13th International Conference on Security of Information and Networks

Power analysis side-channel attacks on symmetric block cipher Magma

Southern Federal University, Russia
Stanislav Zhdanov, **Ekaterina Maro**

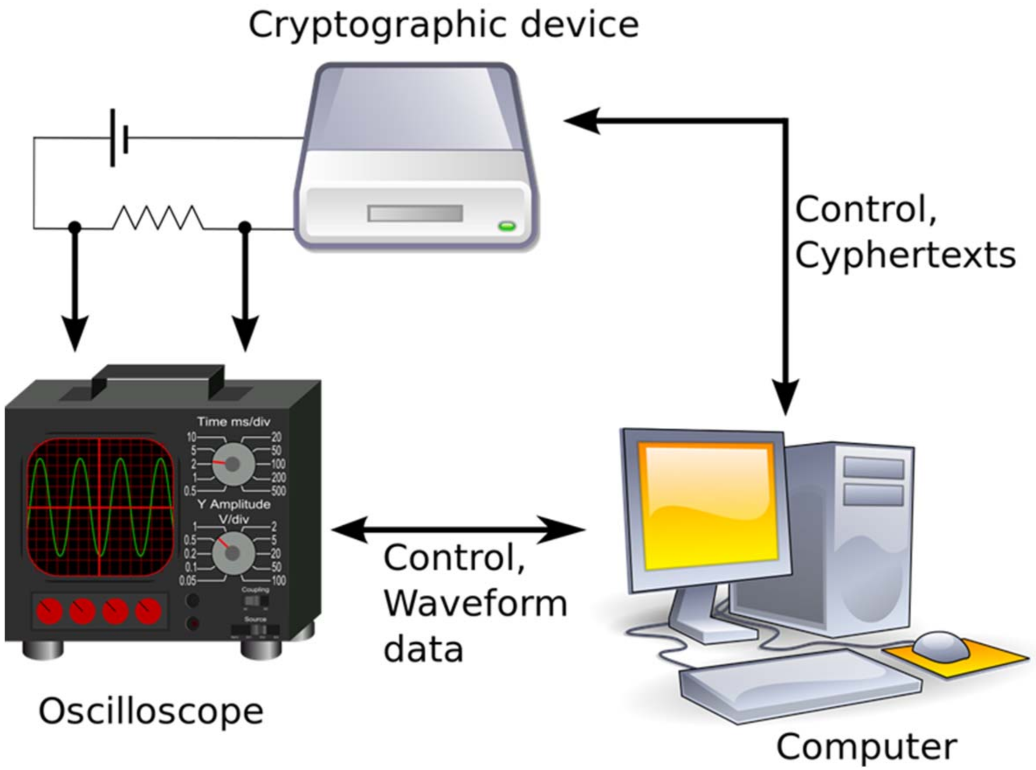
Side-channel attacks (SCA)

Side-channels attacks (SCA) is a class of attacks aimed at vulnerabilities in the **practical implementation** of cryptosystems (hardware or software).

Example of side-channels:

- Computation time (timing attack).
- Power consumption (simple power analysis (SPA) and differential power analysis (DPA)).
- Electromagnetic emitting.
- Acoustic channel (noises arising from computations operation).
- Hardware or software fault: random or malicious (incorrect application conditions, electrical circuit analysis and etc.).

