A Countermeasure For Differential Power Analysis Attack

Mehri Yahyaei

Direct Manager of IT Laboratories, Research Centre of Informatics Industries
(RCII. Co)

Research Center of Informatics Industries (RCII)

RCII was established in 1991

- Research in new domestic and global achievements and technologies in the area of ICT;
- Conducting strategic studies in the area of ICT;
- Research and development of laboratories in areas of CA and PKE;
- Research on security and quality of software's and establishing appropriate laboratories;
- Research on and development of open system software;
- Preparing a security assessor and a security provider;
- Sampling from all imported goods;
- Inspection and sampling of domestic and exporting industrial and consuming electrical, electronic and clinical equipment;

RCII

Laboratory Of Cryptography (RCII)

Outline of the Talk

❑ What is Side Channel Attacks(SCA)?

❑ Power Based Side Channel Analysis

❑ Electromagnetic Side-Channel Analysis

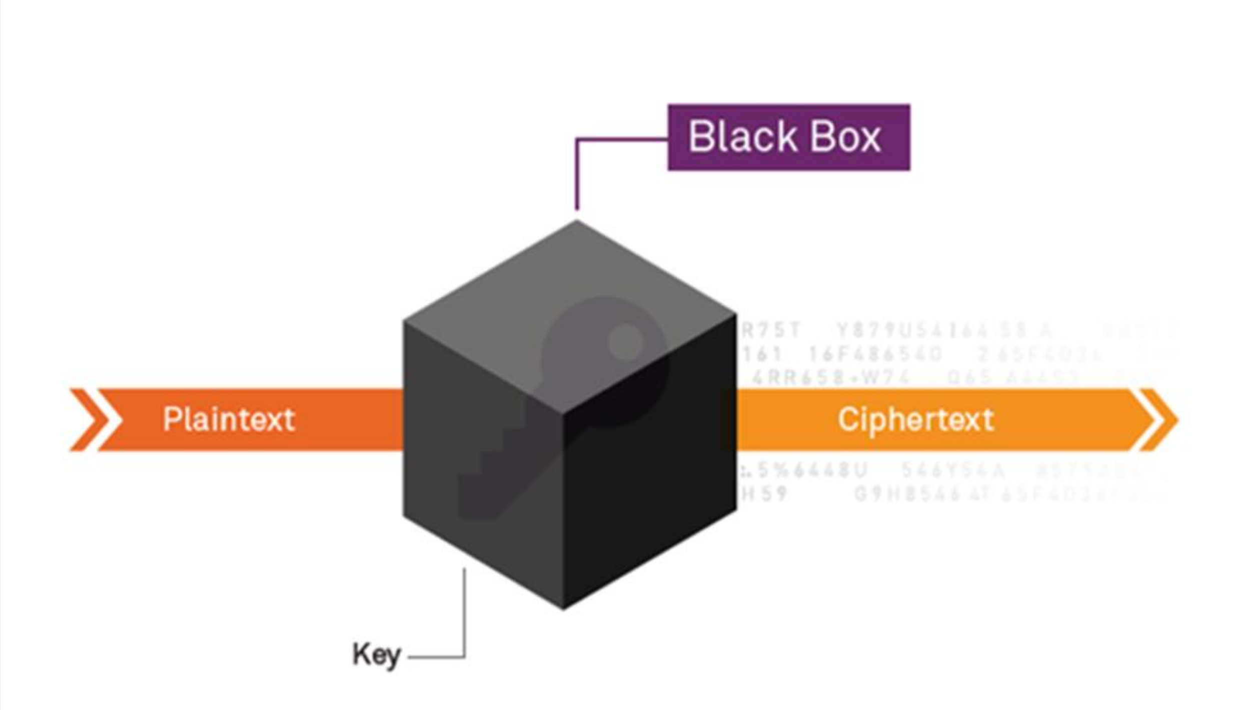
❑ Timing Attacks

❑ Attacks and Countermeasures

❑ Experimental And Simulation Results

What is Side-Channel Attacks

It is typically assumed that the implementations of cryptography computations are ideal “black-boxes” whose internals can neither be observed nor interfered with by any malicious entity.

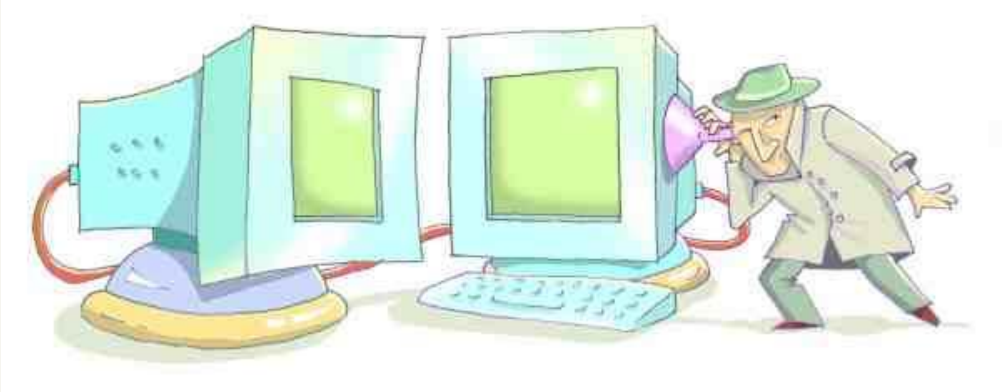


What is Side-Channel Attacks

A side-channel attack is any attack based on information gained from the physical implementation of a system (process), rather than theoretical weaknesses in the algorithms.

