Lehrstuhl für Sicherheit
in der Informationstechnik

24. November 2014

MA:

Static Timing Analysis for Glitch Detection

Static timing analysis is a well known step during logic synthesis. Most research focuses on using the results of this analysis for optimizing the maximum clock frequency where the output is still logically correct. That means all setup and hold time constrains must be fulfilled and glitches may only occur before the setup time and after the hold time.

Although such glitches have no influence on the logically correct behavior of the circuit and can only be observed in a slightly higher power consumption, they may temporally unmask masked signals or be exploitable in side channel attacks.

Today's analysis techniques of such glitches are mainly simulation based approaches. The task of this Master's Thesis is to transfer the principles of the static timing analysis to glitch detection.

The individual task are:

- Creating an interface to an existing (open source) timing analysis tool
- Automatic worst-case analysis
- Evaluating whether a certain glitch is critical in terms of side channel leakage
- *optional: Giving suggestion how to minimize the glitches (or even automatically reorder the circuit)*

Requirements:

- Outstanding C/C++ skills
- Good understanding of the digital synthesis flow (background in EDA preferred)
- Basic knowledge on structural verilog (or vhdl)
- Basic knowledge in DPA

If you are interested, please send your application to:

Technische Universität München
Lehrstuhl für Sicherheit in der Informationstechnik
Michael Tempelmeier
Arcisstraße 21
80333 München
oder per Email: michael.tempelmeier@tum.de

Visit us on the internet at: http://www.sec.ei.tum.de/