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

Forschungspraxis, Master's Thesis

Flip-Flop Classification - in a New Light

The aim of sequential netlist reverse engineering is to extract the control logic out of a given design netlist. In order to derive this information, first, the existing flip-flops have to be classified into state flip-flops which belong to the control logic and data flip-flops. Based on the correctly classified state flip-flops the control logic can be extracted in form of a finite state machine. There exist already a number of different state flip-flop identification methods which use various strategies for classification [1] [2].

The aim of this work is to improve and enhance flip-flop classification.

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

Reference:

- [1] Brunner, Michaela, Johanna Baehr, and Georg Sigl. "Improving on state register identification in sequential hardware reverse engineering." 2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 2019.
- [2] Fyrbiak, Marc, et al. "On the difficulty of fsm-based hardware obfuscation." IACR Transactions on Cryptographic Hardware and Embedded Systems (2018): 293-330.

Prerequisites

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

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