STSM Report

REFERENCE: Short Term Scientific Mission, COST Action IC1204
Beneficiary: Martin Petrvalsky, Slovakia, martin.petrvalsky@tuke.sk
Host: Nele Mentens, Belgium, nele.mentens@kuleuven.be
Period: from 24/02/14 to 28/05/14
Place: KU Leuven, Belgium
Reference code: COST-STSM-IC1204-16890

1. Purpose of the visit

For this mission, the main focus was to investigate and describe possible attacks on Field Programmable Gate Arrays (FPGA) running cryptographic algorithms (e.g. ciphering, deciphering or digital signatures). Emphasis was on power consumption based side-channel attack, on connections between the attack and hardware/software and also on finding new information leakages on FPGAs.

Next objective of the mission was the parameters clarification of measuring devices for a successful attack and comparison of the results between measuring setups in KU Leuven and TU Kosice laboratories. The outcomes of the mission could be useful in some industrial applications – for example extremely secure devices in military or bank applications, where used resources (chip area, time, money) are not critical. It is important to know the limits of the side-channel attacks deployed on hardware level. This mission tried to clarify these limits and it suggested effective countermeasures.

The results could be used for development of specialized cryptographic hardware as a part of a project, in which our department and Slovak company Micronic specialized in cryptography participate. KU Leuven has workplace with high-end hardware specialized for side-channel attacks, which is not available in TU Kosice (FPGA boards, oscilloscope, differential probes, ...) and also there are qualified researchers in the field of the attacks with excellent results, who inspired me and helped me with my work. The results and experience gathered from the mission will help me with my further PhD research.

There is a gap between security of proposed countermeasure schemes and implementations of these schemes in current cryptography. We agreed on

realization of hardware implementation of promising scheme called *inner product masking* [1], which can defend the implementation against DPA attack. We chose AES algorithm and Altera Cyclone III DISIPA FPGA board [2] as hardware platform. The department in KU Leuven had already developed a software implementation for the 8-bit Atmel AVR ATMega128 in assembly language [3] and hardware implementation was the next logical step. Besides my host, I closely collaborated with Josep Balasch and Oscar Reparaz, who are working in area of side-channel attacks.

2. Description of the work carried out

The first task was to gain all the available information about agreed scheme and hardware [1]-[12]. I studied basic principles of masking schemes, implementation of masking schemes, higher order attacks, higher order masking schemes and their implementations. I focused on information about implementation of the inner product masking (IP masking) [3]. I also acquired available information about the hardware platform - Altera Cyclone III DISIPA FPGA board. I studied the basic differential power analysis (DPA) attack on the board, which was previously deployed in the laboratory of TU Kosice.

The next step was hardware implementation of the IP masking in VHDL for the chosen platform. We agreed that firstly I would write VHDL with purely combinatorial logic. Before realization of IP masking operations I needed to implement operations of the underlaying field - GF(2^8):

- Addition – realized with XOR gates (addition in GF(2^8) is bitwise XOR of inputs)
- Multiplication – realized using Mastrovito's multiplier [13]
- Squaring – realized using net of the XOR gates (the net was computed using properties of squaring and AES irreducible polynomial)
- Inversion – realized using subfield GF(2^4) [14]

I lately added powering to 4 and 16 in GF(2^8) for better effectiveness. The realization of the powering are the same as squaring. For every operation I created highly commented and readable VHDL code and testbench, which is used for testing implementation against precomputed results (using Matlab).

Then I implemented all the basic operation using IP masking scheme needed for AES algorithm:

- Masking

- Unmasking
- Mask refreshing
- Addition
- Addition of a constant
- Multiplication
- Multiplication of a constant
- Squaring, Powering to 4 and 16

These basic operations using IP masking scheme are closely described in [3]. We agreed that the most interesting operation in terms of side-channel attacks would be IP masked version of S-box operation so I needed to implement more complex IP masked operations in VHDL code:

- Inversion
- Affine transformation
- S-box

Similarly as for GF(2^8), I created highly commented and readable VHDL code and testbenches (which were used for testing implementation) for every IP masked operation.

After completing implementation of IP masking VHDL codes, I moved to DPA attacking the FPGA board [2]. I prepared a test measurement in order to compare measurement in two different laboratories (KU Leuven and TU Kosice). The test consisted of simple DPA attack on unmasked operation AES S-box and it was already deployed in TU Kosice before. It was necessary to develop script for measurement (for an oscilloscope control, input data sending and data verification) and script for measured data preprocessing and evaluation – all scripts were developed in Matlab.