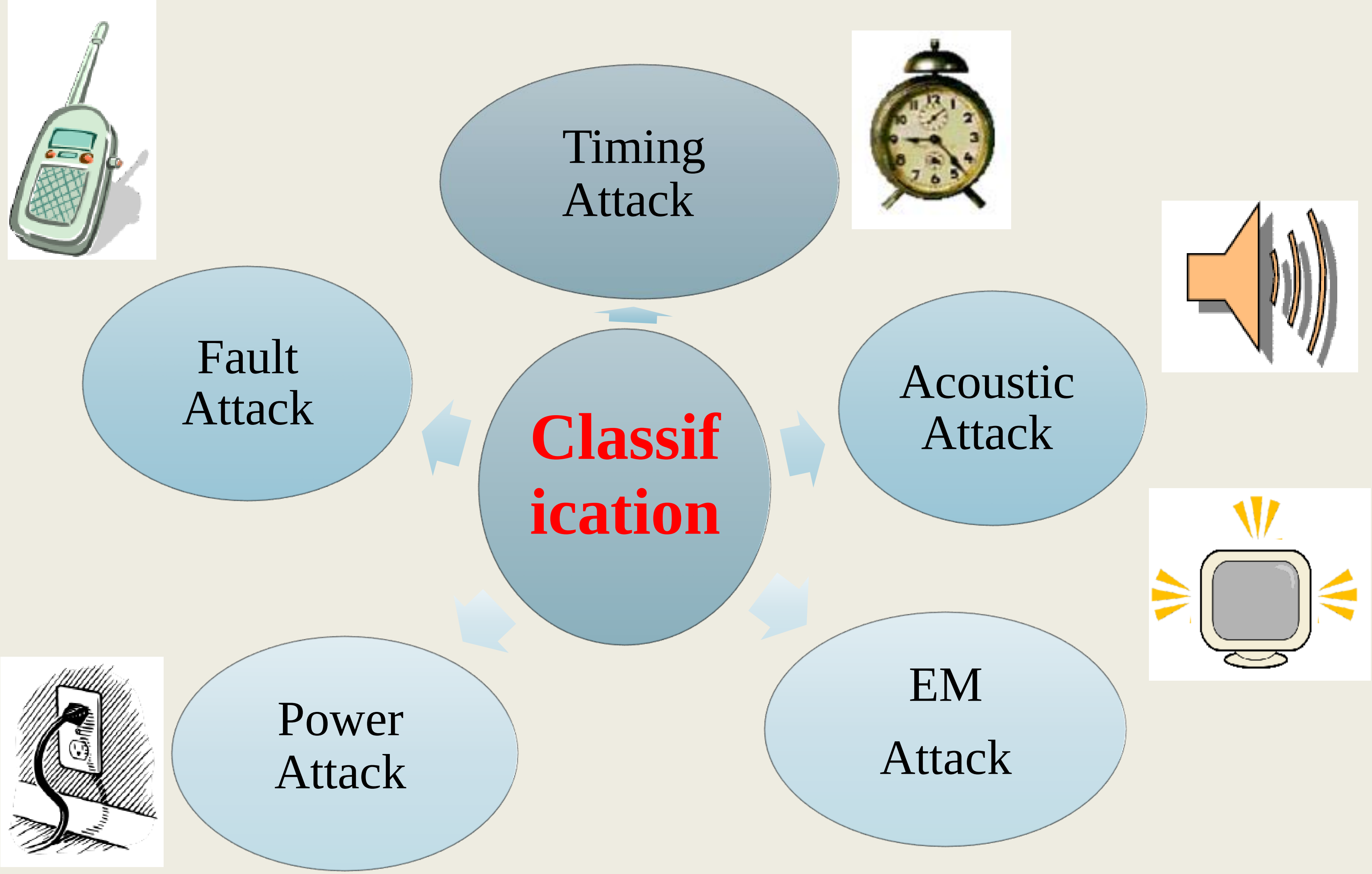
What is Side-Channel Attacks

- A side-channel attack is based on information gained from the implementation of system. Attack vectors can be timing information, power consumption, an acoustic source, optical source, electromagnetic leaks etc.



- It is the correlation between the side channel information and the operation related to the secret key that the SCA attack tries to find.

Side-Channel Classification



Classification

Timing Attack

Acoustic Attack

EM Attack

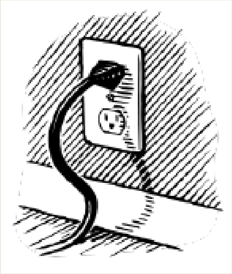
Power Attack

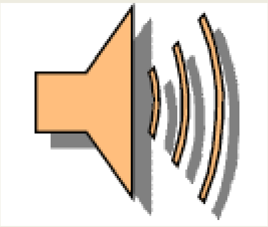
Fault Attack

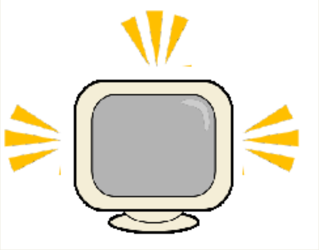
Side-Channel Classification

❑ Information can be extracted from timing, power consumption or electromagnetic radiation

- ***Timing Attack***
- ***Fault Attack***
- ***Power Analysis Attack***
- ***Electro-Magnetic radiations***
- ***Acoustic Attack***
- ***Visible Light Attack***







Timing Attack

- Implementations of cryptography algorithms often perform computations in non-constant time, due to performance optimizations.
- If such operations involve secret parameters, these timing variations can lead to the leak of some information.
- attacker attempts to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms
- Measure the time it takes for a certain unit to perform an operation.
- Keep the input, output, and consumed time.
- Check the correlation between time measurements of guess key or input and empirical result (often statistically).

Fault Attack

- Fault attack on cryptography modules or devices requires:

Fault injection: which is injecting a fault at the appropriate time during the process.

- The injection happens by acting on device's environment and putting it in abnormal conditions. *Such as abruptly low or high voltage, clock, temperature, radiations, light, and so on*

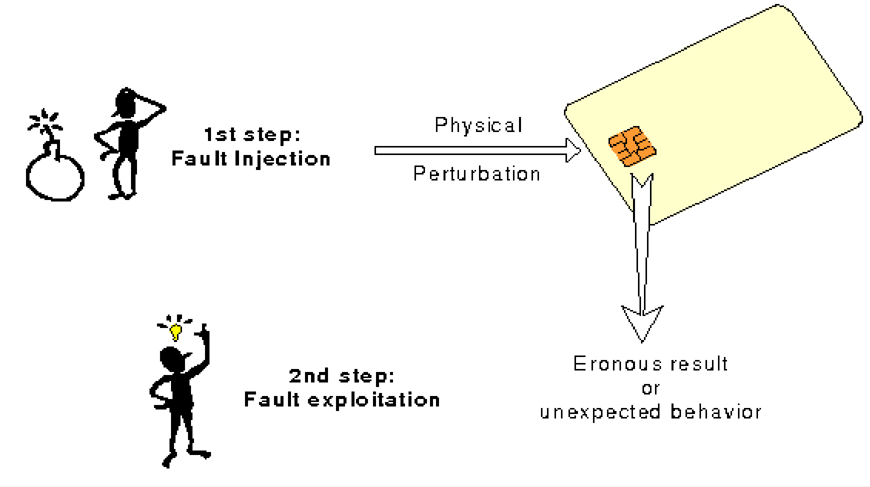
Faults may be induced:

