Influence of Fault-Tolerance Techniques on Power-Analysis Resistance of Cryptographic Design

Jan Říha, Vojtěch Miškovský, Hana Kubátová, Martin Novotný
Czech Technical University in Prague
Faculty of Information Technology
Email: {rihaja11,miskovoj,kubatova,novotnym}@fit.cvut.cz

***Abstract*—As the security is becoming more and more important these days, we still should not forget about reliability. When designing a cryptographic device for some mission-critical or another reliability demanding system, we need to make the device not only attack-resistant, but also fault-tolerant. There are many common fault-tolerant digital design techniques, however, it is questionable, how these techniques affect the attack-resistance. Do they make the device more vulnerable e.g. to side-channel attacks?**

In our work we focused on finding the answer to this question. We experimentally evaluated the influence of information redundancy, space redundancy and time redundancy techniques on resistance against power analysis attack. In this paper we present our observations.

I. Introduction

Security is a common issue in many fields including digital design. Every cryptographic device needs to use some secure cipher. But another important thing is to protect such a device against Side Channel Attacks [1] [2]. Side Channel Attacks do not compromise the cryptographic properties of the cipher, but they exploit the implementation properties of the device. These attacks can be based on e.g. electromagnetic radiation [3] [4], fault injection [5] [6] and so on. In our research we focus on attacks based on power analysis, namely the differential power analysis (DPA) [7] [8]. For the investigation of influence of fault-tolerant architectures on attack-resistance we use AES cipher [9] implemented in FPGA.

Many methods have been developed to protect the cryptographic circuit against power analysis attacks. Popular methods include masking [10] [11] [12], Dual-Rail logic [13] [14] [15] [16] [17] [18], voltage and frequency switching [19] or Threshold implementation [20] [21] [22].

Sometimes such a cryptographic device can be required to be also fault-tolerant [23], e.g. when the device is a part of some mission–critical system. To make the digital design implemented in FPGA fault-tolerant, we can use some common fault-tolerant architectures like space redundancy, time redundancy or information redundancy [23] [24] [25] [26], or we can use FPGA specific methods, e.g. dynamic reconfiguration [27], BIST [28] [29], etc. When using fault-tolerant methods in cryptographic circuits, one important question arises: how do these methods influence the attack-resistance of the design?

In this paper we focus on the common fault-tolerant architectures, specifically space redundancy, time redundancy and parity check. We compare these architectures to a plain implementation of cryptographic algorithm. As a reference design we have chosen AES algorithm without countermeasures against DPA, so we can easily compare the influence of the fault-tolerant architectures.

We provide summary of works related to this topic in Section II. Detailed description of the fault-tolerant architectures we used and our expectations about their influence on DPA resistance are presented in Section III. In Section IV we describe the whole experiment setup. Results of our experimental evaluation are presented and discussed in Section V. Our findings are concluded in Section VI. In Section VII we propose several directions for future research.

II. Related Work

As stated in Section I, there is a lot fault-tolerant design architectures. In this paper we focus on basic fault-tolerant architectures — space redundancy, time redundancy and information redundancy. These architectures can be easily implemented in FPGA, as is shown in [25] and [26].

In this work we experimentally evaluate the resistance against differential power analysis originally introduced by Kocher et al. [7], specifically differential power analysis with correlation coefficients (correlation power analysis) [30] [31].

To the best of our knowledge, there is no research targeting mutual influence of fault-tolerant and attack-resistant digital design available in open literature. Nevertheless, fault-tolerant techniques are similar to countermeasures against fault-injection analysis. Regazzoni et al. [32] [33] focused on influence of fault attack countermeasures (mostly information redundancy of S-Boxes) on power analysis resistance. Based on the simulation of an ASIC circuit running AES algorithm they conclude that fault attack countermeasures are making the device more vulnerable to DPA. More comprehensive comparison was introduced in [34]. The wider range of fault detection methods embraced also space redundancy and information redundancy architectures. An FPGA platform SAKURA-G containing Xilinx Spartan-6 was used. Authors concluded that these methods have negative influence on attack-resistance. Nevertheless, this research was again focused on securing the S-Boxes, which is mainly used by fault attack countermeasures.

Unlike the above mentioned studies, we focus on fault-tolerance in context of reliability. We also make detailed quantification of our results.

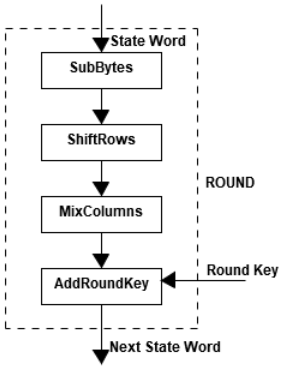


Figure 1. Diagram of a round implementation

III. Architectures

To evaluate and compare the influence of fault-tolerant techniques on resistance against DPA, we implemented one standard AES circuit (without any protection) and five AES circuits employing fault-tolerant techniques:

- information redundancy (parity check of SubBytes function [9]).
- space redundancy at round level
- space redundancy at algorithm level
- time redundancy at round level
- time redundancy at algorithm level

A. Standard AES (reference design)

AES is a common block cipher offering three different lengths of key: 128-bit, 192-bit and 256-bit. For each variant the block is 128 bit long. We chose the 128-bit variant which consists of 10 rounds. Each round is composed of four functions applied in this order: SubBytes, ShiftRows, MixColumns and AddRoundKey. Additionally, the AddRoundKey is once applied before the first round (this is often called the initial round). In the last (10th) round the MixColumns functions is omitted. For each round a new key is derived from the previous one in Key scheduler [9].

