Influence of Fault-Tolerant Design Techniques on Resistance against Differential Power Analysis

Vojtěch Miškovský

Czech Technical University in Prague
Faculty of Information Technology
Department of Digital Design

CryptArchi 2017
June 18–21, Smolenice

Motivation

- Reliability and security are often demanded at the same time
- Both fault-tolerant and attack-resistant design techniques usually have high area and power consumption overhead, that means even higher overhead when both are used
- The overhead of fault-tolerant design can influence the attack-resistance of the device
- The overhead of attack-resistant design can influence the reliability of the device

Long-term goals

- Examine the mutual influence of fault-tolerant and attack-resistant digital design architectures
- Discover some interplay between F-T and A-R design and use it to design both F-T and A-R architecture with lower summary overhead

Current work

- Only attacks based on physical properties of the device (like side-channel attacks or fault attacks) are related to digital design
- We started with the most common one — Differential power analysis (DPA)
- We experimentally evaluate how basic fault-tolerant architectures affects the resistance against DPA
- FPGA implementation of AES is used

Related work

Similar study was presented by Regazzoni et al.[1]

Table: Comparison of key features of Regazzoni et al. approach and our approach

Regazzoni	Our Approach
Fault attack resistant design	Fault-tolerant design
S-Box protected	the whole encryptor protected
ASIC	FPGA
Simulated power consumption	Real power consumption

Regazzoni concluded that the designs protected against fault attacks are more vulnerable to power attacks.

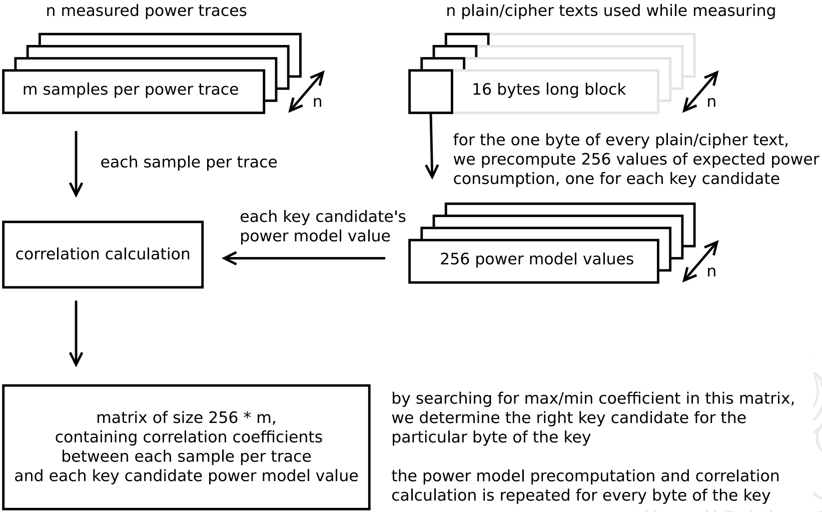
[1] Francesco Regazzoni et al. "Interaction between fault attack countermeasures and the resistance against power analysis attacks". In: *Fault Analysis in Cryptography*. Springer, 2012, pp. 257–272.

Differential Power Analysis

- Side-channel attack, introduced by Kocher et al.[2]
- Exploits the fact that a variable in the implementation exists, that its value
  - depends on the plain/cipher text used,
  - depends on a part of a key,
  - and correlates with the power consumption of the device
- Correlation power analysis is an enhanced variant of DPA, attacking one byte of a key at a time, analyzing correlation between:
  - measured power consumption samples
  - and estimated power consumption model, based on plain/cipher text and a one of the key candidates

[2] Paul Kocher, Joshua Jaffe, and Benjamin Jun. "Differential power analysis". In: *Annual International Cryptology Conference*. Springer. 1999, pp. 388–397.

