July 2020

CES Chair for Embedded Systems
Prof. Dr. J. Henkel

Master Thesis

Securing Partial Bitstreams of Adaptive Reconfigurable Processors

Image Source: https://www.pxfuel.com/

Run-time reconfigurable processors are gaining more interest with time as they provide application-specific accelerators that improve the overall execution time. Moreover, they can provide an upper bound for the worst-case execution time. Therefore, they are applicable for real-time performance.
Partial bitstreams are used to load the accelerators at runtime. They are stored in the memory of the processor. The partial bitstreams are not encrypted by default.
This is a major source of vulnerability. Important information about the state of the system and the executed application could leak. In order to prevent this information leakage, the partial bitstreams have to be secured.

Tasks of the student
The student shall perform these tasks but is not limited to them.

- Investigate possible protection methods for the partial bitstreams
- Investigate different key management methods
- Implement protection for the partial bitstreams preventing information leakage

Skills required for the thesis

- Programming Skills (C, C++, Python)
- Knowledge of VHDL

Skills acquired with the Thesis

- Work in a research environment
- Experience with security concepts on hardware level
- In depth knowledge of adaptive reconfigurable processors

Contact
Hassan Nassar, M.Sc., hassan.nassar@kit.edu
http://ces.itec.kit.edu/~nassar

Dr.-Ing. Lars Bauer, lars.bauer@kit.edu
http://ces.itec.kit.edu/~bauer