In our implementation each round is processed in one clock cycle. The datapath of the design consists of a combinational circuit implementing all four round functions, a register holding the result of the round (state word) and a next round key generator. Therefore the encryption takes 11 clock cycles (10 rounds + the initial round). Simplified diagrams of a round and the whole cipher module are shown in Figure 1 and Figure 2.

B. SubBytes Parity Check

This fault-tolerant architecture is designed to detect fault by parity check in a large, non-linear part of AES design which are the modules implementing SubBytes function (S–Boxes) [26]. Since SubBytes, being a nonlinear function, does not preserve parity, we needed to implement parity predictor. We use two parity predictors. The first one is predicting the parity of the output using the input and the second one is predicting

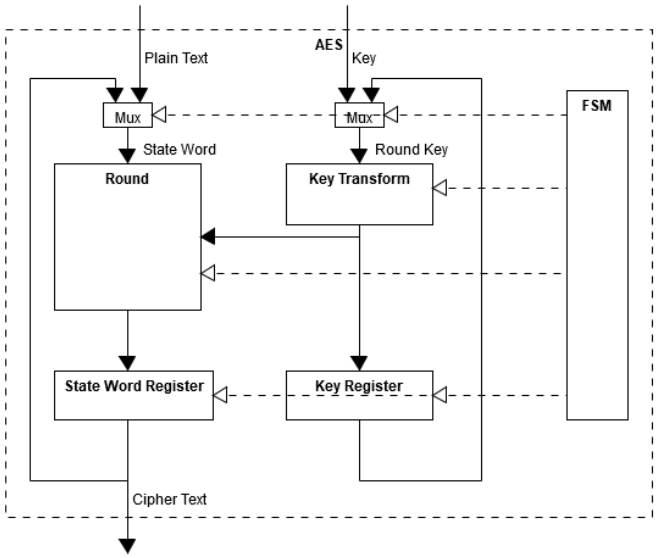


Figure 2. Diagram of AES module implementation

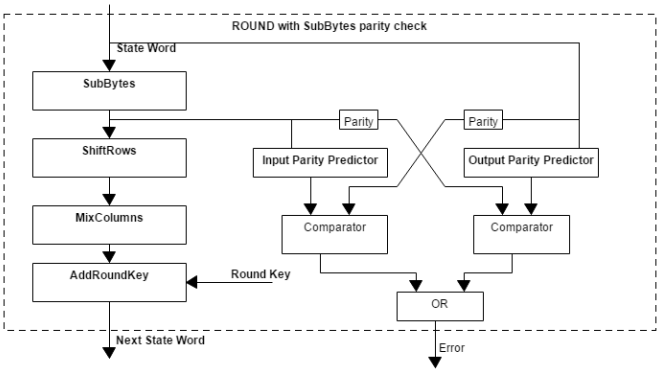


Figure 3. Diagram of a round with parity checked SubBytes

the parity of the input using the output. Both predicted values are compared with the real values and a fault is indicated when they differ. There are both input and output parity checkers for each of 16 S–Boxes. Diagram of a round with parity checked SubBytes function is shown in Figure 3.

As this architecture introduces very low area overhead, we expect the power consumption to be similar to the power consumption of the reference design and we also expect this design not to affect the DPA resistance. On the other hand, this architecture does not provide any fault correction. It provides just the fault detection, moreover limited to S-Boxes only.

C. Space Redundancy — Round Level

We use common fault-tolerant architecture — Triple-Modular Redundancy (TMR) [23]. It is based on three copies of a module and a majority voter. When one of the modules is faulty, the majority voter ensures that the result is still correct. It can also detect faults in two modules (unless the faults are equal). Diagram of this architecture is shown in Figure 4.

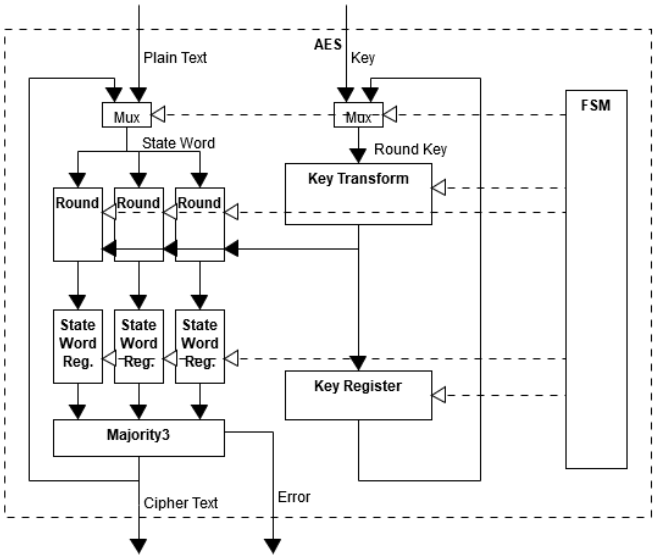


Figure 4. Diagram of AES secured by space redundancy at round level

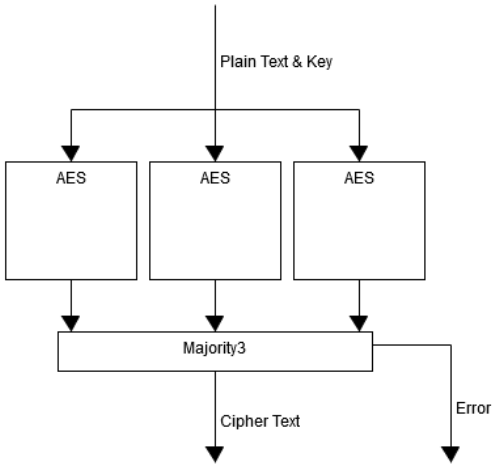


Figure 5. Diagram of AES secured by space redundancy at algorithm level

In this case we use TMR at round level, so the datapath of the design is triplicated.

