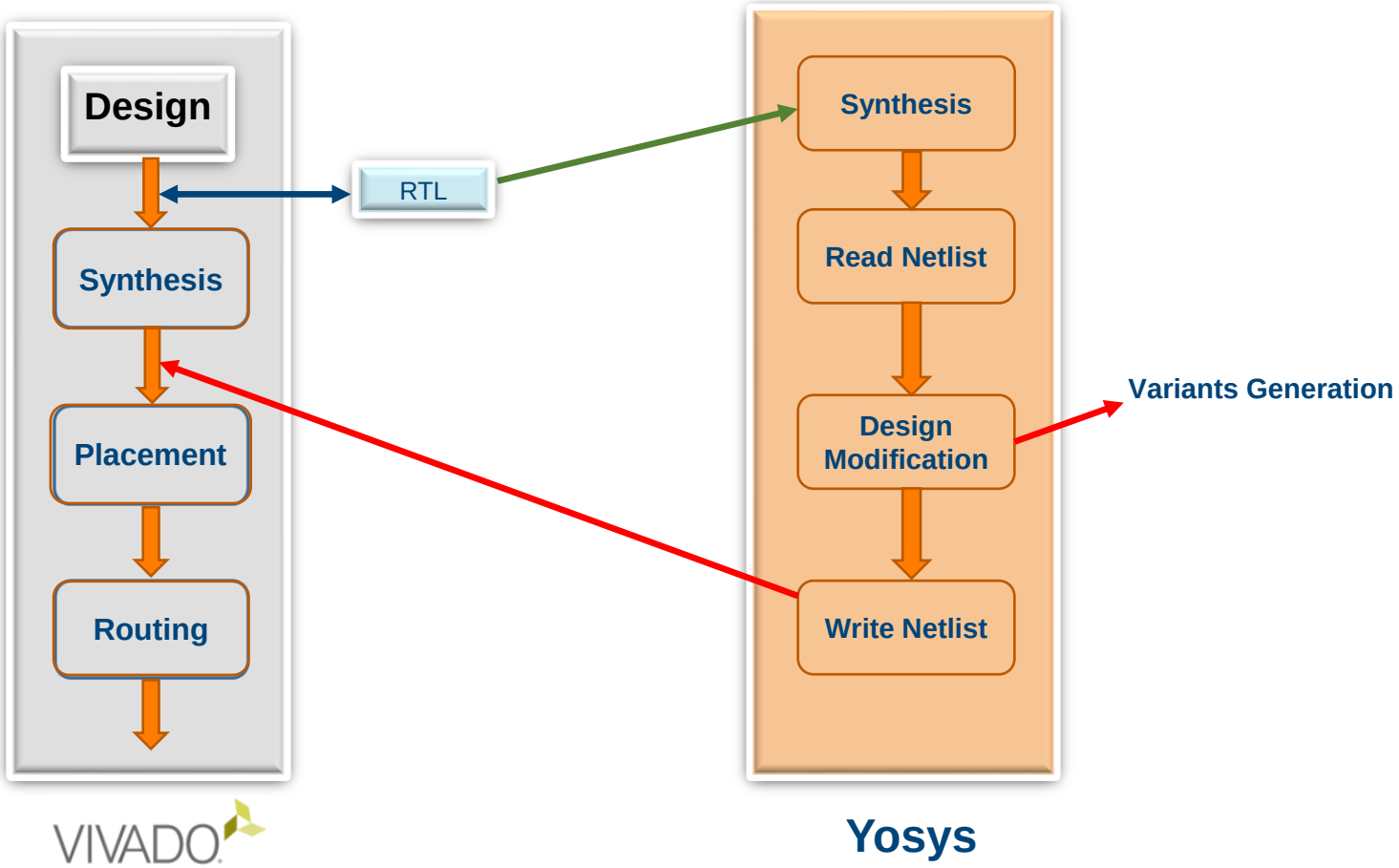
Proposed Approach
Basic Idea

- Manipulate the AES design during the synthesis process
  - *Greater flexibility than during the PnR process* [Bosch]
- Vivado doesn't permit modifications at the netlist level
  - *Bypass the problem by employing third-party, open-source tools in conjunction with Vivado*
- Yosys is an open-source synthesis framework which allows flexible synthesis flow
  - *Modifications and manipulations of the design*
  - *Introducing additional parameters resulting in a multitude of implementation variants of the same circuit*

[Bosch] B. Hettwer, J. Petersen, S. Gehrer, H. Neumann and T. Guneysu, "Securing Cryptographic Circuits by Exploiting Implementation Diversity and Partial Reconfiguration on FPGAs," 2019 Design, Automation & Test in Europe Conference Exhibition (DATE), Florence, Italy, 2019, pp. 260-263.

