June 9, 2014

Yaara Neumeier, Faculty of Engineering, Bar-Ilan University

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

STSM Scientific Report

Design and Evaluation of High Rate Robust Codes

Summary:

Cryptographic primitives are vulnerable to fault injection attacks [Polian13]. Robust non-linear error detecting codes have been shown to be an efficient countermeasure against these attacks. There are only two high-rate robust codes: the Quadratic-Sum (QS) code [Karpovsky07] and the Punctured-Cubic (PC) code [Neumeier12]. All other known high-rate codes are not robust; that is, there are errors, which are never detected by these codes. The QS and the PC codes are optimal for protecting memories; however, as shown in [Tomashevich12] and [Shumsky13], performance of these codes degrades and may even fail altogether when applied to real designs of cryptographic modules and Final State Machines (FSMs).

The purpose of this STSM was to evaluate the ability of high rate robust codes to protect real hardware from fault injection attacks.
The goal of this STSM was to establish a synthesis flow, evaluate the area overhead, performance, and power consumption of circuits protected by high rate robust codes.

My STSM host, Prof. Polian's team in Passau, has the equipment, synthesis tools, and vast experience in the synthesis of circuits that implement cryptographic functions such as encryption and decryption, and Dr. Keren's team in Bar-Ilan has experience in the development of high rate codes with specific parameters. During the visit I worked together with Victor Tomashevich (a Ph.D. student in Passau) on the low cost implementation and embedding of shortened Quadratic-Sum codes [Pesso13] and Punctured-Cubic codes into the Polian's team's designs, and together we started to define test and evaluation procedures for these codes.

The results obtained during the STSM, along with results from previous experiments were submitted as a paper to the DFTS conference (the paper is attached).

Overview:

In this STSM, we used the hardware implementation of the new lightweight cipher PRINCE [Borghoff12] and its sub-blocks to study the impact of different error detecting codes on the true fault detection probability. Moreover, we specifically considered fault injections in particular locations that lead to an actual fault-based attack [Jovanovic12].

Prior to the visit, Victor Tomashevich constructed an FPGA-based fault injection infrastructure. To evaluate the fault detection abilities of high rate robust codes on practical devices, we designed and implemented predictors and checkers for the PRINCE cypher and its sub-blocks. We implemented the QS and the PC codes for different code parameters, and compared the results to those of linear codes.

To evaluate the efficiency of the implemented codes we used a fault injection campaign. The injection campaign included injection of all the possible single faults (with respect to 10000 different random inputs), 10000 random double-faults and 10000 random multiple-faults. We also considered a list of exploitable faults, which are used in practical fault attacks.

Experimental Results:

The fault detection abilities of linear (non-robust) codes and the robust QS and PC codes for several parameters were evaluated and compared. Robust codes, and in particular PC exhibited better protection against attackers that can choose a specific fault pattern (the worst scenario).

The results were evaluated using the Attack Success Rate (ASR), which is defined for a given fault as the ratio between the number of inputs that the fault did not detect in their presence, and the total number of inputs, that is, ASR is the probability that a given fault is not detected.

The results indicate that, although the average ASR (over all injected faults) for robust codes was similar to the ASR for linear codes with the same rate, linear codes have many undetected faults, and robust codes have no undetected faults (or very few undetected faults). In this sense, the PC code performed better than the QS code. Moreover, as the redundancy increased, the maximal ASR for the robust codes decreased. This result indicates that robust codes provide better security in terms of the worst case (a case where an attacker can choose a specific fault). The detailed results are presented in our paper (attached).

Conclusions:

In this STSM we established a synthesis flow for the evaluation of circuits protected by high rate robust codes. Robust codes were shown to provide better security against worst-case scenarios and also exhibited a good match with theoretical information-level predictions.

Future work will concentrate on:

- Improving the area overhead, latency, performance and power consumptions of the implementations.
- Characterizing faults that were undetected using these codes.
- Defining an error model that characterizes the injected faults in a real system.
- Construction and implementation of codes that detect malicious attacks and correct random transient faults.
- Designing codes for non-uniform distributions of information words.

It is expected that this STSM will pave the way for a fruitful collaboration between the two research groups.

References:

[Karpovsky07] M. G. Karpovsky, K. J. Kulikowski, and Z. Wang, “Robust error detection in communication and computation channels,” Int’l Workshop on Spectral Techniques, 2007.

[Neumeier12] Y. Neumeier, O. Keren, “Punctured Karpovsky-Taubin binary robust error detecting codes for cryptographic devices,” Proc. IEEE Int’l On-Line Test Symp., 2012.

[Pesso13] Barenghi Y. Pesso, Y. Neumeier and O. Keren, "Efficient Implementation of Checkers for Punctured Cubic Codes", Trustworthy Manufacturing and Utilization of Secure Devices workshop, Freiburg, Dec. 2013.

[Polian13] I. Polian and M. Kreuzer, “Fault-based attacks on cryptographic hardware,” Proc. IEEE Int'l Symp. on Design and Diagnostics of Electronic Circuits and Systems, 2013.

[Shumsky13] I. Shumsky and O. Keren, "Security-Oriented State Assignment", TRUDEVICE, The 1st Workshop on Trustworthy Manufacturing and Utilization of Secure Devices, 2013.

[Tomashevich12] V. Tomashevich, S. Srinivasan, F. Foerg, and I. Polian, “Cross-level protection of circuits against faults and malicious attacks,” Proc. IEEE Int'l On-Line Test Symp., 2012.

[Borghoff12] J. Borghoff et al., “PRINCE: A low-latency block cipher for pervasive computing applications,” in ASIACRYPT, 2012.

[Jovanovic12] P. Jovanovic, M. Kreuzer, and I. Polian, “Multi-Stage Fault Attacks on Block Ciphers,” Cryptology ePrint Archive, Report 2013/778, 2013.