This architecture causes high area overhead (the round logic is triplicated), which leads to increased power consumption. This increase should triplicate the information available in the power consumption, thus it should increase the signal to noise ratio, which would make the device more vulnerable to DPA. On the other hand, the power consumption of the majority voter can introduce some additional noise.

D. Space Redundancy — Algorithm Level

This architecture is based on TMR, as so as the one in Section III-C. The difference is in the redundancy level. In this case the whole AES module is triplicated. Diagram of this architecture is shown in Figure 5.

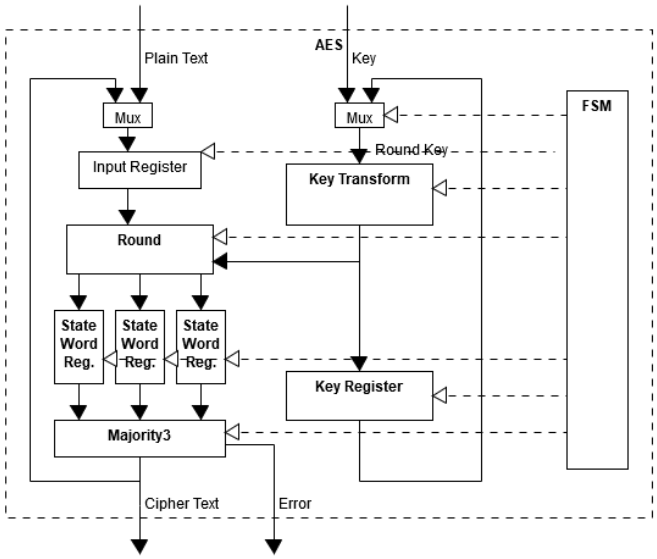


Figure 6. Diagram of AES secured by time redundancy at round level

In this case we also expect increased power consumption. In comparison with the round level, the overall power consumption increase should be higher, but the additional information in this increase should be the same. Therefore we expect this architecture to have lower influence on DPA resistance than the architecture described in Section III-C.

E. Time Redundancy — Round Level

Time redundancy is based on repeating the same calculations on the same data multiple times. In this architecture each round is run three times, each result is stored in a register and then the results are compared by majority voter similarly to the one in Section III-C. With this approach, only the transient faults are considered. Diagram of this architecture is shown in Figure 6.

This architecture introduces minimal area overhead (only the voter and registers for result of each iteration are added). Compared to the reference circuit described in Section III-A, the information available in the power consumption is exposed three times in the circuit with time redundancy. This should not affect the DPA resistance significantly.

F. Time Redundancy — Algorithm Level

This architecture is very similar to the one in Section III-E. The difference is, that in this case we do not repeat each round separately, but we repeat the whole encryption. The results are also stored and then compared by a majority voter. Diagram of this architecture is shown in Figure 7.

We expect the same influence on DPA resistance as in Section III-E.

IV. Measurement

In this section we describe the hardware and software used for the measurement and we also discuss how we evaluated the results.

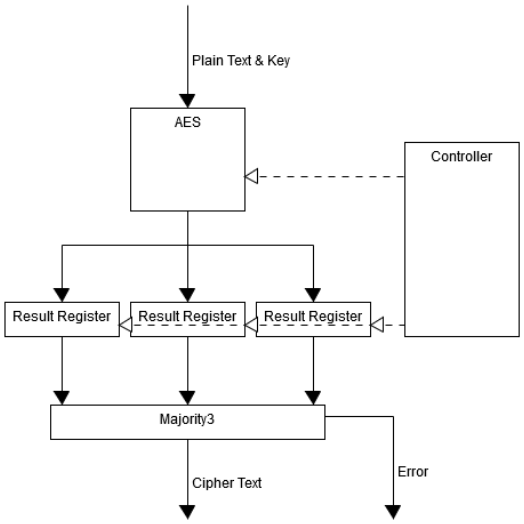


Figure 7. Diagram of AES secured by time redundancy at algorithm level

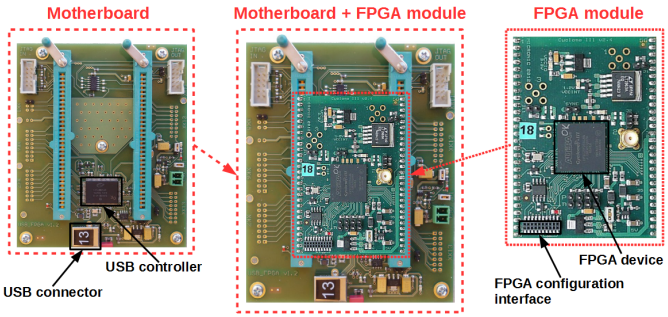


Figure 8. Evariste III platform board with Altera Cyclone III module

A. FPGA Platform

The attack was performed on Evariste III platform with Altera Cyclone III FPGA module [35]. The Evariste platform is shown in Figure 8. All AES variants were synthesized by Altera Quartus II 13.1. The frequency of the FPGA was set to 1 MHz.

B. Power Analysis

The power consumption was measured by Agilent DSO 7104A oscilloscope. How the oscilloscope is connected to the Evariste board is shown in Figure 9.