The last work that was carried out was the leakage measurement of the implemented masked operations. We agreed that we would test masking with parameter n=2 (level of security – see [3]). IP masked squaring was chosen as a first target due to its simplicity. Various measurements were conducted. I performed first order DPA attack to make sure there are not any first order flaws. Then I deployed second order attack on original implementation of IP squaring (all shared values of masking was computed at the same time) and I also tried the second order attack on implementation, where all shares were computed at different time.

The second attacked operation was IP refreshing of mask. It was chosen because of the possible first order DPA flaw revealed in [15]. Performed attacks were similar as described for IP squaring with emphasis on the possible first order flaw. Special scripts were needed for mask refreshing. The operation needed also random data besides input data in order to refresh the mask. New protocol of data transferring on serial link was developed and applied to transmit the data correctly.

3. Description of the main results obtained

The first main result was developed and tested hardware implementation of IP masked operations. They were written in VHDL language and for Altera Cyclone III FPGA target. I developed 6 entities for underlying field GF(2^8), 12 entities for IP masking, testbenches for every entity and Matlab scripts for testing. All entities were developed using only combinatorial logic with the most complex developed operation (IP masked S-box) that used 13,202 logic elements. Therefore maximal frequency was below 10 MHz, which could not be deployed in real application. In future it will be necessary to simplify developed complex operations using registers, to adhere the temporal division of the shares of masked values and to take into the account the results of DPA measurements.

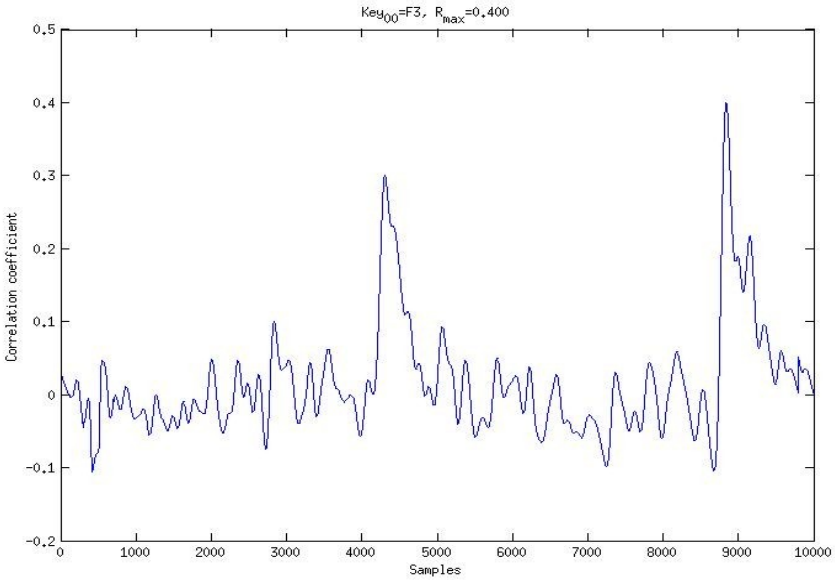

Figure 1: Correlation analysis of unprotected S-box on Altera Cyclone III FPGA board. Parameters of the measurement: sample rate 12.5 GS/s, 500 MHz band, 500 measurements with random input data. The current flow from decoupling capacitor to FPGA was measured (sensing point 4 on our evaluation board). Left peak is flaw from the S-box operation, peak on the right is leakage from writing the result to UART.

The second result was deployed DPA attack using unprotected S-box operation on our hardware platform. The first measurement was unsuccessful due to wide spectrum of the measured signal (3 GHz). We narrowed the band to 500 MHz in the second measurement. The correlation analysis of the second measurement (Fig. 1) showed two significant correlation peaks at the correct time slots and for the correct key byte (0xF3).

Main purpose of the unprotected S-box measurement was to calibrate the setup for next measurements and to compare results of the same board with equal configuration in different labs. The results shown in Fig. 1 are roughly the same compared to the results obtained in TU Kosice laboratory before (correlation value of the peak is around 0.3 to 0.4; values of the incorrect hypotheses are 0.1 to 0.2). This fact is important for the collaboration between our departments.

