Chair of Integrated Digital Systems and Circuit Design

RWTH AACHEN UNIVERSITY

Research Activity (HiWi, Master/Bachelor Thesis)

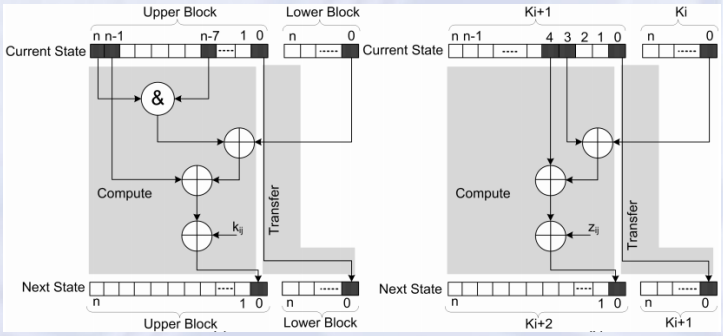
Cryptographic Engines Design for Mobile Applications

We are living in the era of ubiquitous computing. As much as big-data poses the corner stone for us to build up an intelligent world, it challenges our wisdoms for information processing. Local and distributed data capture, analytics and storage built into edge devices renders energy efficiency a primary design concern. Transferring data across the cloud of gateways and network severs also raises the critical challenge of privacy for edge applications under stringent cost constraints.

In this work we aim to explore energy- and area-efficient hardware designs of crypto-graphic engines which thereby enable their integration into energy and cost constrained mobile devices.

The project shall start with a deep dive into state-of-the-art crypto-graphic standards covering various abstraction levels from RTL, data-flow, logic and circuits.

We are looking for students that are eager to contribute to this research activity as HiWi. Depending on the background, Master or Bachelor Thesis can be defined with adequately adjusted research objectives.



Lightweight cryptography in edge devices
[Ege Gulcan, 2015]

Tasks

1. Realize lightweight cryptographic engine (behavioral RTL)
2. Review of cryptographic standards and hard-ware implementations for edge applications;
3. Optimization and evaluation of selected cryptographic engines;
4. Optimization of the cryptographic engines by introducing novel data flow;
5. Exploration of physical design space for cryptographic engines considering gate length, V_{th}, and V_{DD} at advanced process nodes.

Requirements

1. Knowledge on RTL and logic design;
2. Understanding basic cryptography;
3. Experiences in EDA is a plus;
4. Self-motivated;
5. Good English (spoken and written).

Contact

Prof. Dr.-Ing. Tobias Gemmeke
gemmeke@ids.rwth-aachen.de
+49 241 80 97600

Dr.-Ing. Xin Fan
fan@ids.rwth-aachen.de
+49 241 80 97606