Heat

Cold

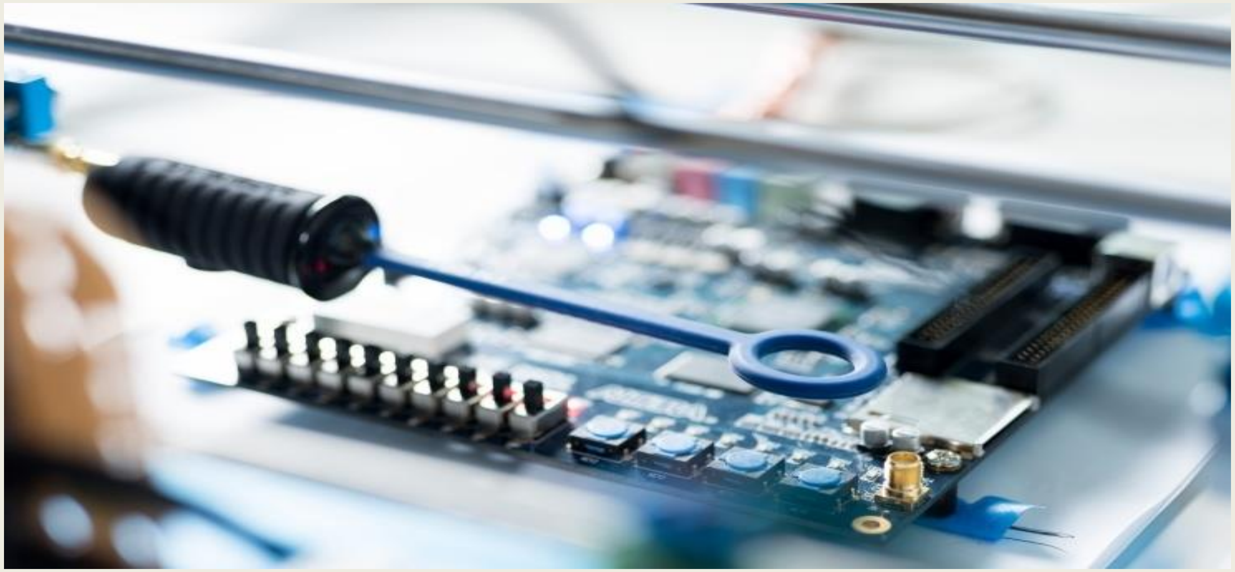
Low power

Microwaves



Electro-Magnetic Attack

- As electrical devices, the components of a computer often generate electromagnetic radiation as part of their operation.
- An attacker that can observe these emanations and can understand their causal relationship to the underlying computation and data may be able to infer a surprising amount of information about this computation and data.



Power Analysis Attack

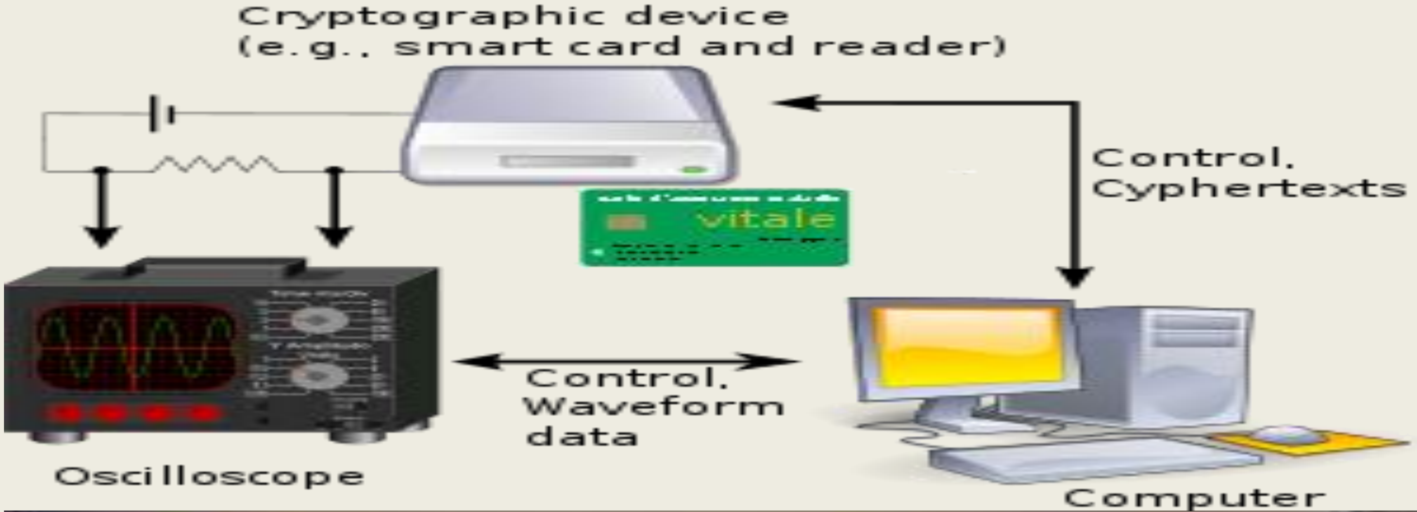
- The power consumption of a cryptography device may provide much information about the operations that take place and the involved parameters.
- Power analysis attack can be divided into simple(SPA) and differential power analysis (DPA).
- In SPA attacks, the aim is essentially to guess from the power trace which particular instruction is being executed at a certain time and what values the input and output have.
- Therefore, the attacker needs an exact knowledge of the implementation to mount such an attack.
- DPA attack does not need the knowledge of the implementation details and alternatively exploiting statistical methods in the analysis process.

Power Analysis Attack

A power analysis attack can be essentially decomposed into the following three steps:

- ❑ Identify a relationship between secret key information and instantaneous power consumption. Also need to determine the required inputs to the system, the output values to be measured, and when to capture them.
- ❑ Extract the state by measuring and recording the items identified earlier including the power consumption. The collection of measurements also known as the traces can be made in a noninvasive manner while a system performs a cryptography operation.
- ❑ Evaluate the relationship between the measured items by processing the extracted information.