The measured data were obtained by a simple C language based application. For each encryption we obtained a power-trace of 1000 samples. Powertraces of each used architecture are shown in Appendix, in Figure 12.

The power analysis was done by a script written in MATLAB. We analyzed the data using the DPA with correlation coefficients [30]. Concerning power model, we use Hamming distance between the value at the beginning of the 10th round (STATE 9) and the ciphertext (STATE 10), as depicted in Figure 10. The key was divided into bytes.

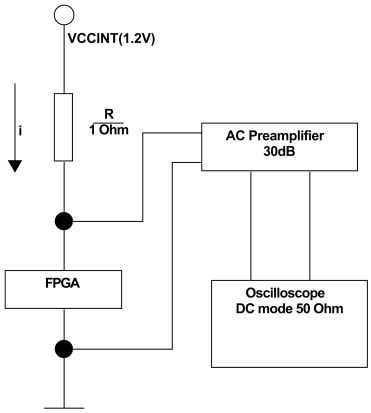


Figure 9. Diagram of connection of the oscilloscope

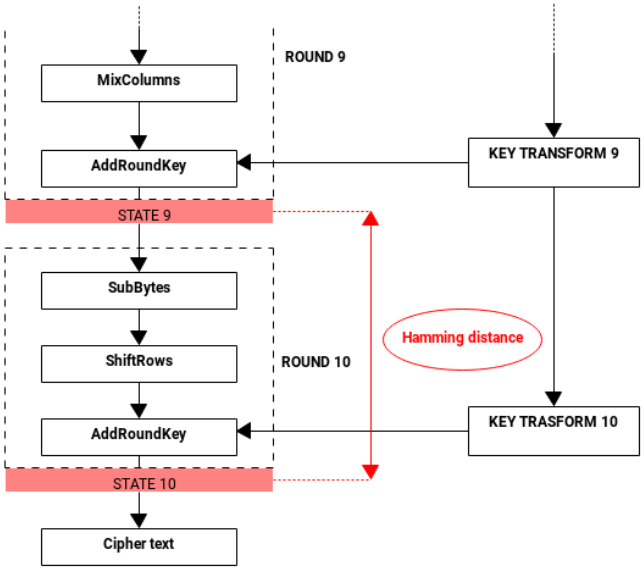


Figure 10. Diagram of the used power model

The key candidate choice was based on the most significant change of the correlation in the correlation matrix. Correlation plots of each architecture are made of 2000 powertraces and they are shown in Appendix, in Figure 13.

C. Evaluation

As quantification of the DPA resistance we used the minimal amount of power traces leading to the key candidate which was the correct key for all bytes, hereinafter referred to as *minTraces*.

For each variant of AES we collected 50 different sets of power traces thus we obtained 50 *minTraces* for each variant.

V. Results

The AES variants are compared by median of *minTraces* and its interquartile range, because the standard deviation was up to 20% of the mean and quantiles are less susceptible to

Table I
COMPARISON OF AES VARIANTS BASED ON MEDIAN AND INTERQUARTILE RANGE OF *minTraces*

Architecture	Median	Interquartile range	Difference from AES
AES	850	175	0%
AES-SPC	950	250	+12%
AES-HR-R	900	275	+6%
AES-HR-A	812	150	-4%
AES-TR-R	1025	250	+21%
AES-TR-A	1037	275	+22%

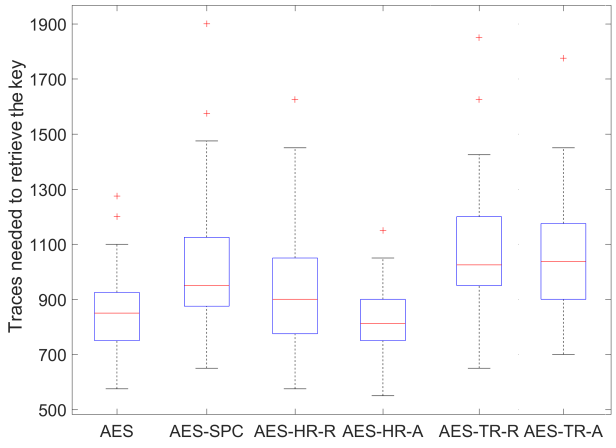


Figure 11. Box plot of *minTraces* of measured AES architectures

long-tailed distributions and outliers than means (as stated in [36], pages 85–86).

The comparison of medians and interquartile ranges is shown in Table I with following meaning of the abbreviations:

- **AES:** Standard AES module (reference design, Section III-A)
- **AES-SPC:** SubBytes parity check (Section III-B)
- **AES-HR-R:** Space Redundancy at round level (Section III-C)
- **AES-HR-A:** Space Redundancy at algorithm level (Section III-D)
- **AES-TR-R:** Time Redundancy at round level (Section III-E)
- **AES-TR-A:** Time Redundancy at algorithm level (Section III-F)

As we can see, the differences between studied AES architectures lie within the interquartile range, therefore the results are statistically insignificant. Almost all architectures show positive influence on DPA resistance. The overlap of the interquartile ranges can be seen at the box plot in Figure 11. In the following we discuss obtained results and we confront them with our assumptions stated in Section III.

A. SubBytes Parity Check (AES-SPC)

This architecture made the design little less vulnerable to DPA. This is probably caused by the parity checkers, which act like a noise generator. Nevertheless, the influence is low.

