Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Bachelor's Thesis

Implementation and evaluation of masked cryptography on an industrial microcontroller by means of formal methods (AISEC)

Implementing cryptographic algorithms in hardware or software requires special care. With side-channel attacks, an attacker can extract sensitive information. Masking [1] is an established countermeasure to harden implementations against these attacks by splitting secret information into shares and “masking” these shares with random data. However, implementing masking is a tedious and error-prone task, as it requires keeping all masked shares separated in a circuit. Recent works have shown how formal verification can prove the security of masked hardware [2] and software [3] implementations. Applying these tools to more complex implementations or FPGAs is an active research topic.
Depending on your skill set and interest, you can focus on either hardware or software implementations. Within this research, practical and theoretical topics for either a bachelor or master thesis, or a research internship are available. This work can be conducted in German or in English.

Prerequisites

* Experience with Python
* For focus on hardware implementations: (System) Verilog or VHDL
* For focus on software implementations: C and Assembly (ARM/RISC-V)
* Basic understanding of cryptographic algorithms (e.g. AES) and side-channel attacks
* Optional: Knowledge on masking

Contact

Please send an email with:
* A short CV
* Your last grading sheet
* 3-5 dates, which fit to your schedule, for a meeting.
* Whether you are interested in a master/bachelor thesis, or a research internship and masking in software or hardware
Felix Oberhansl,

felix.oberhansl@aisec.fraunhofer.de

[1] Suresh Chari, Charanjit S Jutla, Josyula R Rao, and Pankaj Rohatgi. Towards sound approaches to counteract power-analysis attacks. In Annual International Cryptology Conference. Springer, 1999
[2] David Knichel, Pascal Sasdrich, and Amir Moradi. SILVER – Statistical Independence and Leakage Verification. In IACR ASIACRYPT-2020. Springer, 2020
[3] Gilles Barthe, Marc Gourjon, Benjamin Grègoire, Maximilian Orlt, Clara Paglialonga, and Lars Porth. Masking in Fine-Grained Leakage Models: Construction, Implementation and Verification. In TCHES-2021. 2021

Advisors

Georg Sigl
Felix Oberhansl (Fraunhofer AISEC)