Power Analysis Attack



Side-channel Attacks Countermeasures

Countermeasures have been classified into two main categories:

(1) eliminate or reduce the rate of release of such information

(2) eliminate the relationship between the leaked information and the secret data

Countermeasures could be applied on three different levels:

1. **Software(Algorithmic)**
2. **Hardware**
3. **Software-hardware-interactions**

Side-Channel Attacks Countermeasures

Dedicated software (Algorithmic) implementations

In this method, the aim of the attempts is to confront the attacks through making the algorithm more resister.

One of the most powerful software techniques to counteract such attacks is to **mask all input and intermediate data** in order to de-correlate any information leaked through side channels from actual secret data being processed.

Side-channel Attacks Countermeasures

Dedicated hardware implementations:

Implementing an algorithm in hardware such that it offers protection against side channel attacks raises even more concerns.

- ***System-level countermeasures***
- ***Gate-level countermeasures***
- ***Transistor level countermeasures***

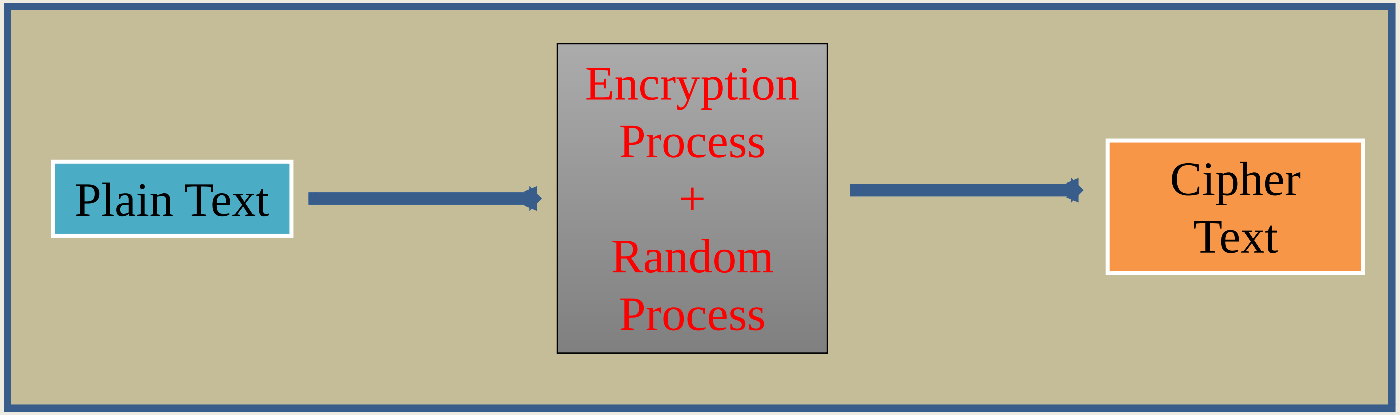
Description Of Purpose

Ongoing research on a masking countermeasure for the side channel attack is taking place. In which the goal is to modify the hardware implementation of the algorithm such that the breaking point in terms of power leakage is masked using a variety of randomized operations in that interval. Although there are arguments concerning the results of testing masking approaches.

The experiment set consists of three different AES encryption hardware modules and an oscilloscope.

We developed AES in microcontroller. Randomized algorithms mentioned are programmed onto this configuration on top of the encryption algorithm. For example, in AES, these perturbing algorithms are added during the final round which most DPA attacks occur in.