Proposed Approach

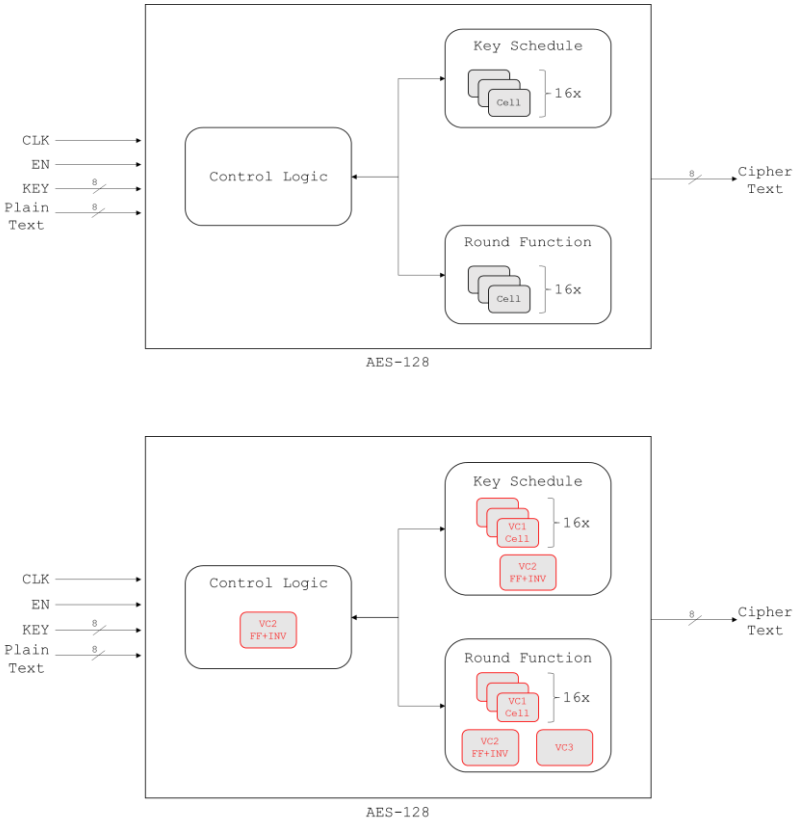
Generation of Variants



Proposed Approach

Generation of Variants

- We use a serialized version of AES
  - The implementation consists of a *Control Logic* module, a *Round Function* module and a *Key Scheduling* module
- Three variant classes are proposed
  - Data Hiding (VC1)
  - Dummy logic generation (VC2)
  - Modified mapping (VC3)

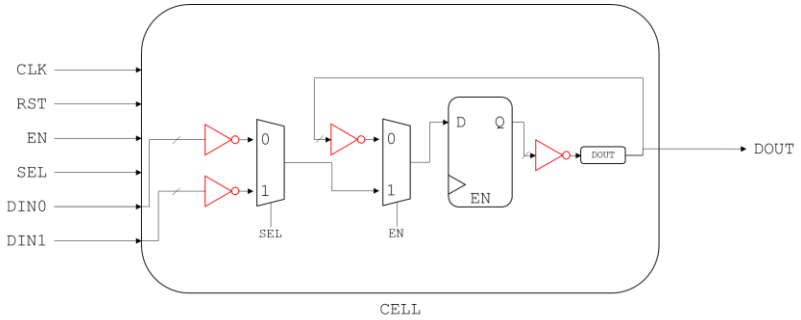


Variant Classes are proposed methods of manipulating the circuit and can be applied to a module or the entire design.