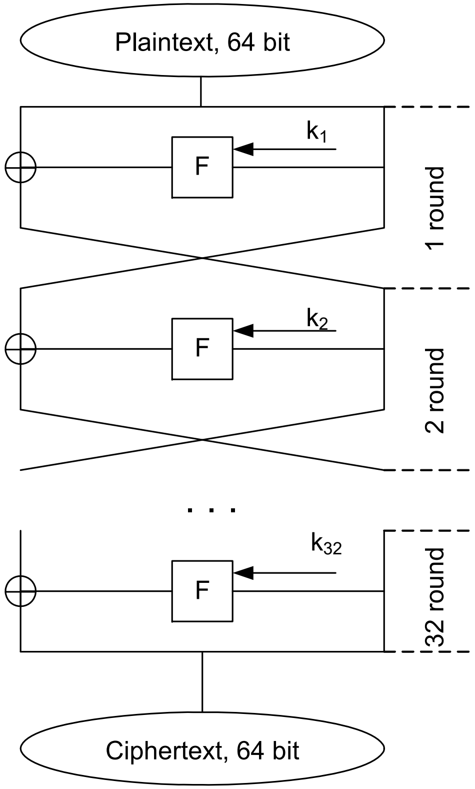
Power analysis attacks



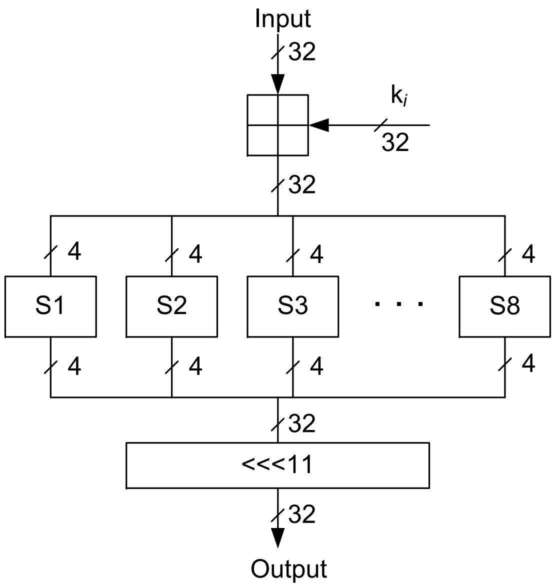
Power analysis attack methods:

- Simple power analysis (SPA).
- Differential power analysis (DPA: First-order DPA and High-order DPA).
- Correlation power analysis (CPA).
- Template power analysis.

Magma cipher (GOST R 34.12-2015, n=64)



Function F (round *i*)



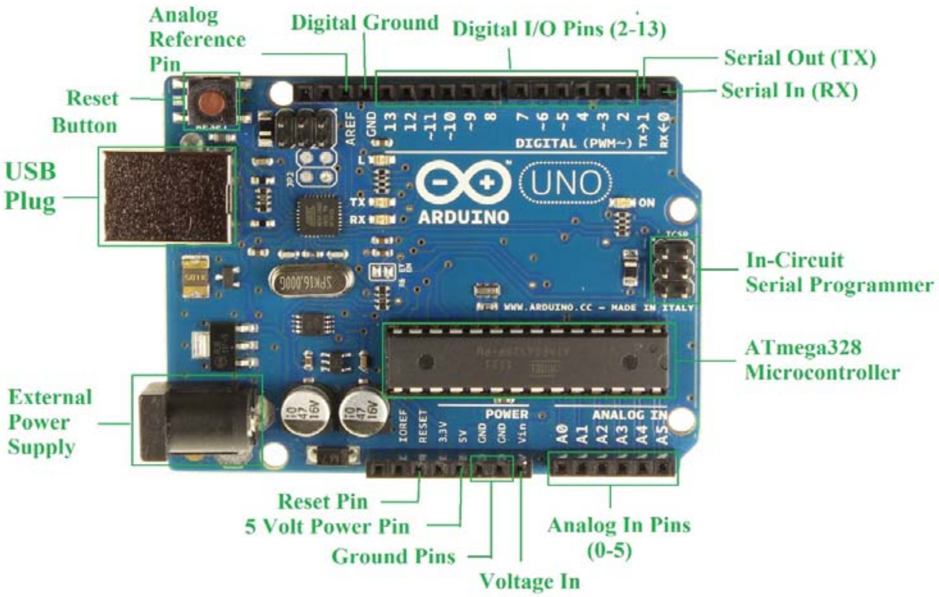
Secret Key, 256 bit: Key={K1, K2, K3, K4, K5, K6, K7, K8}