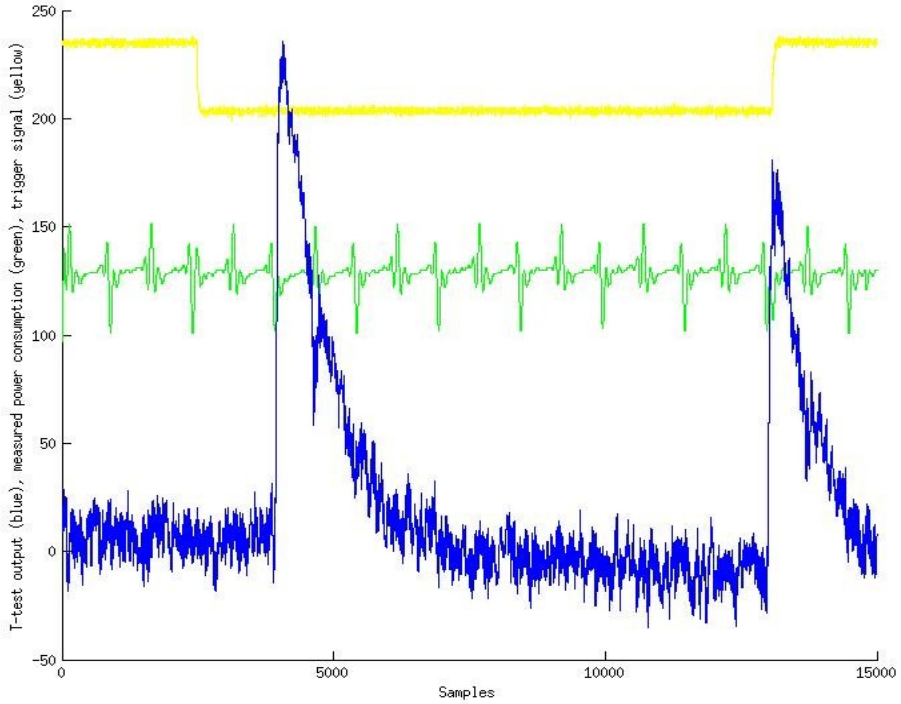

Figure 2: T-test of IP squaring (fixed 0x00 vs. random) with one input masking share fixed to value 0x00. Squaring of all shares was done simultaneously. Altera Cyclone III FPGA board was used for this measurement. Parameters of the measurement: sample rate 25 GS/s, 500 MHz band, 10,000 measurements. The current flow from decoupling capacitor to FPGA was measured (sensing point 4 on our evaluation board). Left peak is first order flaw from the IP squaring operation with fixed one share, peak on the right is leakage from writing the result to UART.

Next step was DPA attack on basic IP masked operations. Measured data was evaluated using a t-test trying to find statistically significant difference between fixed input and random input measured trace sets [16] (or fixed versus

another fixed input). Before attacking on IP masked operation I always performed measurement with one masked share fixed to zero. These measurements were done for testing if I could detect first order leakage. Example of the test measurement can be found in Fig. 2 (IP squaring with fixed share to zero).

The first measured and evaluated IP masked operation was squaring due to its simplicity. I ran various measurements of IP squaring with slightly different configurations. Introductory measurement analysis showed first order flaw during the cycle with LED toggling. It was caused by toggling input (fixed 0x00 and random) in a way that LED was toggling, which was evaluated as a leakage. LED switching was disabled and input data were chosen randomly between fixed and random. This upgrade fixed the problem with false detection.