B. Space Redundancy (AES-HR-R, AES-HR-A)

In this case the difference of *minTraces* is very low. The algorithm level redundancy is the only architecture which made the design less resistant. In case of the round level, the resistance is a bit increased. This result is contrary to our assumptions. On the other hand, the results are both very similar to the original AES implementation, so it is hard to make any conclusion.

C. Time Redundancy (AES-TR-R, AES-TR-A)

Despite our assumptions, the time redundancy proved to have the highest influence on the DPA resistance of the measured architectures. The median of *minTraces* is on the edge of interquartile range of the original AES implementation. However, this result may have simple explanation: as long as we obtained 1000 samples per a powertrace in all studied architectures, in case of the time redundancy architectures the sample resolution was three times lower. This could be the cause of the *minTraces* increase.

VI. CONCLUSION

As we show in Section V, the measured fault-tolerant architectures had minimal influence on resistance against DPA. Most of the architectures even increased the resistance.

The parity check of SubBytes introduces noise and it increases the resistance a bit. The space redundancy seems to balance the noise and information increase. The time redundancy shows the highest influence but it is based on the longer duration of encryption and can be evaded by e.g. attacking one third of the powertrace.

For our purposes of making a device fault-tolerant and attack-resistant at the same time, these results proved that we can use the studied fault-tolerant architectures without making the device more vulnerable to DPA. The difference is statistically insignificant and above that, it is usually positive.

These results are in contradiction with results of similar studies mentioned in Section II [32] [33] [34]. Even though this difference can be made by a slightly different focus of the fault detection, it would be good to repeat the measurement using another FPGAs to examine the possibility that the results could differ across different FPGA platforms.

VII. FUTURE WORK

We plan to continue this research by measuring the influence of another fault-tolerant architectures on power analysis resistance. We also plan to repeat the measurement with various FPGAs and make a comparison.

Another important problem when designing a device protected against faults and attacks is evaluation of reliability of the currently used attack countermeasures.

While it is obvious that there is a close relation between fault-tolerance and resistance against fault attacks, there are differences between them. Fault-tolerance serves to keep device operational when a spontaneous defect is introduced, while the resistance against fault attacks prevents an intentional fault injection and any fault related information leakage.

We plan to examine the relation between those properties closely.

As long as the overhead of both fault-tolerant and attack-resistant architectures is high, we want to use the results of this research to introduce new digital design architectures, which will fulfill this dependability properties and decrease the overhead.

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 SGS17/017/OHK3/1T/18. We also want to thank Tomáš Zimmerhakl providing us the fault-tolerant AES implementations.

REFERENCES

[1] T.-H. Le, C. Canovas, and J. Clédiere, "An overview of side channel analysis attacks," in *Proceedings of the 2008 ACM symposium on Information, computer and communications security*, pp. 33–43, ACM, 2008.

[2] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," in *Annual International Cryptology Conference*, pp. 398–412, Springer, 1999.

[3] J. R. Rao and P. Rohatgi, "EMpowering Side-Channel Attacks.," *IACR Cryptology ePrint Archive*, vol. 2001, p. 37, 2001.

[4] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 251–261, Springer, 2001.

[5] E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," in *Annual International Cryptology Conference*, pp. 513–525, Springer, 1997.

[6] H. Ziade, R. A. Ayoubi, R. Velazco, *et al.*, "A survey on fault injection techniques," *Int. Arab J. Inf. Technol.*, vol. 1, no. 2, pp. 171–186, 2004.

[7] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Annual International Cryptology Conference*, pp. 388–397, Springer, 1999.

[8] M.-L. Akkar, R. Bevan, P. Dischamp, and D. Moyart, "Power analysis, what is now possible...," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 489–502, Springer, 2000.

[9] N. F. Pub, "197: Advanced encryption standard (AES)," *Federal Information Processing Standards Publication*, vol. 197, no. 441, p. 0311, 2001.

[10] F.-X. Standaert, E. Peeters, and J.-J. Quisquater, "On the masking countermeasure and higher-order power analysis attacks," in *Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on*, vol. 1, pp. 562–567, IEEE, 2005.

[11] J. Blömer, J. Guajardo, and V. Krummel, "Provably secure masking of AES," in *International Workshop on Selected Areas in Cryptography*, pp. 69–83, Springer, 2004.

[12] F. Regazzoni, Y. Wang, F.-X. Standaert, *et al.*, "FPGA implementations of the AES masked against power analysis attacks," *Proceedings of COSADE*, vol. 2011, pp. 56–66, 2011.

[13] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proceedings of the conference on Design, automation and test in Europe-Volume 1*, p. 10246, IEEE Computer Society, 2004.

[14] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic: DPA-resistance without routing constraints," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 172–186, Springer, 2005.

[15] K. Tiri, D. Hwang, A. Hodjat, B.-C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "Prototype IC with WDDL and differential routing–DPA resistance assessment," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 354–365, Springer, 2005.

[16] Z. Chen and Y. Zhou, "Dual-rail random switching logic: a countermeasure to reduce side channel leakage," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 242–254, Springer, 2006.

[17] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 232–241, Springer, 2006.

[18] J.-L. Danger, S. Guilley, S. Bhasin, and M. Nassar, "Overview of dual rail with precharge logic styles to thwart implementation-level attacks on hardware cryptoprocessors," in *Signals, Circuits and Systems (SCS), 2009 3rd International Conference on*, pp. 1–8, IEEE, 2009.

