Tutor/in: 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 cryptography implementations against side-channel and fault attacks.

The exercise part of the course relies on a practical hands-on project. During the project students will be asked to implement and optimize cryptographic algorithms on a RISC-V based microcontroller using both C and assembly.

As a tutor you will provide technical support to students during the project period in form of (virtual) meetings or remote supervision (e.g., chat or mail) and help with the organization of the project (preparation).

Timeline and working hours:
From 01.04.2022 until 29.07.2022 with a total of 84 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