Experimental And Simulation Results



Plain Text

Encryption Process + Random Process

Cipher Text

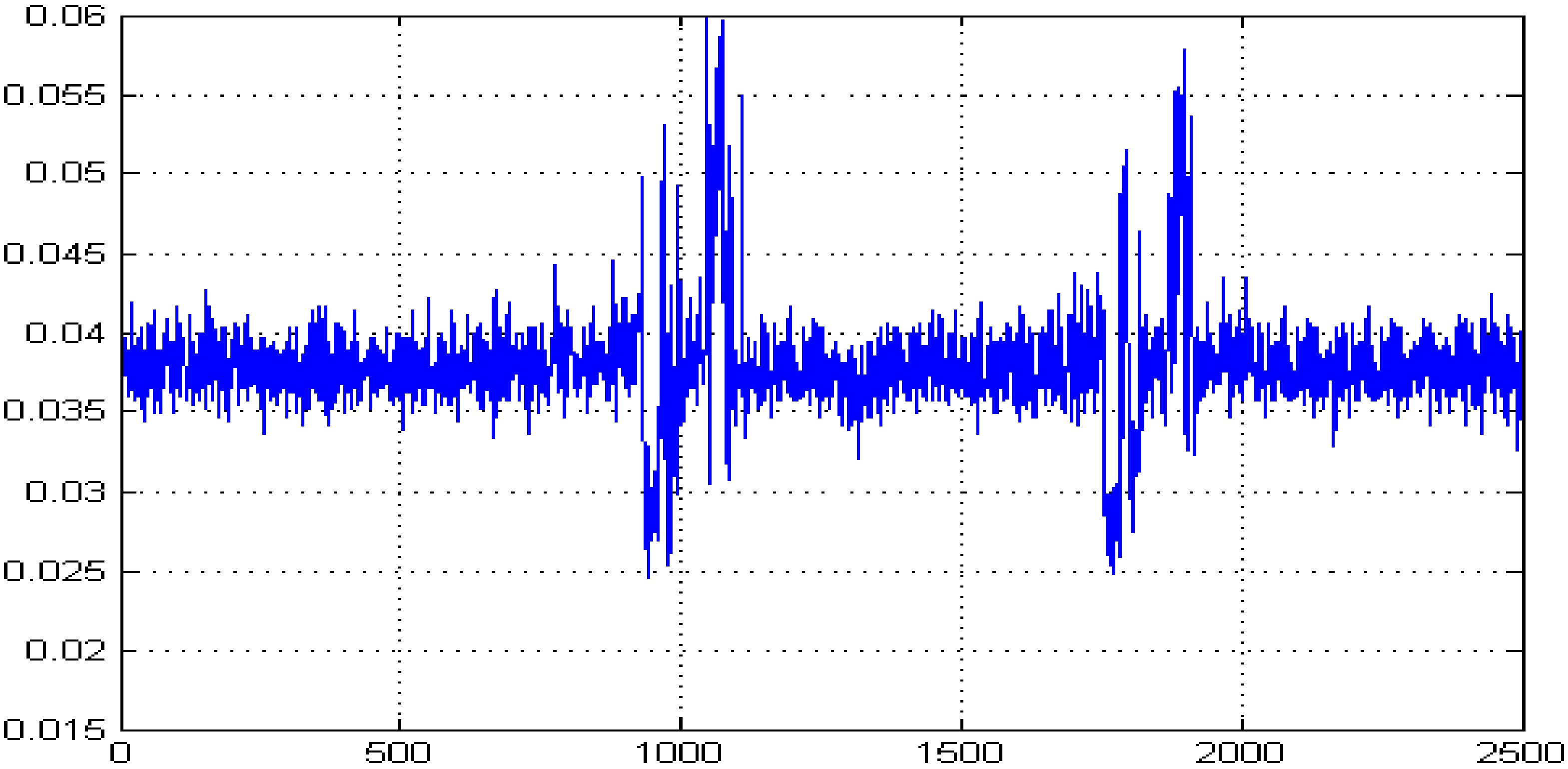
Experimental And Simulation Results

- ❑ A RAM module of the FPGA platform can be utilized for this purpose.
- ❑ Then, a tiny micro-machine addresses this memory in the scheduled order.
- ❑ The exchange of processing unit types may be applied at various places.
- ❑ Random Concurrent Binding In this approach the number of units running in parallel varies as well as the binding of an operation to a specific unit.
- ❑ Therefore, several random combinations of unit types as provided by the method purpose featuring different degrees of parallelism and bindings may thus be generated.

Experimental And Simulation Results

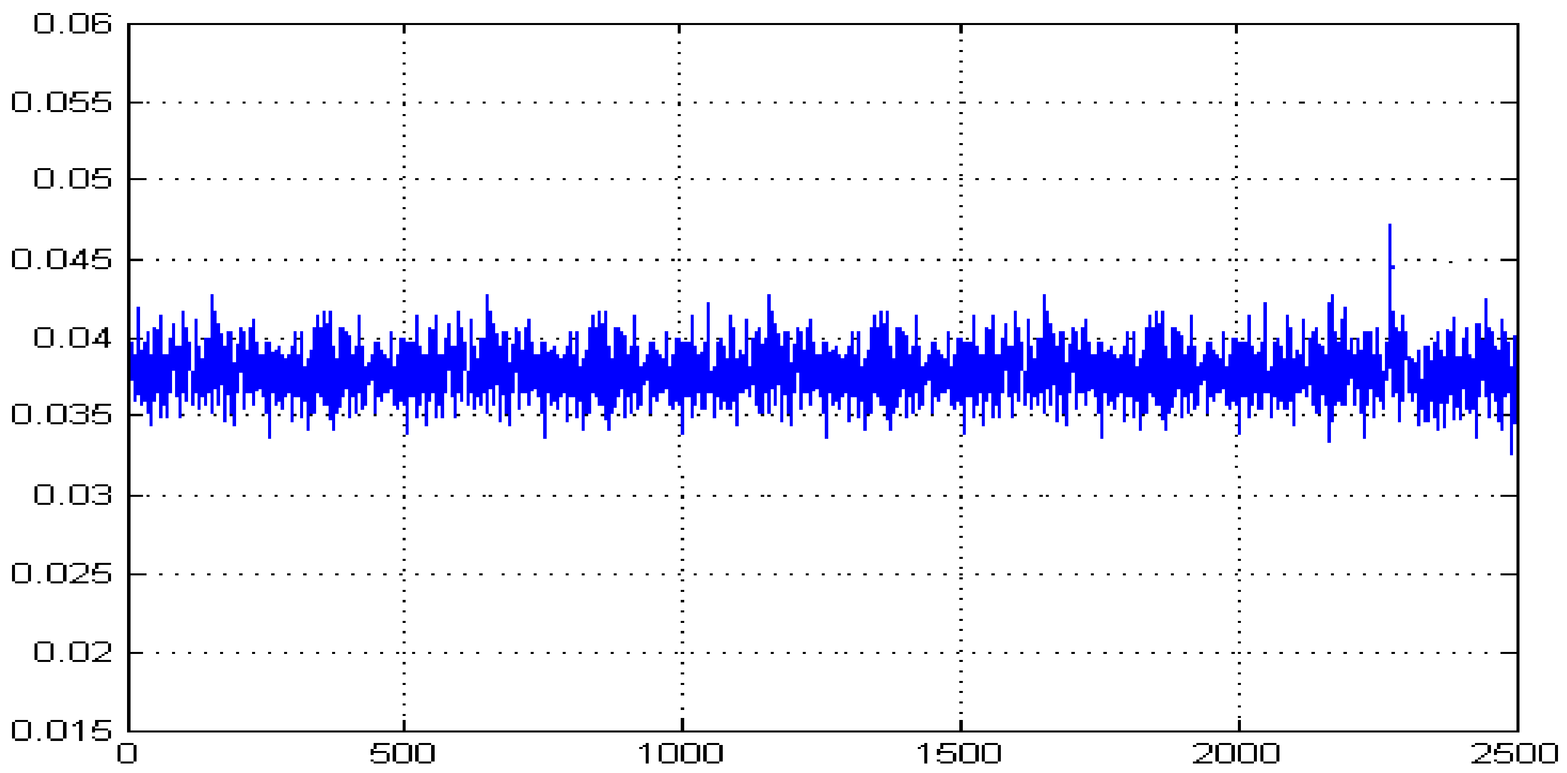
- ❑ The provided method is a kind of investigating method and computational plan (idea) in which a virtual operation will be started as a trick, while the parallel cryptography algorithm is operating in the core of the processor, the place in which cryptography (cipher) is in operation.
- ❑ For each cryptographic algorithm, Weaknesses are identified and at the same time as the algorithm is executed, our method which is a type of virtual operation, is executed at exactly the same weak point.