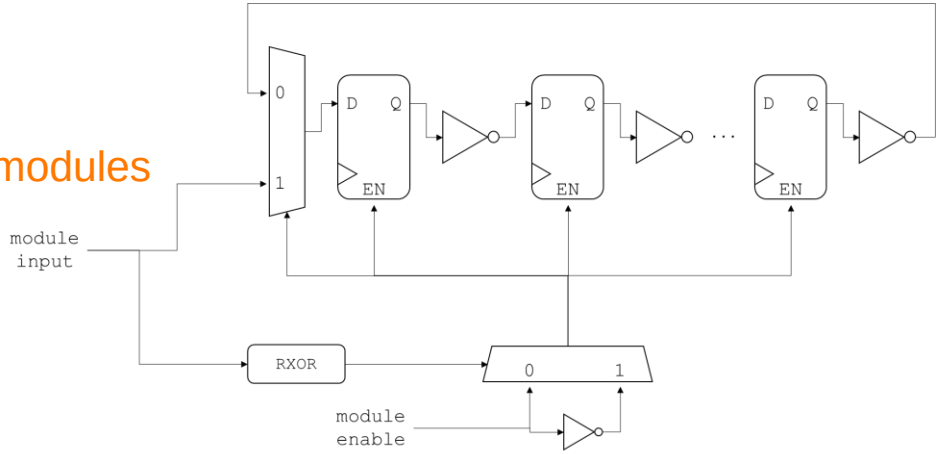
Proposed Approach

Generation of Variants

- Variant Class 1: Data Hiding
  - Applies Boolean transformation to the value stored in the *Cell* sub-module



- Variant Class 2: Dummy Logic
  - Introduces Register-Inverter Chains
  - Can be inserted to any of the three modules



- Variant Class 3: Sub-par Mapping
  - Selected functions of a module are restricted to LUT4 mapping
  - The rest of the design is mapped to LUT6

Results

Measurement Setup

- Hardware: XilinxZYNQ UltraSCALE+
- AES operating frequency: 30MHz
- For each variant, a total of 10,000 traces were recorded with an averaging factor of 250
- To emulate the effect of dynamic reconfiguration of circuits using PR, we combine and shuffle the traces of proposed variants

Results

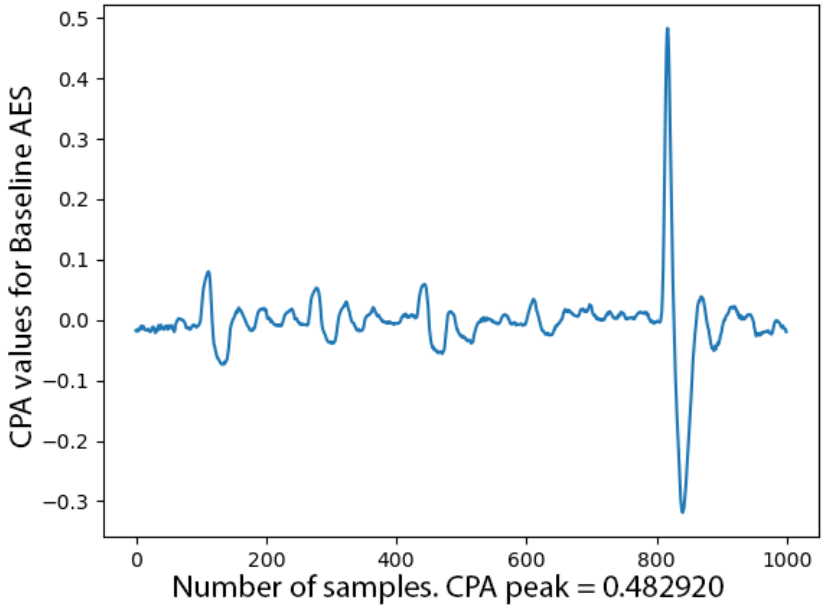
Experimentation Details

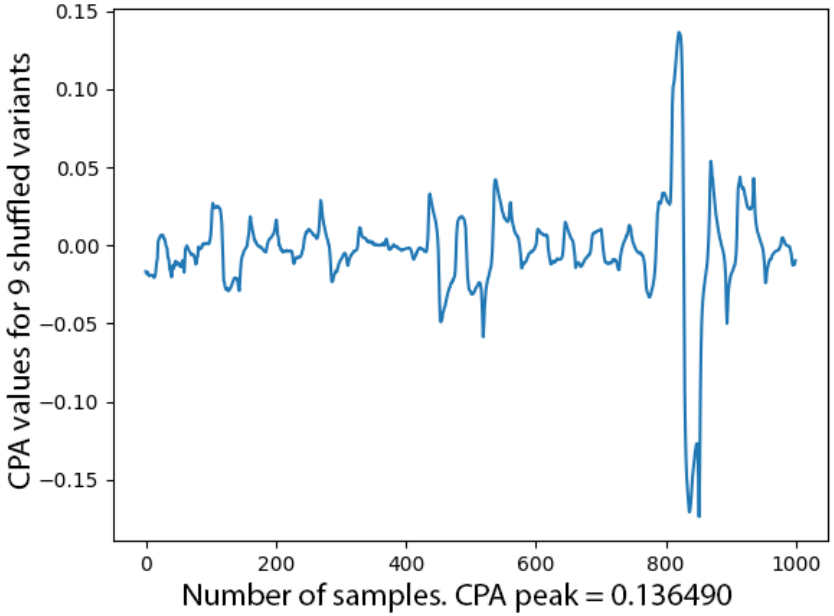
- Attack: Correlation Power Analysis
- Leakage Model: Hamming Distance between two consecutive S-box outputs in first round
- CPA value of each (measured) variant indicates the relative level of security
- A protected implementation is created by shuffling the traces of 9 different versions from the three variant classes