Round Key, 32 bit: k_i={K1, K2, K3, K4, K5, K6, K7, K8, K1, K2, K3, K4, K5, K6, K7, K8, K1, K2, K3, K4, K5, K6, K7, K8, K8, K7, K6, K5, K4, K3, K2, K1}

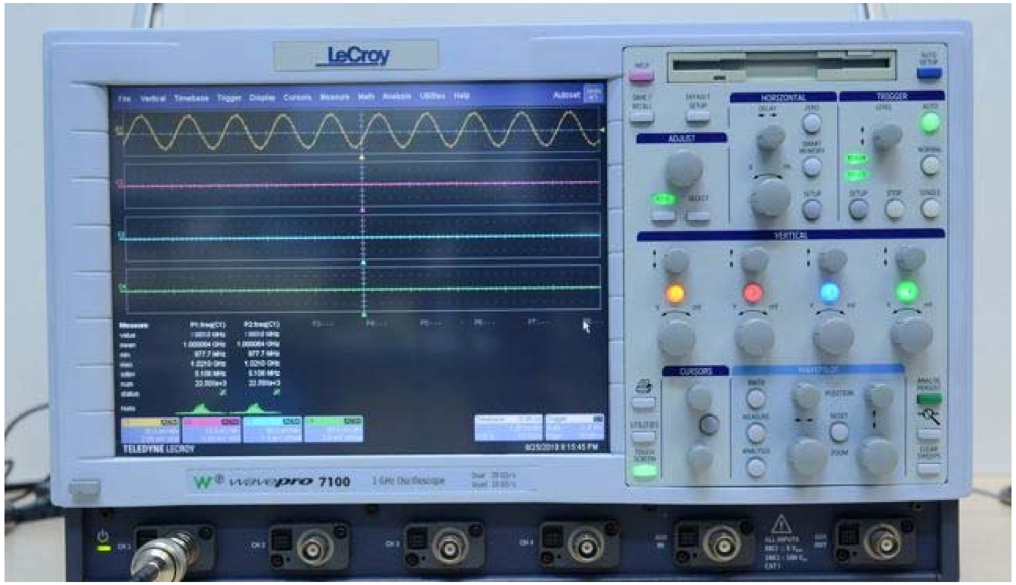
Magma encryption algorithm is a symmetric block cipher bases on Feistel network and consists of 32 encryption rounds with operations:

- Addition with a round key modulo 2^{32};
- Substitution in eight S-blocks;
- Cyclic left shift by 11 positions.

