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

Forschungspraxis, Master's Thesis

Shining a Light onto Obfuscation

Hardware obfuscation gains more and more attention in the area of IP protection. It is used to prevent IP overproduction, IP theft or counterfeiting. A special case of hardware obfuscation on gate-level netlists is sequential obfuscation which targets memory elements in a circuit [1] or the finite state machine structure [2].

The aim of this work is to improve and enhance sequential hardware obfuscation.

Please contact me to get more information about the topic and the aim of this work.

Reference:

- [1] Karmakar, Rajit, Santanu Chatopadhyay, and Rohit Kapur. "Encrypt flip-flop: A novel logic encryption technique for sequential circuits." arXiv preprint arXiv:1801.04961 (2018).
- [2] Chakraborty, Rajat Subhra, and Swarup Bhunia. "HARPOON: An obfuscation-based SoC design methodology for hardware protection." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 28.10 (2009): 1493-1502.

Prerequisites

- Basic knowledge in Python
- Basic knowledge in Verilog or VHDL

Contact

Michaela Brunner, M.Sc.

Technical University of Munich, Chair of Security in Information Technology

Room N1008, Email: michaela.brunner@tum.de

Advisors

Michaela Brunner