The shuffling is expected to mimic the behavior of actual PR

Results

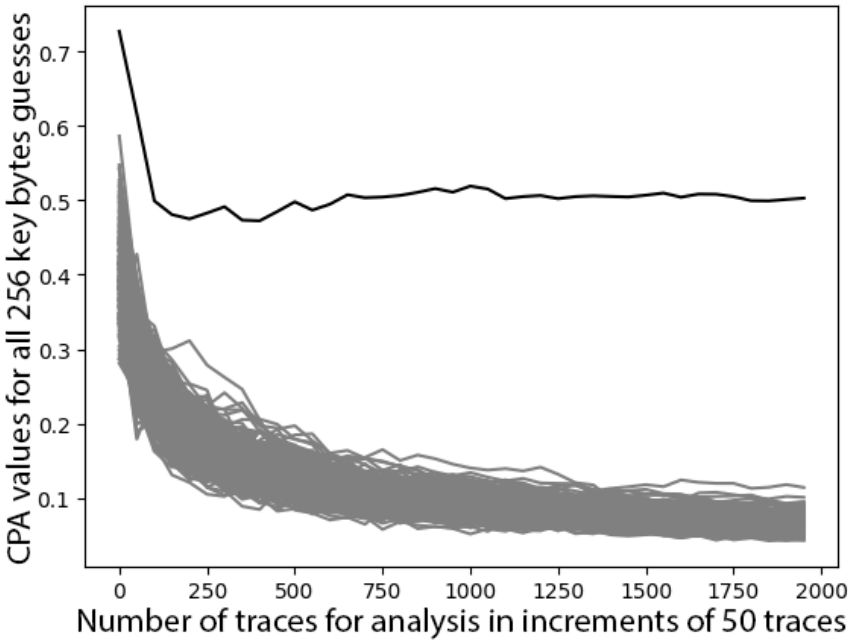
CPA for Reference AES Design

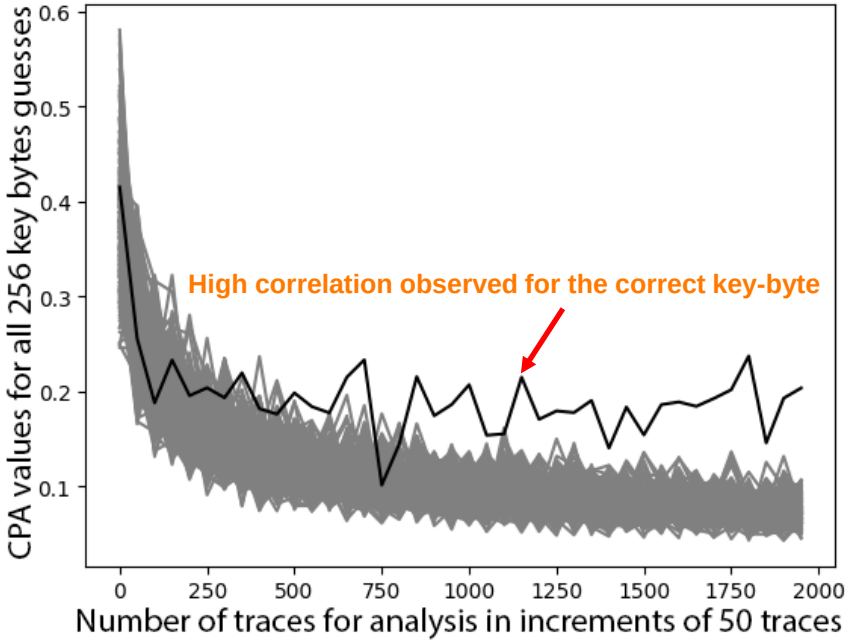




Results

Maximum Absolute Correlation over number of traces





Conclusion

- Resistance against CPA attacks improved by ~12.6x with the PR based shuffling countermeasure
- The proposed approach is also expected to make fault attacks harder
- High resource overhead
- Throughput penalty due to reconfiguration time

Conclusion

- Resistance against CPA attacks improved by ~12.6x with the PR based shuffling countermeasure
  - Absolute trace count still too low
  - Can be easily combined with countermeasures on algorithmic level (e.g. masking)