[19] S. Yang, W. Wolf, N. Vijaykrishnan, D. N. Serpanos, and Y. Xie, "Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach," in *Proceedings of the conference on Design, Automation and Test in Europe-Volume 3*, pp. 64–69, IEEE Computer Society, 2005.

[20] Y. Desmedt, "Some recent research aspects of threshold cryptography," in *International Workshop on Information Security*, pp. 158–173, Springer, 1997.

[21] S. Nikova, C. Rechberger, and V. Rijmen, "Threshold implementations against side-channel attacks and glitches," in *International Conference on Information and Communications Security*, pp. 529–545, Springer, 2006.

[22] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang, "Pushing the limits: a very compact and a threshold implementation of AES," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 69–88, Springer, 2011.

[23] D. Pradhan, *Fault-tolerant computer system design*. Upper Saddle River, N.J: Prentice Hall PTR, 1996.

[24] I. Koren, *Fault-tolerant systems*. Amsterdam Boston: Elsevier/Morgan Kaufmann, 2007.

[25] L. Anghel, D. Alexandrescu, and M. Nicolaidis, "Evaluation of a soft error tolerance technique based on time and/or space redundancy," in *Integrated Circuits and Systems Design, 2000. Proceedings. 13th Symposium on*, pp. 237–242, IEEE, 2000.

[26] G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "A novel parity bit scheme for SBox in AES circuits," in *Design and Diagnostics of Electronic Circuits and Systems, 2007. DDECS'07. IEEE*, pp. 1–5, IEEE, 2007.

[27] J. Emmert, C. Stroud, B. Skaggs, and M. Abramovici, "Dynamic fault tolerance in FPGAs via partial reconfiguration," in *Field-Programmable Custom Computing Machines, 2000 IEEE Symposium on*, pp. 165–174, IEEE, 2000.

[28] J. Smith, T. Xia, and C. Stroud, "An automated BIST architecture for testing and diagnosing FPGA interconnect faults," *Journal of electronic testing*, vol. 22, no. 3, pp. 239–253, 2006.

[29] A. Alaghi, M. S. Yarandi, and Z. Navabi, "An optimum ORA BIST for multiple fault FPGA look-up table testing," in *2006 15th Asian Test Symposium*, pp. 293–298, IEEE, 2006.

[30] J.-S. Coron, P. Kocher, and D. Naccache, "Statistics and secret leakage," in *International Conference on Financial Cryptography*, pp. 157–173, Springer, 2000.

[31] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 16–29, Springer, 2004.

[32] F. Regazzoni, T. Eisenbarth, L. Breveglieri, P. Ienne, and I. Koren, "Can knowledge regarding the presence of countermeasures against fault attacks simplify power attacks on cryptographic devices?," in *Defect and Fault Tolerance of VLSI Systems, 2008. DFTVS'08. IEEE International Symposium on*, pp. 202–210, IEEE, 2008.

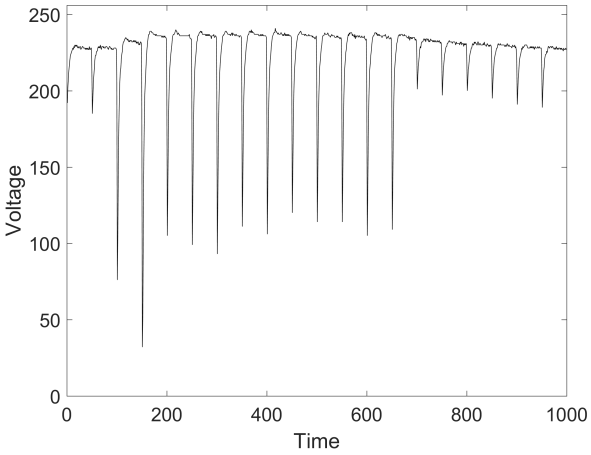
[33] F. Regazzoni, L. Breveglieri, P. Ienne, and I. Koren, "Interaction between fault attack countermeasures and the resistance against power analysis attacks," in *Fault Analysis in Cryptography*, pp. 257–272, Springer, 2012.

[34] J. Dofe, H. Pahlevanzadeh, and Q. Yu, "A Comprehensive FPGA-Based Assessment on Fault-Resistant AES against Correlation Power Analysis Attack," *Journal of Electronic Testing*, vol. 32, no. 5, pp. 611–624, 2016.

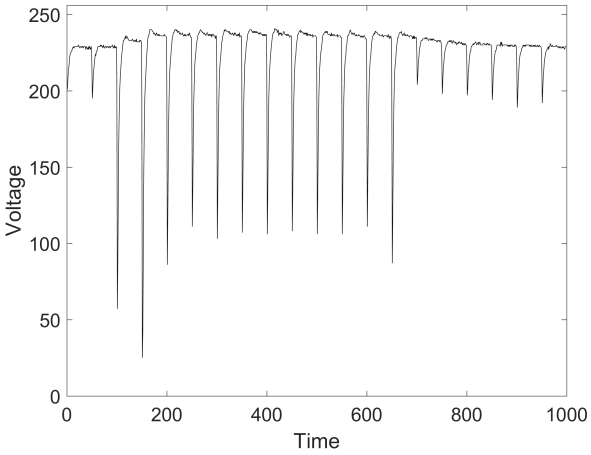
[35] V. Fischer, F. Bernard, and P. Haddad, "An open-source multi-FPGA modular system for fair benchmarking of true random number generators," in *Field Programmable Logic and Applications (FPL), 2013 23rd International Conference on*, pp. 1–4, IEEE, 2013.

[36] R. J. Serfling, *Approximation theorems of mathematical statistics*, vol. 162. John Wiley & Sons, 2009.