Equipment for power measurements

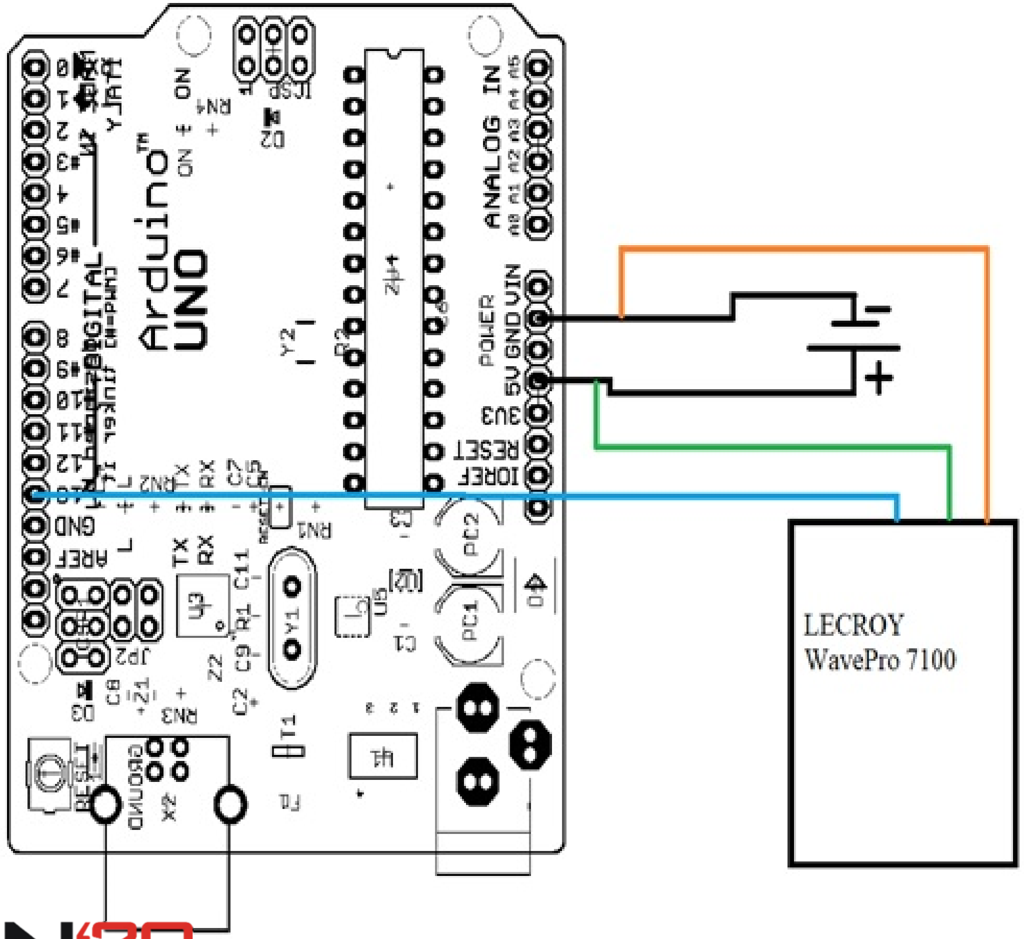


Arduino uno board : ATmega328P chip - logic chip for data processing with 16 MHz frequency, 6 analog and 14 digital input/output pins.



LECROY WavePro 7100A oscilloscope with a bandwidth of 1 GHz and a sampling frequency of 10 GHz / 4 channels.

