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

Bachelor's Thesis

Hardware Trojan Detection based on Controllability and Observability

In a world of multinational production chains, Hardware Trojans inserted by untrusted third parties are an emerging threat for the security of integrated circuits. Current Hardware Trojan detection methods focus on unrealistically small designs.

In this thesis, you will implement the COTD-Analysis Method for Hardware Trojan Reverse Engineering [1] and check the feasibility of this approach for real-world Trojan examples.

[1] H. Salmani, "COTD: Reference-Free Hardware Trojan Detection and Recovery Based on Controllability and Observability in Gate-Level Netlist," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 2, pp. 338-350, Feb. 2017.

Prerequisites

The following list of prerequisites is neither complete nor binding, but shall give you an idea, what the topic is about.

- Sufficient knowledge in a High-Level Programming language such as python, c, c++, rust, perl, etc. to implement the method and analyze the results
- Basic to intermediate knowledge of a hardware description languages (HDLs) such as vhdl or verilog, as the design under test is given in a HDL.

Contact

If you are interested in this topic, don't hesitate to ask for details via

alex.hepp@tum.de

Please include a grade report and a CV, so I can evaluate different focus areas to fit your experience.

Advisors

Alexander Hepp