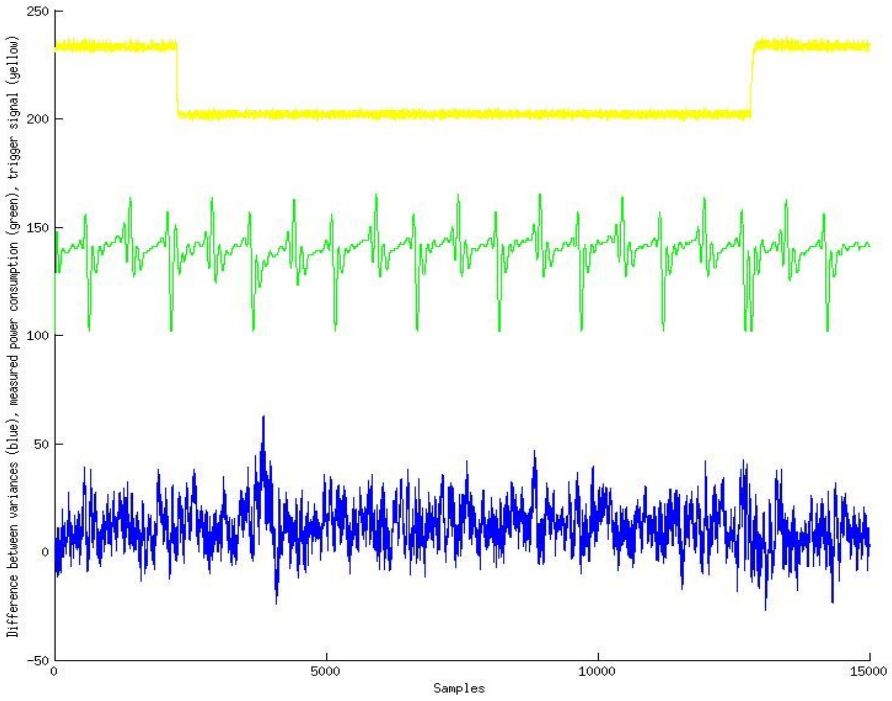

Figure 3: Analysis of difference between variances (blue graph) of two group of traces during IP squaring (all shares at the same time). First group with input 0, second group was with random input. The figure shows second order leakage univariate (in one point at the time) around sample 4,000 – at the exact point where the IP squaring was taking place – one clock cycle after trigger (yellow graph) goes to 0. Trigger was down for 7 clock cycles, which can be seen on the green graph of power consumption. Altera Cyclone III FPGA board was used. Parameters of the measurement: sample rate 25 GS/s, 500 MHz band, 45,000 measurements. The current flow from decoupling capacitor to FPGA was measured (sensing point 4 on our evaluation board).

After fixing the false detection, I run the attack on IP squaring, where all the masked shares were evaluated at the same time. First order leakage was not

detected (as expected). Then I evaluated the data for the second order attack (using second statistical moment using one leakage point in time [12]). The results showed second order flaw exactly at the point in time when the masked data was handled (Fig. 3).

Next measurement was done on IP squaring implementation with separately evaluated shares. Similarly as for the measurement before the first order DPA attack was not showing any leakages. Then I applied second order attack using first statistical moment in two separate leakage points in time (bivariate 1st order attack in [12]). This attack was not successful with the same amount of the measured traces as for univariate second order attack. This can mean that computing each share separately is more secure than computing them at the same time. In my opinion, much more traces are needed (better processing and evaluating) for the successful bivariate attack.

Last measurements were done for IP refreshing of the mask. In [15] it was theoretically proven that IP refresh scheme contains first order flaw. My task was to prove that this leakage can be measured. First, I tried to specify one share (e.g. fixed to 0x00), which produced measurable first order leakage. Then I tried purely combinatorial implementation with random shares. With 45,000 measurements I was not able to detect any first order leakage (second order univariate was, indeed, detectable because all shares were handled in the same cycle). Then I tried to artificially write the vulnerable intermediate value (according to [15]) to register in order to increase leakage (our experience was that the value leaks information if it is written to the register). Even with registered intermediate value I was not able to detect the theoretical first order flaw. We suggested that much more traces were needed for a successful attack on the vulnerable intermediate value.

4. Future collaboration with host institution (if applicable)

The Altera Cyclone III FPGA board was borrowed to the host institution and the basic information was provided to the host institution researchers. In upcoming months our departments can collaborate and work on the topic in parallel.

The rest of the developed IP masking operations on the hardware platform need to be adapted and tested for the possible leakages. Our departments can now perform the development and measurements in the future. The first task will

be to determine number of traces needed to reliably reveal the first order flaw in IP refreshing suggested in [15]. This is necessary to be sure that we can find other possible first order leakages by measurements in the future and create secure library of IP masked operations.

5. Projected publications/articles resulting or to result from the STSM

For the publication/article some of the future steps are necessary to be taken. The main issues that are needed to be solved are:

- Test and adjust all the IP masking operations that are needed for complete AES algorithm.
- Increase the efficiency (speed, area, time) of the implementation so that the IP masking library can be used in real applications (extremely secure military or bank applications).
- Solve the problem with the need of the enormous amount of randomness for the IP operations.

