Chair of Applied Cryptography
Prof. Sebastian Faust

Technische
Universität
Darmstadt

Master's thesis proposal

Efficient Cryptographic Schemes secure against real Side-Channel-Attacks

Side-channel-attacks can have substantial security implications in the real world. Classical cryptography often uses the black box model for security proofs. Since the Adversary can often learn more than only the input and output of cryptographic schemes, it is essential to analyze such schemes' leakage. These leakages depend on many influencing factors such as Hardware and Program Code. Therefore we build the tool scVerif to verify the side-channel leakage of an implemented code in cooperation with NXP [1].

The main goals of this thesis are to find a cryptographic scheme secure against side-channel-attacks and to apply/improve the results given in [1].

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

1. The thesis aims to implement a cryptographic scheme that is secure against side-channel attacks described in [1].
2. The student can use the tool scVerif to verify the leakages of his implemented scheme and improve his implementation with the optimization techniques described in [1]
3. Afterward, there is the possibility to verify the results with real measurements in cooperation with NXP.
4. Additional work for a good thesis:
   - Improve the techniques to find new optimization techniques.
   - The student can analyze his achievements with real measurements and try to find leakages not covered by the leakage model in [1].

Prerequisites:

- Background in cryptography
- Good grades
- Good working knowledge of written/oral English

If you are interested please send a mail with a transcript to the address given below.

Contact:

Maximilian Orlt, S2|20, 313
maximilian.orlt@tu-darmstadt.de

References

[1] G. Barthe, M. Gourjon, B. Gregoire, M. Orlt, C. Paglialonga, and L. Porth. Masking in fine-grained leakage models: Construction, implementation and verification. Cryptology ePrint Archive, Report 2020/603, 2020. https://eprint.iacr.org/2020/603.