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

Seminar

Protecting Cloud FPGAs against a Malicious Cloud Provider

FPGAs are becoming a commonly used platforms in cloud environments which lead to the emergence of the FPGA-as-a-service computation paradigm. In such a scenario, it is vital to protect the bitstream from an untrusted cloud provider, such that it cannot steal intellectual properties contained in the customer design and prevent the insertion of trojans inside a design. This seminar should present the mechanisms suggested by the research community to address these two issues and put them in perspective with what commercial cloud providers are currently offering.

References

[1] C.Jin et al., **Security of Cloud FPGAs: A Survey,** preprint available at https://arxiv.org/pdf/2005.04867.pdf

[2]H. Englund et al., **Secure acceleration on cloud-based FPGAs - FPGA enclaves,** 2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)

[3] A. Duncan et al., **SeRFI: Secure Remote FPGA Initialization in an Untrusted Environment**, 2020 IEEE 38th VLSI Test Symposium (VTS)

Contact

Request Toppic

Advisors

Mathieu Gross