6. Confirmation by the host of the successful execution of the mission

The STSM was executed successfully. All objectives were accomplished. The main contributions are:

- Developed and tested hardware implementation of the IP masking operations for FPGA board.
- DPA attack measurements of unprotected S-box, which were used for calibrating the setup. The attack helped comparing two laboratory setups in KU Leuven and TU Kosice and simplified future collaboration.
- DPA attacks on basic IP masking operations with first results, which can lead to effective and secure IP masked AES implementation on a hardware (FPGA) platform.

7. References

[1] S. Dziembowski and S. Faust. Leakage-resilient circuits without computational assumptions. In R. Cramer, editor, Proceedings of TCC 2012, volume 7194 of LNCS, pages 230–247. Springer, 2012.

[2] M. Varchola, M. Drutarovsky, D. Levicky, O. Grosek, K. Nemoga, P. Zajac, M. Repka, M. Jokay, M. Vojvoda, T. Fabsic, E. Antal, V. Hromada, and L. Cechlar, „DISIPA FPGA BOARD: A Novel Hardware Platform for Power Analysis Attacks,“ Demo Night of International Conference on Reconfigurable Computing and FPGAs (ReConFig), 2013.

[3] Josep Balasch, Sebastian Faust, Benedikt Gierlichs, Ingrid Verbauwhede: Theory and Practice of a Leakage Resilient Masking Scheme. ASIACRYPT 2012. http://dx.doi.org/10.1007/978-3-642-34961-4_45

[4] Louis Goubin, Jacques Patarin: DES and Differential Power Analysis (The "Duplication" Method). CHES 1999. http://dx.doi.org/10.1007/3-540-48059-5_15

[5] Thomas S. Messerges: Securing the AES Finalists Against Power Analysis Attacks. FSE 2000. http://dx.doi.org/10.1007/3-540-44706-7_11

[6] Thomas S. Messerges: Using Second-Order Power Analysis to Attack DPA Resistant Software. CHES 2000. http://dx.doi.org/10.1007/3-540-44499-8_19

[7] Stefan Mangard, Thomas Popp, Berndt M. Gammel: Side-Channel Leakage of Masked CMOS Gates. CT-RSA 2005. http://dx.doi.org/10.1007/978-3-540-30574-3_24

[8] Stefan Mangard, Norbert Pramstaller, Elisabeth Oswald: Successfully Attacking Masked AES Hardware Implementations. CHES 2005. http://dx.doi.org/10.1007/11545262_12

[9] Matthieu Rivain, Emmanuel Prouff: Provably Secure Higher-Order Masking of AES. CHES 2010. http://dx.doi.org/10.1007/978-3-642-15031-9_28

[10] Thomas Roche, Emmanuel Prouff: Higher-order glitch free implementation of the AES using Secure Multi-Party Computation protocols - Extended version. J. Cryptographic Engineering 2(2), 2012. http://dx.doi.org/10.1007/s13389-012-0033-3

[11] Amir Moradi, Oliver Mischke: Glitch-free implementation of masking in modern FPGAs. HOST 2012.
http://dx.doi.org/10.1109/HST.2012.6224326

[12] Amir Moradi, Oliver Mischke: On the Simplicity of Converting Leakages from Multivariate to Univariate - (Case Study of a Glitch-Resistant Masking Scheme). CHES 2013.
http://dx.doi.org/10.1007/978-3-642-40349-1_1

[13] Eduardo Mastrovito: VLSI Architectures for Computations in Galois Fields. Dissertation Thesis, 1991. ISBN 91-7870-737-4

[14] E.N. Mui Practical Implementation of Rijndael S-Box Using Combinational Logic, 2007.
http://www.xess.com/static/media/projects/Rijndael_SBox.pdf

[15] Emmanuel Prouff, Matthieu Rivain, Thomas Roche: On the Practical Security of a Leakage Resilient Masking Scheme. CT-RSA 2014.nation/breakdown of how the living & travel expenses were spent.)

[16] Gilbert Goodwill, Benjamin Jun, Josh Jaffe, Pankaj Rohatgi: A testing methodology for side channel resistance validation.
http://www.cryptography.com/public/pdf/a-testing-methodology-for-side-channel-resistance-validation.pdf