Chair of Applied Cryptography
Prof. Sebastian Faust

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Bachelor / Master's thesis proposal

Faults vs LWR (Learning with Rounding)

An adversary may exploit in many ways the fact that she has physical access to a device performing cryptographic computations. This may result, for example, in retrieving the key used by the device. For example, exploiting his access to the device, she may *inject faults*. That is, she changes one (or more) partial value during the computations. In some cases, these kind of attacks are very powerful [**?**].
There have countless many works studying fault attacks against block ciphers [**?**], but less against other primitives. For this thesis, we will explore faults against schemes based on Learning with Roundings (LWR) [**?**]. In fact, there is an interest in new primitives which are key-homomorphic (or almost), because they are much easier to mask, thus, they are easier to protect against side-channel attacks (another class of physical attacks). Examples of these new primitives are Learning Parity with Noise (LPN) and LWR [**?**].
At Cardis 2016, Berti et al. [1] proved that LPN is resistant against fault attacks. In particular they designed some attacks and showed that these attacks were the most efficient ones. Their results were confirmed by a software simulation of the attack.

The main goal of this thesis is to prove that LWR is resistant against fault attacks. In particular the goal is to implement the software simulation of some attacks against LWR.

The following main steps are planned as part of the thesis work:

1. Understanding LWR and the attacks proposed
2. Implement a software simulation of the attack (the software may be chosen by the student)
3. For a good master thesis you are asked to extend these attacks to other constructions, for example Learning with Errors (LWE) [**?**]

There is the possibility to write a scientific paper from an excellent thesis.

Prerequisites:

- knowledge of linear algebra over finite fields and knowledge of finite rings
- good programming skills [C, Matlab or Python]
- a background in cryptography is helpful but it is not necessary
- good grades
- good working knowledge of written/oral English

If you are interested please send a short motivation 5-10 sentences and a transcript to the address given below.

Contact:

Dr. Francesco Berti, S2|20, 313
francesco.berti@tu-darmstadt.de

References

[1] F. Berti and F. Standaert. An analysis of the learning parity with noise assumption against fault attacks. In K. Lemke-Rust and M. Tunstall, editors, *Smart Card Research and Advanced Applications - 15th International Conference, CARDIS 2016, Cannes, France, November 7-9, 2016, Revised Selected Papers*, volume 10146 of *Lecture Notes in Computer Science*, pages 245–264. Springer, 2016.

[2] S. Dziembowski, S. Faust, G. Herold, A. Journault, D. Masny, and F. Standaert. Towards sound fresh re-keying with hard (physical) learning problems. In M. Robshaw and J. Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 272–301. Springer, 2016.

[3] G. Piret and J. Quisquater. A differential fault attack technique against SPN structures, with application to the AES and KHAZAD. In C. D. Walter, Ç. K. Koç, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2003, 5th International Workshop, Cologne, Germany, September 8-10, 2003, Proceedings*, volume 2779 of *Lecture Notes in Computer Science*, pages 77–88. Springer, 2003.

[4] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, 2009.