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

Forschungspraxis, Assistant (Student), Master's Thesis, Bachelor's Thesis

Machine Learning in Side-Channel Analysis (AISEC)

Utilizing statistical techniques, side-channel analysis exploits information that a cryptographic device is leaking. Possible sources of this leakage are electromagnetic or power side-channel traces. Machine learning based side-channel analysis extends the statistical toolbox with Neural Networks, Belief Propagation or different methods of this field to recombine and exploit leakage.

In collaboration with the Technical University of Munich, the Fraunhofer AISEC's hardware security department offers a variety of open positions in this field. Depending on your strengths, we provide both pure software-based and practical hardware topics, such as the following:

- Trace analysis using explainable machine learning
- Leakage recombination using belief propagation - light-weight or post-quantum algorithms
- Belief propagation performance optimization using GPUs
- Pattern-based triggering using software-defined radios

On request, other topics can be offered.

Prerequisites

- Programming skills, at least one language (Python, C, Rust)
- Interest in hardware security
- Basic Linux skills

Contact

Emanuele Strieder
Telefon: +49 89 322-9986-140
E-Mail: emanuele.strieder@aisec.fraunhofer.de

Fraunhofer Research Institution for Applied and Integrated Security (AISEC)
Department Hardware Security
Parkring 4, 85748 Garching (near Munich), Germany
https://www.aisec.fraunhofer.de

Advisors

Georg Sigl
Emanuele Strieder (Fraunhofer AISEC)