Differential Power Analysis



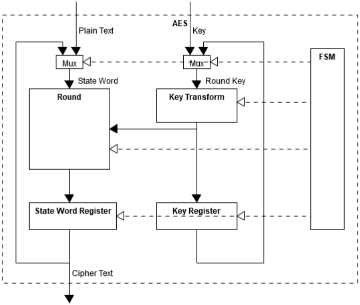
Fault-tolerant architectures

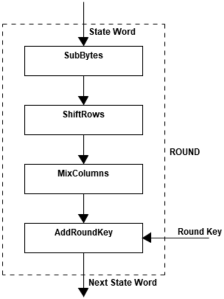
These fault-tolerant architectures were used:

- Information redundancy — S-Box Parity check (AES-SPC)
- Space redundancy
  - round level (AES-HR-R)
  - algorithm level (AES-HR-A)
- Time redundancy
  - round level (AES-TR-R)
  - algorithm level (AES-TR-A)

Plain AES implementation

128-bit variant, 10 rounds
11 clock cycle per encryption (1 initial round + 10 rounds)
After each round the state word is stored in a register



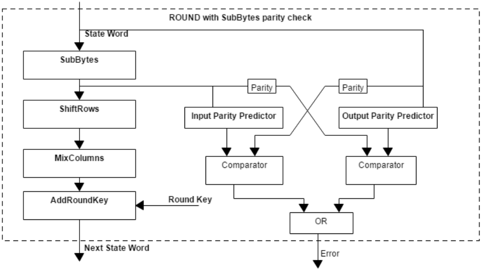


Information redundancy

S-Box (SubBytes function) is secured by parity

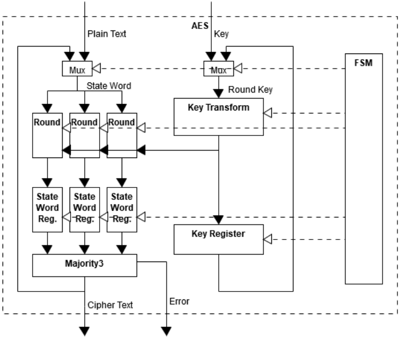
Two parity predictors are used:

- Input parity predictor
- Output parity predictor



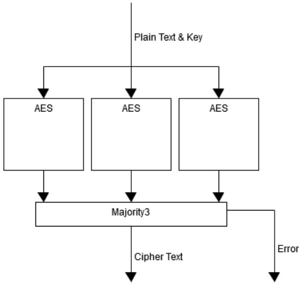
Space redundancy — Round level

The round is protected by TMR (3 copies and a majority voter)



Space redundancy — Algorithm level

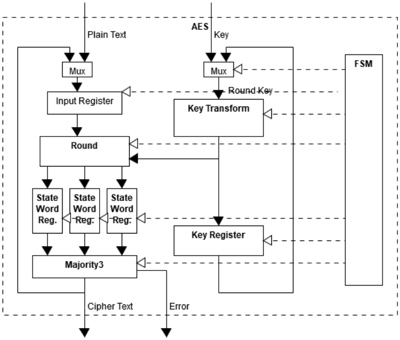
The whole AES is protected by TMR (3 copies and a majority voter)



Time redundancy — Round level

Each round is repeated 3 times and the results are compared by a majority voter

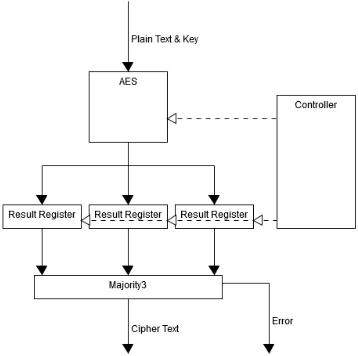
Only works for transient faults



Time redundancy — Algorithm level

The whole algorithm is repeated 3 times and the results are compared by a majority voter

