Report for a Short Term Scientific Mission (STSM), Zagreb
Project
ICT COST Action IC1204: Trustworthy Manufacturing and Utilization of Secure Devices
Involved Institutions
Home institution: Stjepan Picek, Radboud University, Nijmegen, The Netherlands
Host institution: Marin Golub, Faculty of Electrical Engineering and Computing (FER), Zagreb, Croatia

Visit Details
Visiting Researcher: Stjepan Picek
Visiting Period: February 24 – March 24, 2014.

Report Statement

During my visit to FER I worked on several projects that relate to the activities of COST action working groups. More specifically, projects related with groups WG3 - Fault attack detection and protection, WG4 - Reconfigurable devices for secure functions and WG5 - Validation, Evaluation, and Fault Injection.

Improvements of side channel resistance of nonlinear elements of stream and block ciphers

First project deals with the improvements of side channel resistance of nonlinear elements of stream and block ciphers. Increase in DPA resistance can be obtained by changing current nonlinear elements with those that have better transparency order property. Transparency order property defines the resistance of S-boxes to DPA attacks. As presented in [1], our results confirm there is an increase in the number of needed traces when S-box with better transparency order is used. For the 8x8 case, we succeeded in lowering transparency order from 7.86 (AES case) to 7.35 which is as far as we know current lowest transparency order result for S-box of that size.

After working on 8x8 case, when I arrived to FER we continued to conduct the research for the 4x4 case as well as for Boolean functions.

When considering 4x4 case, we found S-boxes that belong to the optimal S-boxes classification (they have best set of properties to protect against linear and differential cryptanalysis) but with better DPA resistance. In accordance with that, we conducted experiments with the PRESENT algorithm (comparing original PRESENT S-box and our evolved S-box) and we found that our new S-box has better DPA resistance. From cryptographic properties perspective, we lowered transparency order from 3.53 (PRESENT) to 3.2 value while keeping nonlinearity and delta uniformity at the maximal value of 4. Furthermore, we showed that S-boxes are not affine invariant when considering transparency order or SNR (DPA) properties (properties related with side channel resistance). Results of those experiments will be presented at the HOST conference [3]. Our

experiments showed that even the simplest affine transformation (adding a constant) can result in the change of SNR (DPA) but to change the transparency order value one needs to perform at least two multiplications with invertible matrices as well as adding two constants in between.

To be able to conduct experiments in a more statistically sound way, we implemented guessing entropy metrics. On the basis of the guessing entropy for the PRESENT algorithm we see that there is increase in the needed number of traces of around 50 to 70%. During my visit we conducted experiments with guessing entropy measure to confirm our previous findings.

When considering Boolean functions, we conducted experiments with several evolutionary computation methods to find 8x1 Boolean functions that have high nonlinearity and low transparency order. We succeeded in finding Boolean functions with lower transparency values than it was previously known. Results are submitted for publication [4, 5].

Submission [4] is entirely the result of the experiments and work at FER.

When looking in Booolean functions with maximum known nonlinearity (116), we succeeded in lowering transparency order from 0.97 to 0.96 and for level 112 from 0.95 to 0.92. Since in Boolean functions the effect of transparency order is weakened by only one output variable we believe that our results represent improvement.

We plan to continue working on this topic where we are now interested in applying multiobjective evolutionary algorithms. Additionally, we plan to compare transparency order property with a newer property that also relates to DPA resistance.

To be able to conduct experiments we needed to develop tool that is able to calculate different properties of Boolean functions and S-boxes. That research is submitted for publication [6]. This tool is capable to analyze nonlinear elements (Boolean functions and S-boxes) of various input and output sizes. Furthermore, this tool is more extensive in its capabilities (number of cryptographic properties) than any other publicly available tool. Some of the capabilities of the tool were implemented during the stay and we continue to add new options to the tool.

Finding faults in smartcards

Second topic deals with methods for finding faults in smartcards and is continuation of work as presented in [2]. Finding faults that can lead to a successful attack is a difficult problem that often takes too much time when using random search. Therefore, we have used directed random search methods – GA. As the first improvement when regarding the speed of search, we added a mechanism for recognizing and avoiding already visited points in the search space. More detailed analysis and experimental work will be presented at the MIPRO conference [7]. In this work we succeeded in finding multiple success points with less than 1500 measurements when random search method even with the twice the amount of traces in average cannot find any success points. Furthermore, we developed new algorithm that combines GA and a local search method – the

memetic algorithm. This algorithm starts as a conventional GA but when arrives in the area that can have successful fault parameters (as recognized by the change of the solution class) than it activates a local search component. This component searches the surrounding space and whenever it locates new interesting point it halves the diameter of the search to find the best set of parameters in the minimum amount of time. Initial simulations are encouraging and now we plan to run new sets of experiments with different targets of evaluation. The work on the memetic algorithm was done during the stay.

Additionally, we started to work on the adaptation of the algorithm so it can be used in electromagnetic fault injection (EMFI) and optical fault injection settings.

Combinational logic circuit: higher throughput by adding pipelining

Third topic deals with the evolving of combinational logic circuit. We are interested in making higher throughput by adding pipelining. Since this is difficult problem and we work on novel implementation the project consists of several parts.

In first part we developed parser that takes Verilog netlist and transforms it into a more appropriate form for evolutionary algorithms to use (first version of parser was done before my stay). After that we developed simulator that transforms parsed list into internal representation that can be used by the evolutionary algorithm.

For the evolutionary algorithm we selected genetic algorithms and genetic annealing.

First tests were done on small simulated lists. Our experiments showed the algorithm works but is very slow. Since the first algorithm used recursive approach we decided to implement an iterative algorithm. Further experiments with new, improved version of the algorithm suggest that the algorithm is fast enough for the practical purposes. Currently, we are preparing the environment to conduct experiments with AES S-box that is realized in composite field arithmetic.

[1] Stjepan Picek, Baris Ege, Lejla Batina, Domagoj Jakobovic, Lukasz Chmielewski and Marin Golub. ”On Using Genetic Algorithms for Intrinsic Side-Channel Resistance: The Case of AES S-Box”. Proceedings of the First Workshop on Cryptography and Security in Computing Systems, Vienna, Austria. Pages 13-18.

[2] Rafael Boix Carpi, Stjepan Picek, Lejla Batina, Federico Menarini, Domagoj Jakobovic and Marin Golub. “Glitch it if you can: Novel parameter search strategies for successful fault injection”, appeared at CARDIS 2013, November 27-29, Berlin, Germany.

[3] Stjepan Picek, Baris Ege, Lejla Batina, Domagoj Jakobovic and Kostas Papagiannopoulos. Optimality and Beyond: The Case of 4x4 S-boxes. Accepted for publication, HOST 2014 Symposium, Washington, USA.

[4] Stjepan Picek, Elena Marchiori, Lejla Batina and Domagoj Jakobovic . Combining Evolutionary Computation and Algebraic Constructions to find Cryptography-relevant Boolean Functions. Submitted for publication.

[5] Stjepan Picek, Lejla Batina and Domagoj Jakobovic. Evolving DPA-resistant Boolean Functions. Submitted for publication.

[6] Stjepan Picek, Lejla Batina, Domagoj Jakobovic, Baris Ege and Marin Golub. S-box, SET, Match: A Toolbox for S-box Analysis. Accepted for publication, WISTP 2014, Heraklion, Greece.

[7] Stjepan Picek, Domagoj Jakobovic, Lejla Batina, Rafael Boix Carpi. Evolving genetic algorithms for fault injection attacks. Accepted for publication, MIPRO 20014, Opatija, Croatia.