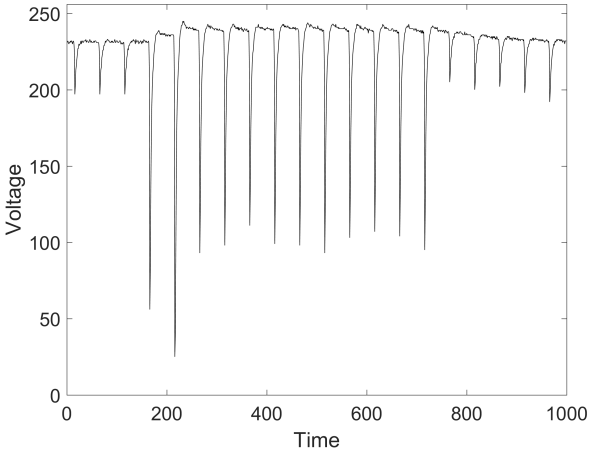
APPENDIX
ADDITIONAL PLOTS



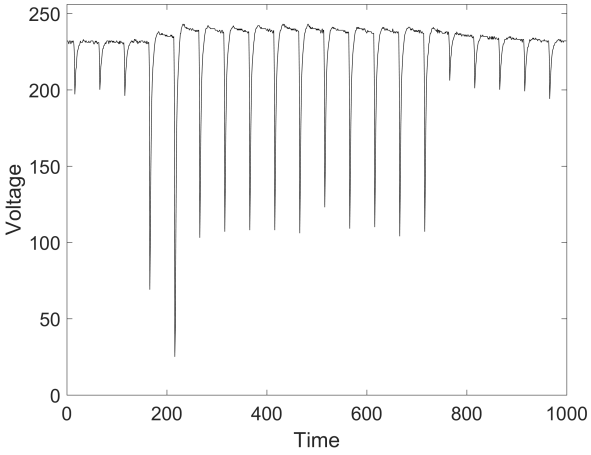
(a) Powertrace of the basic AES implementation



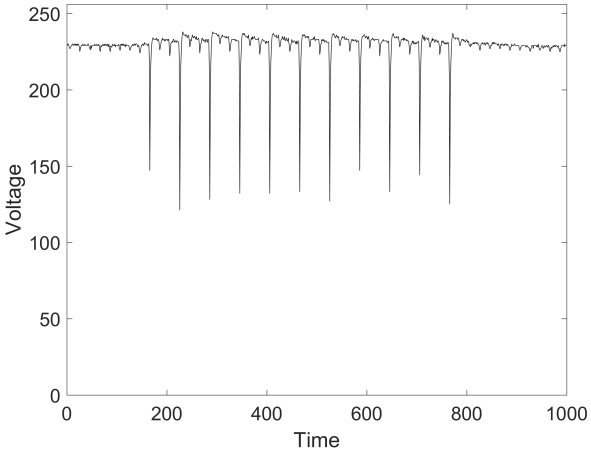
(b) Powertrace of the AES using SubBytes Parity Check



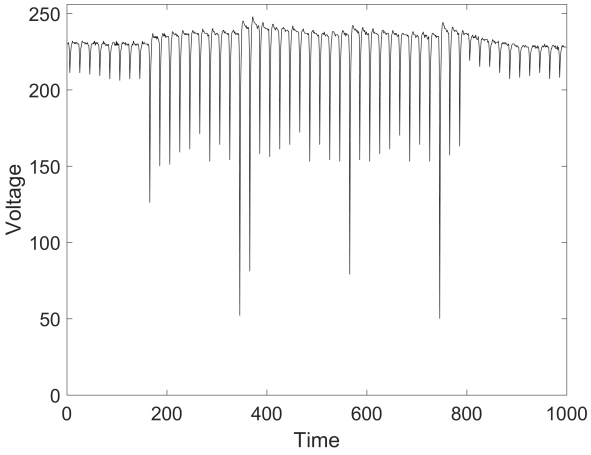
(c) Powertrace of the AES using Space Redundancy at Round level



