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

Seminar

High Level Synthesis for Security

High Level Synthesis (HLS) is an approach to generate HW accelerators from algorithmic descriptions written in a programming language like C or C++. This increases productivity because a designer has not to deal with low level RTL design. However, this layer of abstraction can lead to unwanted effects like higher area consumption or critical implications with respect to securtiy.

The goal of this work is to compare the design quality of HLS designs with direct RTL implementations. The comparison should include subjects like resource consumption, performance and side-channel resistance.

Resources:

- https://www.xilinx.com/products/design-tools/vivado/integration/esl-design.html
- L. Zhang et al., "Examining the consequences of high-level synthesis optimizations on power side-channel," 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, 2018, pp. 1167-1170, doi: 10.23919/DATE.2018.8342189.

Contact

Request Topic

Advisors

Patrick Karl