Experimental And Simulation Results



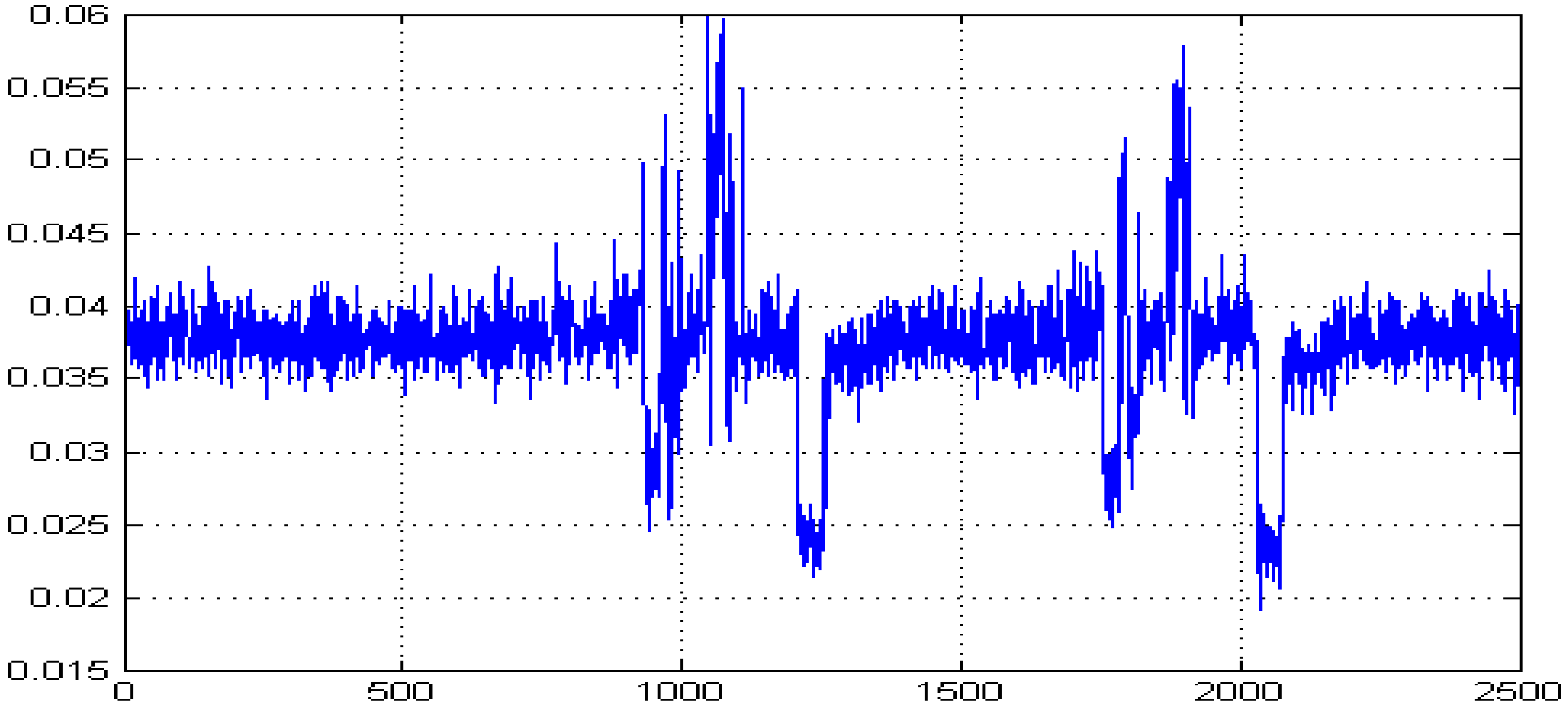
Example power trace of AES execution for one cycle

Experimental And Simulation Results



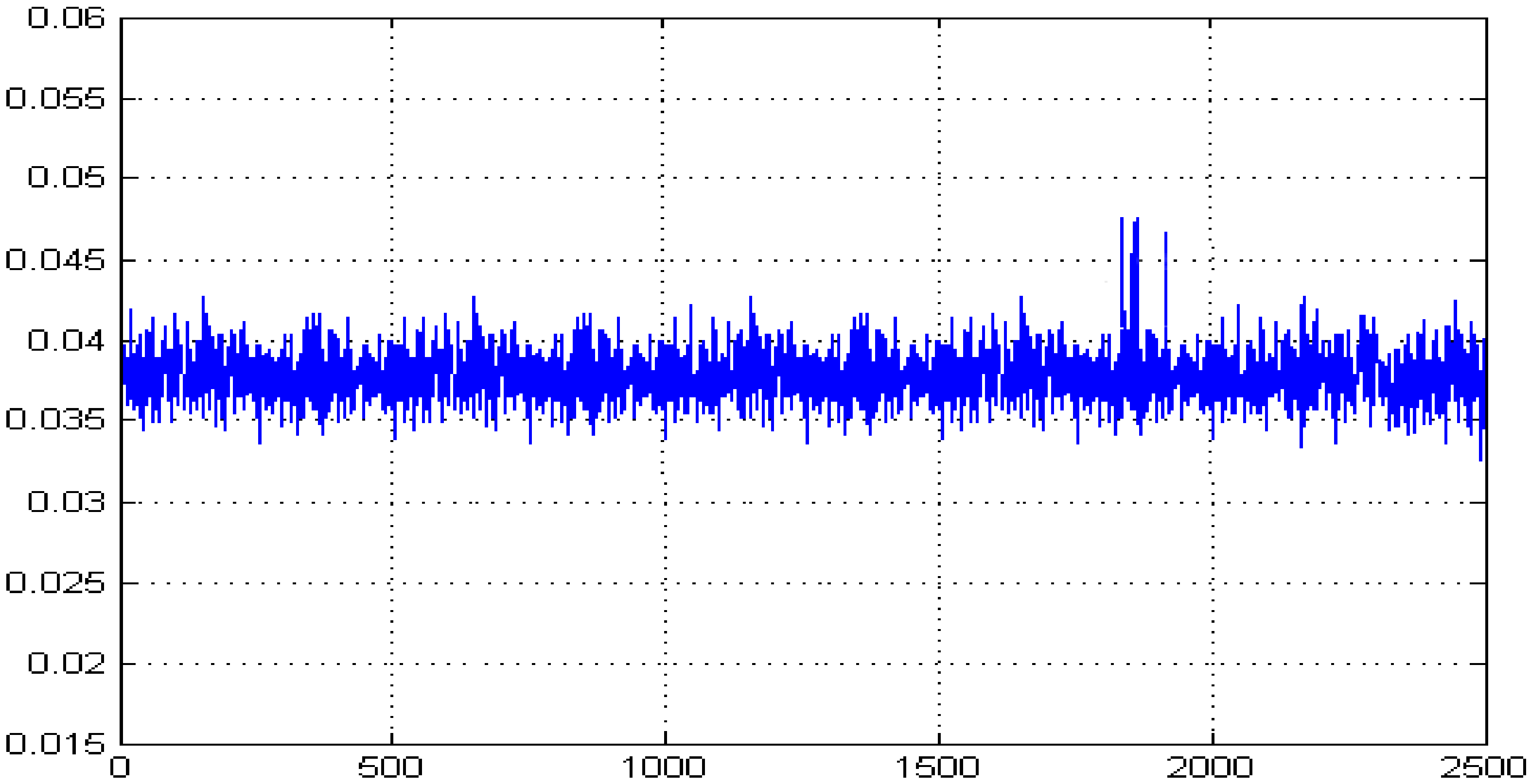
Correlation between the points of the power trace and the Hamming weight of the output of the Sbox

