
Project Title: *“From RTL Design to System-Level Validation: Implementation of an FPGA lightweight cryptography core on real hardware”*

This project is suitable for a BSc student.

Contact Information

- Konstantinos Paraskevopoulos, MSc (UT-EEMCS)
 - k.paraskevopoulos@utwente.nl
 - Dr. ir. Nikolaos Alachiotis (UT-EEMCS)
 - n.alachiotis@utwente.nl
-
-

Project Description

This project addresses the deployment and experimental validation of an FPGA-based hardware security system, based on ASCON cryptographic and authentication modules. The RTL design has been previously implemented and verified using the Vivado design suite. The design has not yet been tested on a physical FPGA platform. The main goal of the project is to integrate the existing design into a complete FPGA-based system interconnected with an embedded processor, enabling real-world operation and measurement. The student will implement the system on hardware, establish processor-to-FPGA communication, and perform experimental evaluation to verify correctness and assess performance. The project emphasizes practical system-level integration and provides experience in transitioning from RTL-level design to real-world FPGA deployment.

Tasks

- **Survey and Literature Review:** Conduct a survey of existing technologies and literature in hardware acceleration for encryption.
- **RTL Level System Optimization & Testing:** Experiment with the already implemented RTL design and propose optimizations. After the optimizations are implemented, conduct testing and validation of the system to evaluate how the system was affected.

- **FPGA System Implementation & Evaluation:** Implement the optimized version of the system on an FPGA interconnected with an embedded systems processor. Conduct testing and valuation and compare theoretical with real-world results. Design a demonstration to show how the system works.

Theory: 20%

Coding/Implementation: 30%

Evaluation: 30%

Writing: 20%