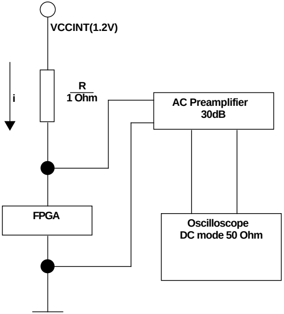
Only works for transient faults



Measurement — Hardware

Evariste II board with Altera Cyclone III FPGA module was chosen as an implementation platform[3]

Power consumption was measured by PicoScope 6404D



[3] Viktor Fischer, Florent Bernard, and Patrick Haddad. "An open-source multi-FPGA modular system for fair benchmarking of true random number generators". In: *Field Programmable Logic and Applications (FPL), 2013 23rd International Conference on*. IEEE. 2013, pp. 1–4.

Measurement — Software

- We developed our own application for DPA
- The correlation calculations are time and memory efficient, highly parallelizable and numerically stable
- Qualities of the application were published at DDECS 2017[4]
- Now we work on GPU implementation
- This application is planned to be extended to a whole DPA framework and published under open-source license

[4] Petr Socha et al. "Optimization of Pearson correlation coefficient calculation for DPA and comparison of different approaches". In: *2017 IEEE 20th International Symposium on Design and Diagnostics of Electronic Circuits Systems (DDECS)*. 2017, pp. 184–189. DOI: 10.1109/DDECS.2017.7934563.

Experiment setup

- We obtained 50 sets of 2000 power traces for each F-T variant of AES, 1000 samples per power trace
- For each set, we performed the DPA with various number of power traces to find the minimal numbers of power traces sufficient to obtain the correct cipher key (*minTraces*)
- The AES variants are compared by medians of the *minTraces*
- Lower *minTraces* means lower resistance against DPA (it is easier to perform the attack)

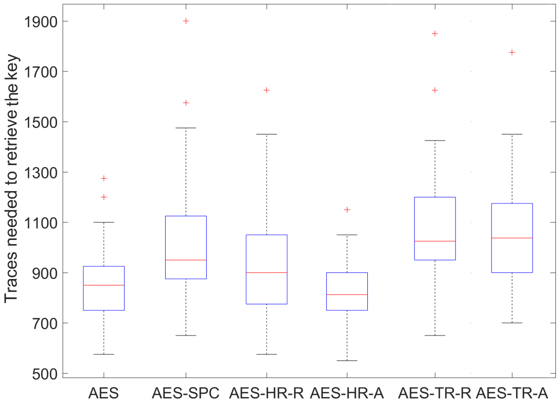
Results

Table: Comparison of AES variants based on median and interquartile range of *minTraces* (minimal number of power traces needed to reveal the correct key) [6]

Architecture	Median	Interquartile range	Diff. from AES
AES	850	175 (20.5%)	0%
AES-SPC	950	250 (26.3%)	+12%
AES-HR-R	900	275 (30.5%)	+6%
AES-HR-A	812	150 (18.5%)	-4%
AES-TR-R	1025	250 (24.4%)	+21%
AES-TR-A	1037	275 (26.5%)	+22%

[6] SPC — S-Box parity check, HR — space redundancy, TR — time redundancy; R — round level, A — algorithm level

Results



[6] SPC — S-Box parity check, HR — space redundancy, TR — time redundancy; R — round level, A — algorithm level

Conclusion

- We show that basic redundancy techniques have insignificant influence on resistance against DPA on implementation not secured against DPA
- We presume these techniques can be used to make DPA resistant devices fault-tolerant
- This statement should be verified using e.g. another FPGA platforms
- Our results are contrary to results presented by Regazzoni et al. We believe that the main reason is the different power consumption evaluation (simulation vs. real measurement)

Acknowledgment

This research has been partially supported by the grant GA16-05179S of the Czech Grant Agency, "Fault-Tolerant and Attack-Resistant Architectures Based on Programmable Devices: Research of Interplay and Common Features" (2016-2018) and CTU project SGS17/213/OHK3/3T/18.