Experimental And Simulation Results

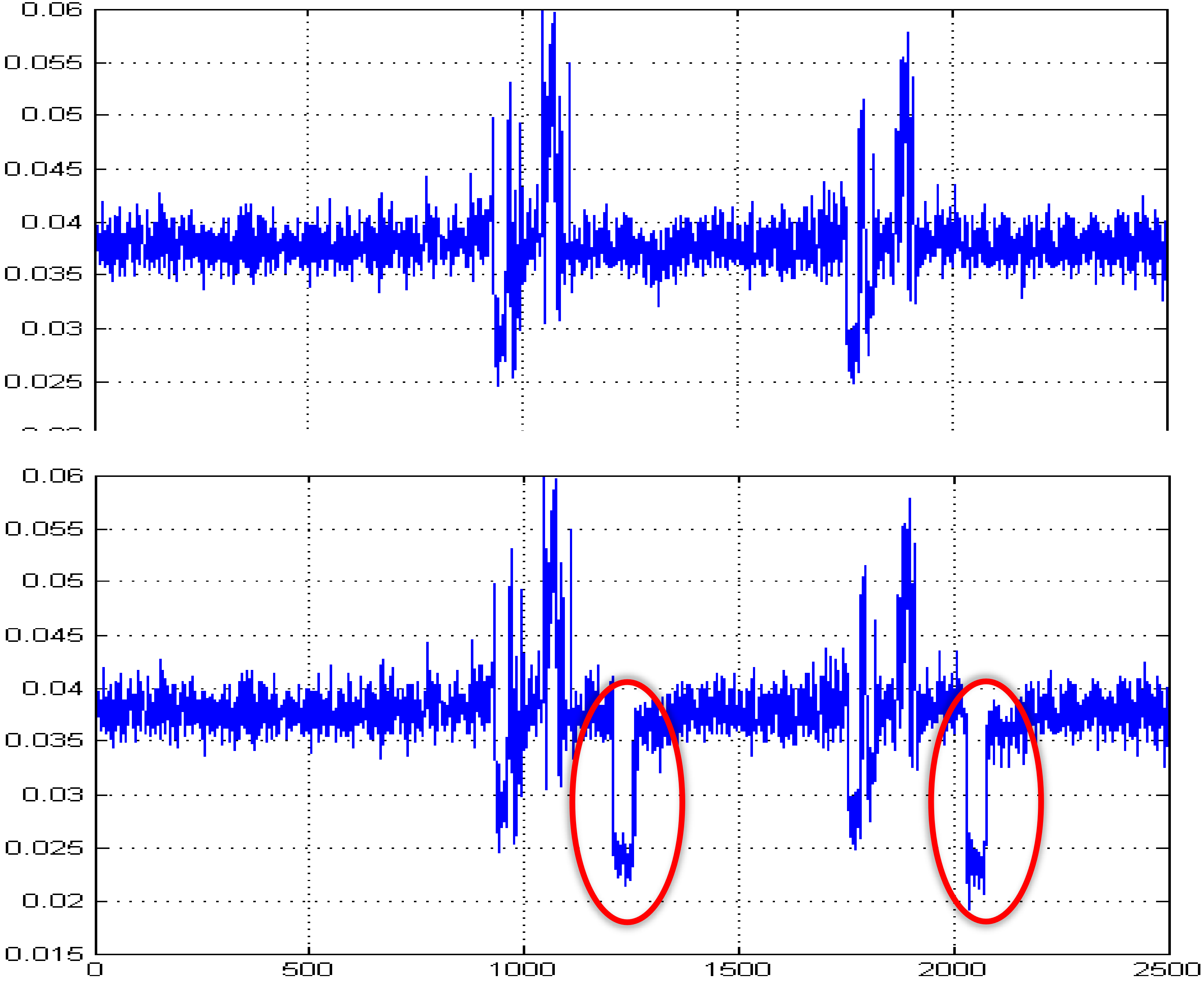


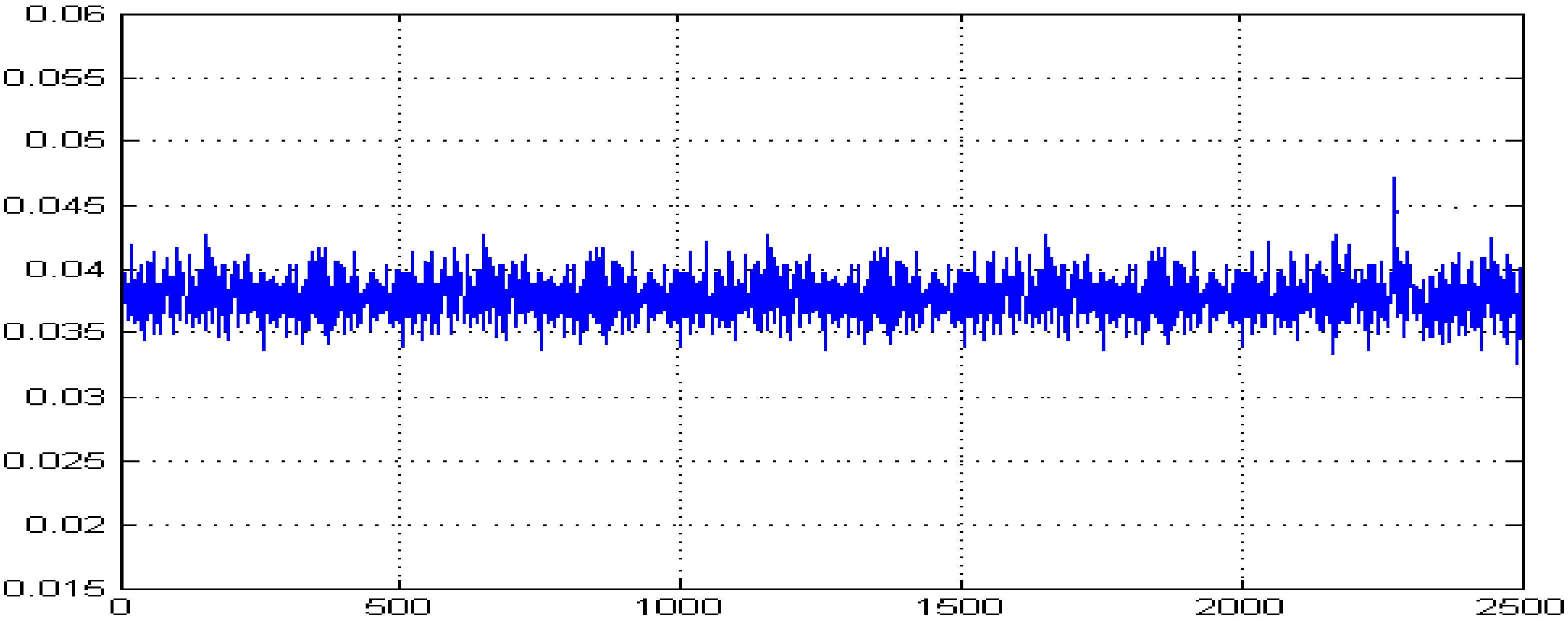
Example power trace of AES execution for one cycle after implementation

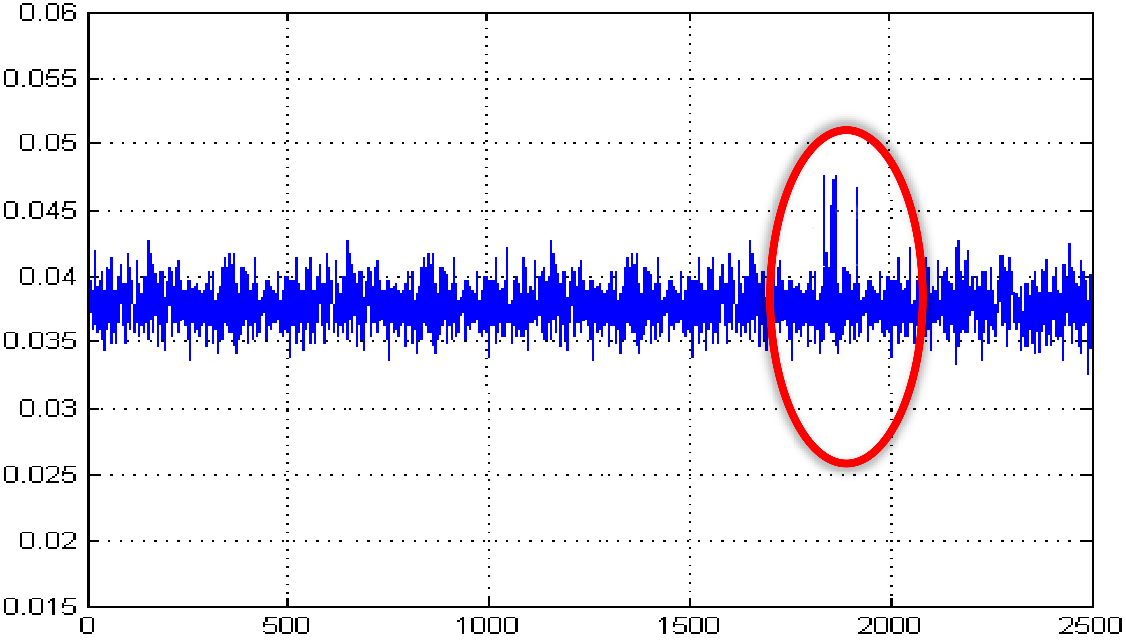
Experimental And Simulation Results



Correlation between the points of the power trace and the Hamming weight of the output of the Sbox after implementation


0.06
0.055
0.05
0.045
0.04
0.035
0.03
0.025
0.06
0.055
0.05
0.045
0.04
0.035
0.03
0.025
0.02
0.015
0
500
1000
1500
2000
2500


0.06
0.055
0.05
0.045
0.04
0.035
0.03
0.025
0.02
0.015
0
500
1000
1500
2000
2500


0.06
0.055
0.05
0.045
0.04
0.035
0.03
0.025
0.02
0.015
0
500
1000
1500
2000
2500

Conclusions

- ❑ This presenting a new countermeasure against Side-Channel Analysis (SCA) attacks, whose implementation is based on a hardware-software co-design.
- ❑ The hardware architecture consists of a microprocessor, which executes the algorithm using a false key, and a coprocessor that performs several operations that are necessary to retrieve the original text that was encrypted with the real key.
- ❑ The coprocessor hardly affects the power consumption of the device, so that any classical attack based on such power consumption would reveal a false key.
- ❑ Experimental results show in all cases that the system is effectively protected by revealing a false encryption key.

References

1. Paul Kocher, Joshua Jaffe, and Benjamin Jun, “Differential Power Analysis”, Advances in Cryptology – CRYPTO ’99, LNCS 1666, Aug. 1999, pp. 388-397.
2. Adi Shamir, “Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies”,, LNCS 1965, 2000
3. P. Sasdrich, O. Mischke, A. Moradi, T. Gneysu, Constructive side-channel analysis and secure design, 6th International Workshop,, Revised Selected Papers, Springer International Publishing 2015.
4. W. Cheng, S. Guilley, J.-L. Danger, C. Carlet and S. Mesnager, Optimal Linear Codes for IPM, Jan. 2020
5. S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards. New York, NY, USA: Springer, 2007.
6. C. Glowacz and V. Grosso, "Optimal collision side-channel attacks" in Smart Card Research and Advanced Applications, Prague, Czech Republic:Springer, vol. 11833, pp. 126-140, Nov. 2019.

THANK YOU FOR
YOUR LİSTENİNG

DO YOU HAVE
ANY QUESTİONS?