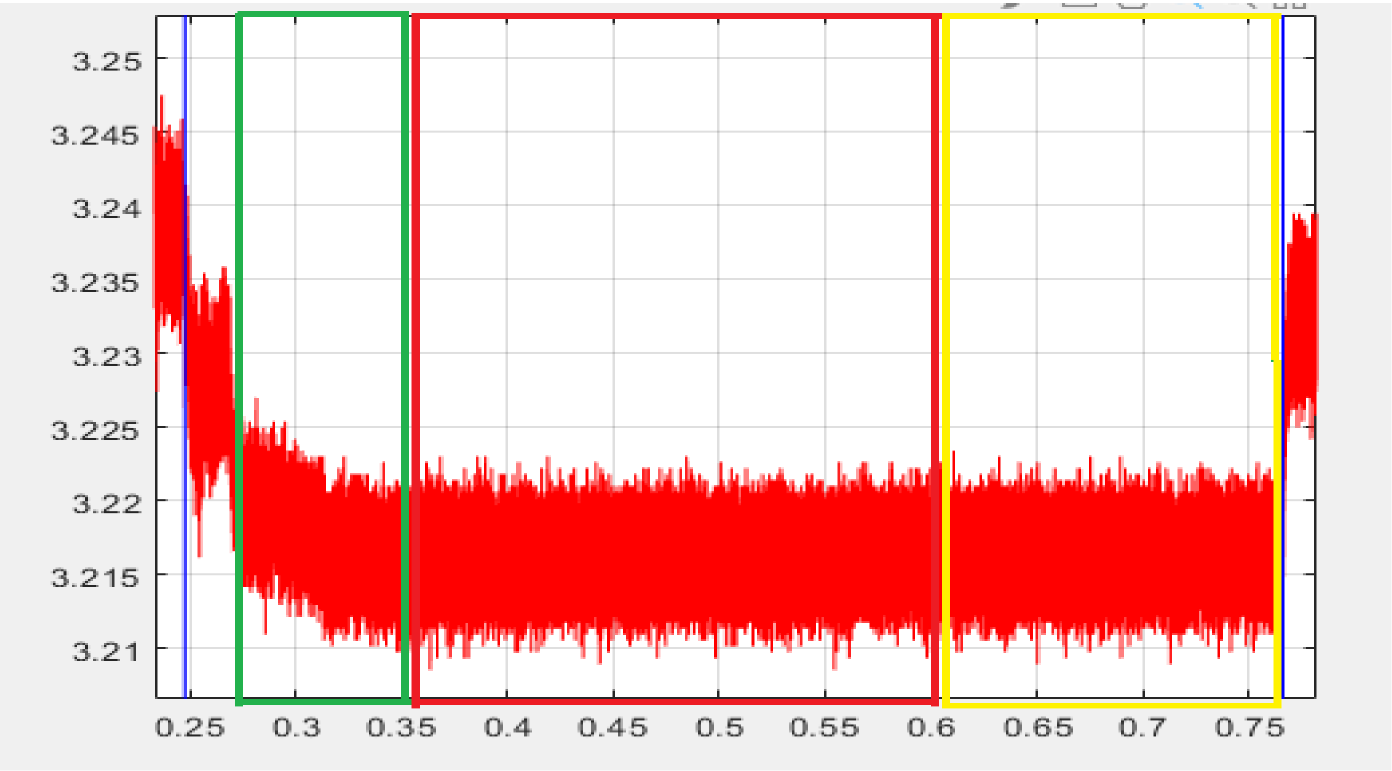
Power measurements



Arduino Uno board is powered by source (total voltage is 6 V). The first oscilloscope probe was connected to the “5V” power pin and the second to the “GND”.

We tracked start and end points of the Magma cryptographic algorithm by LED element, which was connected to Arduino board (LED element was inactive during encryption process).

