STSM Project Report: Lejla Batina

ICT COST Action IC1204: Trustworthy Manufacturing and Utilization of Secure Devices

Visitor: Dr. Lejla Batina, Radboud University, Nijmegen, The Netherlands, lejla@cs.ru.nl

Host institution: Prof. Dr. Tim Güneysu, Prof. Dr. Christof Paar, RUB, Bochum, Germany

Visiting Period: October 1 – November 15, 2013.

Background:

In Nijmegen we work on various topics in physical security, mainly considering side-channel analysis and fault attacks on various platforms, including countermeasures. Our main expertize lies on the evaluation side, investigating formal and at the same time generic ways to systematically and rigorously evalute physical leakages from side-channels that are available to the adversary. We also work on the defending side finding new countermeasures that meet the tight constraints of lighweight security applications. Typical platforms to perform practical evaluations include various smart cards, with or without hardware co-processor, for example Java cards.

Planned Research:

As all physical leakages stem from certain weaknesses of implementations, there is a difference among varios physical attacks that is platform and implementation dependent (hardware or software). In Nijmegen, we have worked on fault analysis attacks on smartcard implementations. The intention for this STSM was to extend this research direction with the researchers from RUB by using an FPGA platform.

Topic 1: The first topic we had planned to work on is side-channel protection through FPGA reconfiguration. It was shown in the previous work of Mentens et al. [1] that dynamic reconfiguration can also improve the resistance of cryptographic systems against physical attacks. They introduce a new class of countermeasures that provides increased resistance, in particular against fault attacks, by randomly changing the physical location of functional blocks on the chip area at run-time.

We have decided to extend this idea into a broad concept of "Evolutionary computation on FPGAs". The goal was to pick a broad multidisciplinary topic that requires different backgrounds and on which several researchers and PhD students could collaborate. The groups involved within COST are from Nijmegen, Bochum, Leuven and Zagreb. In particular, Bochum and Leuven have a lot of expertize with FPGA platforms for cryptography and cryptanalysis. Their tasks range from new designs and the evaluations of their complexity and efficiency, partial reconfiguration and software-hardware approach for recent FPGA platforms. Researchers from Zagreb, on the other hand, work extensively on genetic algorithms for cryptography. Their contribution will be on the side of reconfiguration through evolutionary computation. For Nijmegen, a detailed analysis and security evaluation is left for a later stage of this project.

The first problem to consider is the side-channel protection of FPGAs using platform-specific

features. We have identified three approaches: 1) using Multiplexers and Flip-flops to increase the complexity of implementation options; 2) using partial reconfiguration and building on the results from [1]; 3) using hardware-software approach and adding the functionality of a microcontroller available on the FPGA platform of interest.

We have started with 1) during the STSM in Bochum. The main goal was to increase the implementation complexity to additionally complicate the task of attackers. One example of increasing this complexity is when using different implementations of the AES Sbox to increase the complexity of the attackers' tasks. Namely, it should be more difficult for the attacker to mount a successful DPA or a fault attack when an AES encryption is performed differently every time (i.e. using different computations of binary field arithmetic e.g. using tower fields of the degree extension 2 or 4). The complexity is typically measured as Signal-to-Noise (SNR) ratio for side-channel analysis [2] or by using the entropy measure introduced by F.-X. Standaert et al. [3].

Our first tasks include: adding register stages (pipelining/small additional complexity), using reconfigurable LUTs, implementing SBox in different manners e.g. tower fields implementations.

Research performed during the visit:

Together with Nele Mentens from KU Leuven we have worked on a small use-case considering pipelining within a single AES Sbox. The idea was to evaluate the impact that a certain number of pipelining stages has on the throughput. To generate all possible configurations with the register stages we are using random search algorithms for this optimization problem and the next step will benefit from genetic algorithms. After the performance evaluation we will consider the impact on side-channel security. The exploration of the solution space so far shows that there are an optimal number of stages that maximizes the performance. Our experiments so far aim at a detailed investigation for a few small (but fixed) numbers of stages. Therefore, to have a complete design space exploration and comprehensive results accordingly, will take a few more months. The first results of our research will be submitted to the IEEE HOST symposium.