(d) Powertrace of the AES using Space Redundancy at Algorithm level

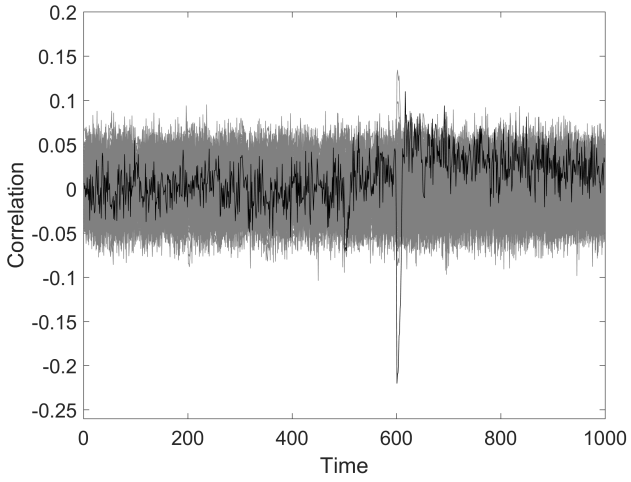


(e) Powertrace of the AES using Time Redundancy at Round level

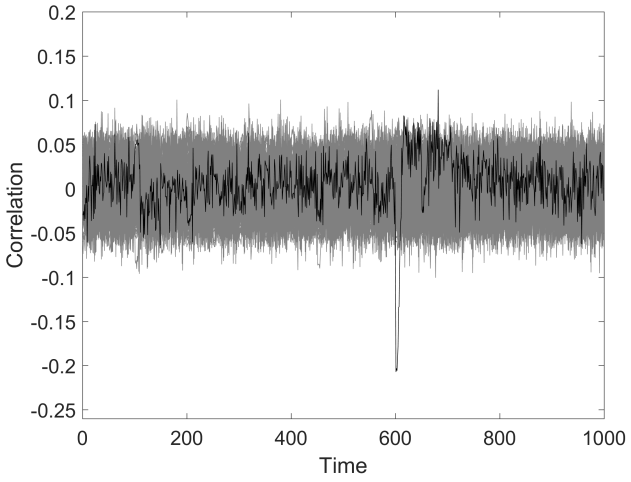


(f) Powertrace of the AES using Time Redundancy at Algorithm level

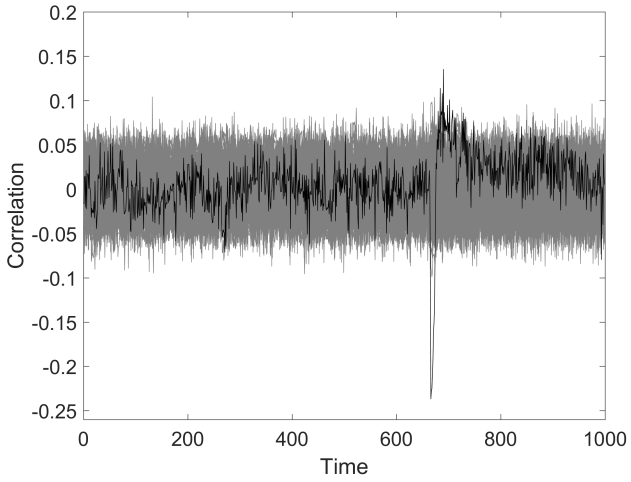
Figure 12. Powertraces of all Implemented Architectures



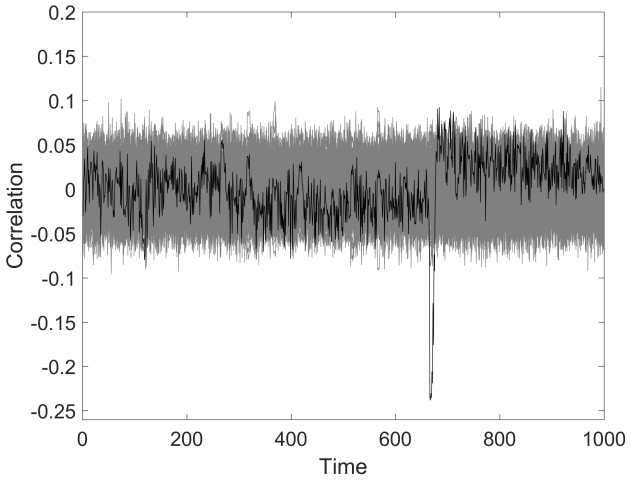
(a) Correlation plot of the basic AES implementation



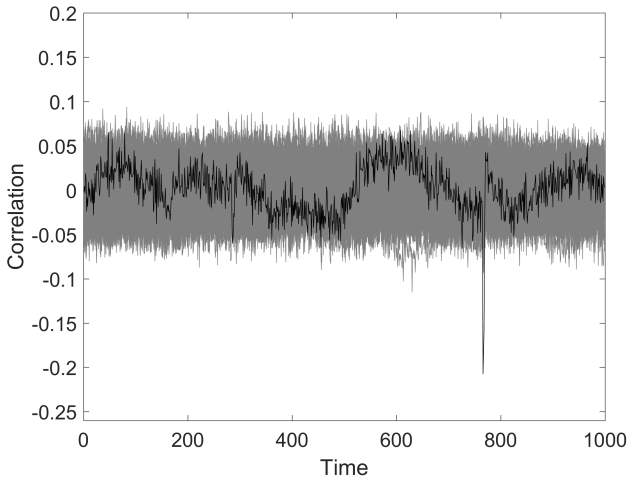
(b) Correlation plot of the AES using SubBytes Parity Check



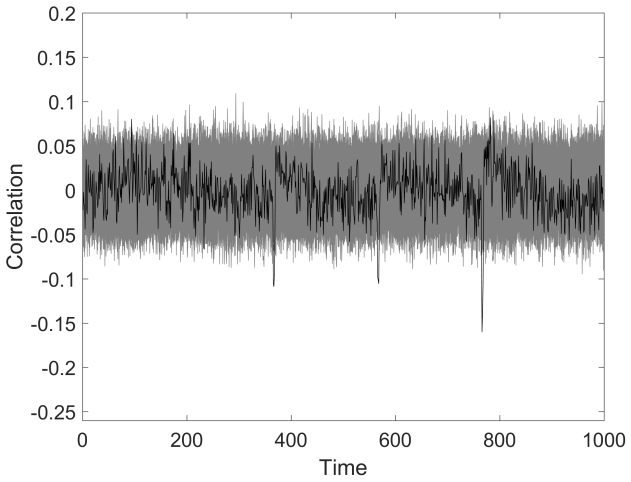
(c) Correlation plot of the AES using Space Redundancy at Round level



(d) Correlation plot of the AES using Space Redundancy at Algorithm level



(e) Correlation plot of the AES using Time Redundancy at Round level



(f) Correlation plot of the AES using Time Redundancy at Algorithm level

Figure 13. Correlation plots of all Implemented Architectures