Experimental power traces for one-round Magma



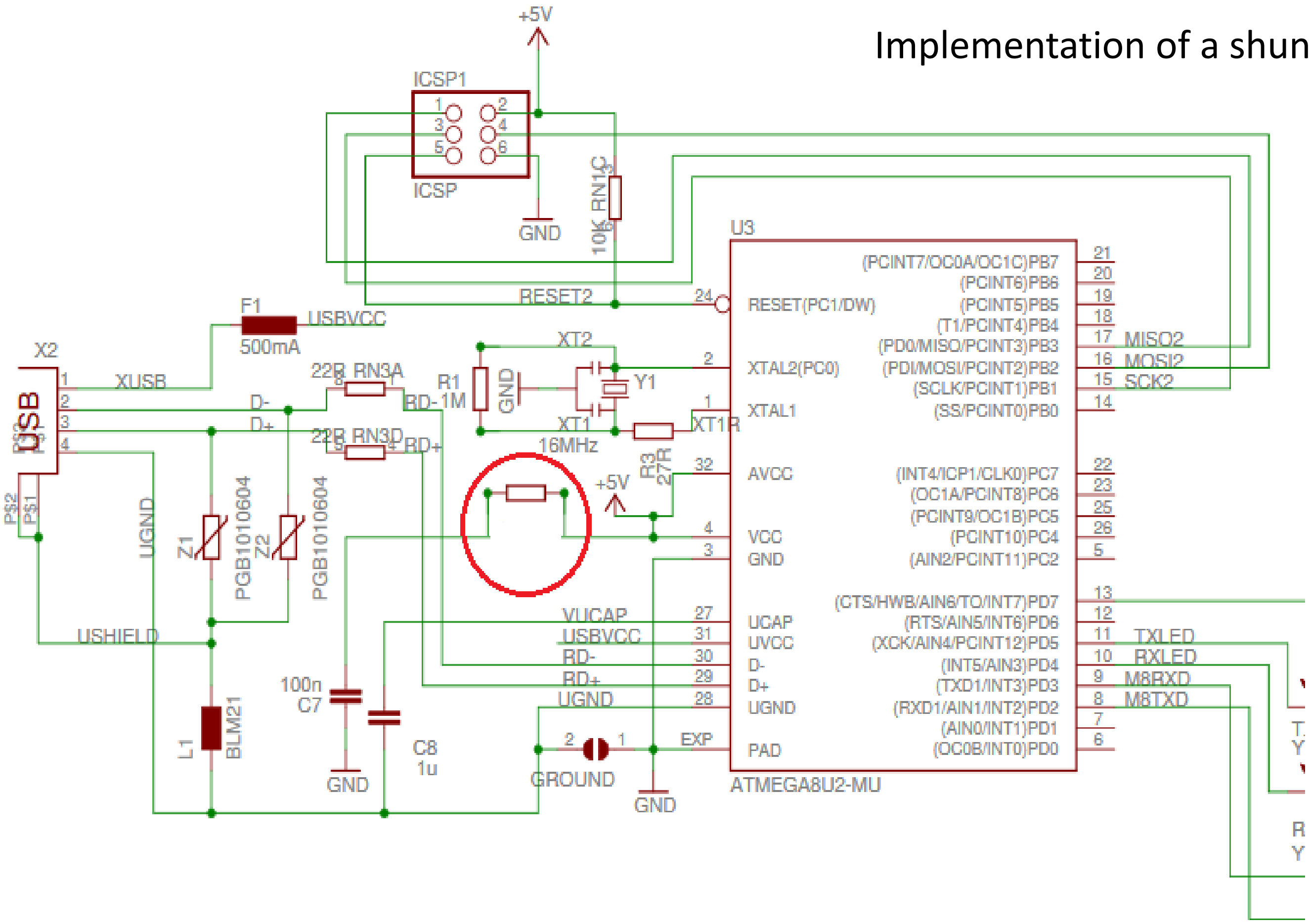
Green area contains the addition modulo 2^{32} .

Red area contains substitution operations in the S-boxes.