Future work:

Future directions will involve several researchers from the four research groups where we plan to experiment with different options outlined above. Especially, due to the rich equipment in our hardware security lab in Nijmegen, we will be intensively engaged in the evaluation phase for each implementation and architectural option. Together with the group from Zagreb we will also work on the generation of possible solutions using evolutionary computation. The amount of work planned will be submitted to several conferences and journals. Finally, PhD students involved will continue with the joint work, visiting each other and learning from different expertizes of the groups involved. We detail the steps to follow in the sequence.

The next step is to evaluate all the hardware options using Multiplexers and Flip-flops. In addition to pipelining and composite field arithmetic we plan to use reconfigurable LUTs as implementation options. This is ongoing work performed separately in Bochum and Leuven (different implementation options) after which side-channel evaluation will follow in Nijmegen. The intention is to find the best approach and the best trade-off in terms of costs and security.

As mentioned above, evolutionary computation will be used to find optimal solutions. The challenge for this task is in finding suitable cost functions and representations of hardware implementations such that e.g. genetic algorithms can search for "good" solutions. Our strategy includes regular Skype meetings and discussions with all the partners involved. Also, a few more STSM should follow this line research.

Topic 2: Another topic follows up on the recent work of several COST partners (RU Nijmegen, RU Bochum and KU Leuven) [4] and it considers implementations with hardware resource restrictions and ultra-low power implementations of cryptographic primitives. In this work we give comprehensive area, power and energy analysis of the most recently developed lightweight block ciphers and we compare them to the standard AES algorithm. Our evaluation method consists of: (1) calculating the toggle count of the internal nodes of the implementation and (2) estimating the pre-layout power consumption and the derived energy using Cadence Encounter RTL Compiler and ModelSIM simulations. The idea behind is using the fact that most of the power consumed in a CMOS circuits stems from dynamic power. In the paper published at RFIDSec13 we show that the area is not always correlated to the power and energy consumption, which is of importance for mobile battery-fed devices. Our next goal is to investigate the relation between the number of toggles from an HDL implementation and power reports from synthesis. In this way we could verify the validity of our approach i.e. the model used for power consumption and set new items for the research agenda.

Research performed during the visit:

We have discussed the results obtained in [4] and we have also identified a few errors and inconsistencies. The correct report is available online [5]. Future plans include experimenting with the GEZEL platform and discussing the possibilities of getting power consumption reports from this tool making the design exploration in this way even more low-power oriented. Concrete steps would include implementing all lightweight block ciphers in GEZEL and comparing the results. More precisely, our model is based on the switching activity as the most dominant factor for power consumption but this is somewhat limited. In particular, the impact of technology scaling (assuming that the contribution from leakage power becomes substantial) should be also considered.

[1] Nele Mentens, Benedikt Gierlichs, Ingrid Verbauwhede. "Power and Fault Analysis Resistance in Hardware through Dynamic Reconfiguration". CHES 2008: 346-362.

[2] Stefan Mangard. "Hardware Countermeasures against DPA ? A Statistical Analysis of Their Effectiveness". CT-RSA 2004: 222-235

[3] François-Xavier Standaert, Tal Malkin, Moti Yung. "A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks". EUROCRYPT 2009: 443-461

[4] Lejla Batina, Amitabh Das, Baris Ege, Elif Bilge Kavun, Nele Mentens, Christof Paar, Ingrid Verbauwhede and Tolga Yalcin. "Dietary Recommendations for Lightweight Block Ciphers: Power, Energy and Area Analysis of Recently Developed Architectures", RFIDSec13, July 9-11, Graz, Austria.

[5] Lejla Batina, Amitabh Das, Baris Ege, Elif Bilge Kavun, Nele Mentens, Christof Paar, Ingrid

Verbauwhede and Tolga Yalcin. “Dietary Recommendations for Lightweight Block Ciphers: Power, Energy and Area Analysis of Recently Developed Architectures”, Cryptology ePrint Archive: Report 2013/753.