Assistant (Student)

HIWI: Advanced Cryptographic Implementations

The course Advanced Cryptographic Implementation (ACI) provides an introduction to advanced implementation techniques to optimize state-of-the-art cryptographic algorithms on embedded systems, including advanced countermeasures to secure cryptographic implementations against side-channel and fault attacks. The course relies on a practical hands-on project. During the project students are asked to implement and optimize cryptographic algorithms on a RISC-V based microcontroller using both C and assembly. As a HIWI you will help improving the current RISC-V based evaluation framework and tooling, and improve the current solutions of the project by implementing and/or optimizing portions of current cryptographic implementations.

Timeline and working hours:
From 01.04.2022 until 31.08.2022 with a total of 160 hours. Flexible working hours and flexible working period are possible.

Prerequisites

* Basic knowledge of cryptography
* Hands-on experience with C/ASM programming and microcontrollers
* Self-motivated and independent working style
* Previous knowledge of RISC-V and attendance to the course are desirable, but not required

Contact

Fabrizio De Santis

fabrizio.desantis@siemens.com

Advisors

Fabrizio De Santis