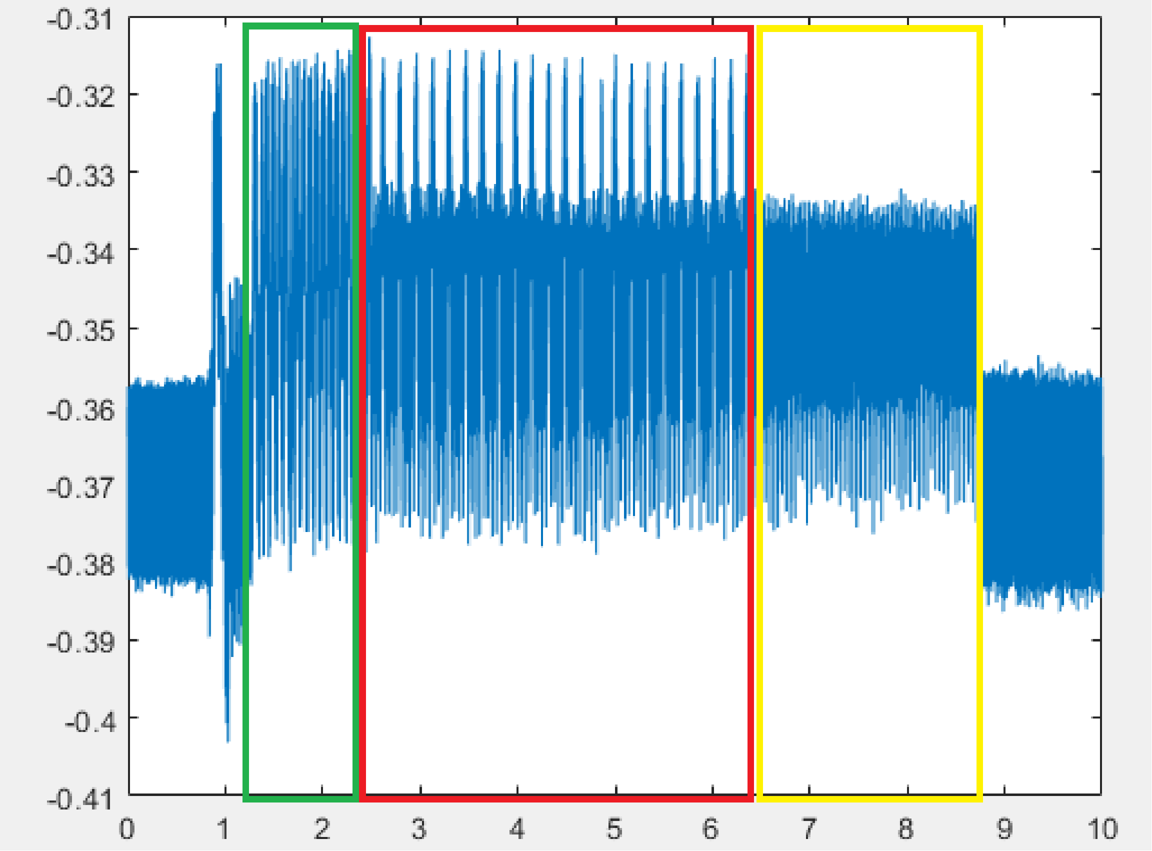
Yellow area contains a 11-bit left shift operation.

Modified Arduino board scheme

Implementation of a shunt resistor (100 Ohm)



Experimental power traces for one-round Magma (modified)



The green area contains the addition modulo 2^{32}

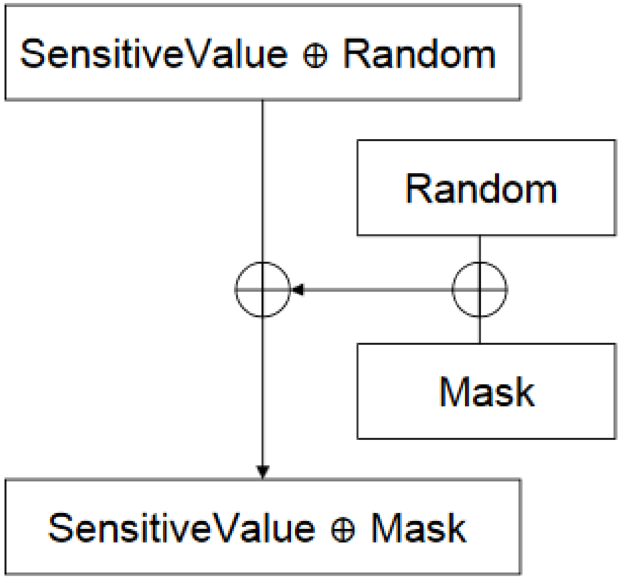
The red area contains substitution operations in the S-boxes.

The yellow area contains a 11-bit left shift operation.

SCA Countermeasures

- Random Delay Insertion (Desynchronisation)
- Noise Generator
- Shuffling
- Masking (Boolean masking, Arithmetic masking)

and etc.



Conclusion

Experiment result shows that even with small amounts of power consumption measurements it is possible to identify areas (chart's segments) with main encryption transformations for Magma cipher.

Presented measurements can be used as basis for further implementation of simple and differential analysis of encryption process on Arduino board, as well as development module for detecting Magma cipher cryptographic operations on considered IoT device.

Thank you
for your attention