Tutor/in: Advanced Cryptographic Implementations (SS2024)

The course "Advanced Cryptographic Implementation" is focuses on advanced techniques for engineering state-of-the-art cryptographic implementations for embedded systems. It offers a comprehensive exploration of efficient methods for implementing cryptographic algorithms, along with countermeasures to safeguard these implementations against side-channel and fault attacks.

During the course, students will have the opportunity to engage in a practical, hands-on project that will enable them to acquire the necessary skills to implement cryptographic algorithms on a microcontroller.

As a tutor you will provide technical support to students during the summer semester in form of meetings and/or supervision (e.g., chat or mail).

Timeline and working hours:

From 15.04.2024 until 31.07.2024 with a total of 84 hours. Flexible working hours and working period are possible.

Prerequisites

- Self-motivated and independent working style.
- Hands-on experience with programming and microcontrollers.
- Previous knowledge of ARM and/or RISC-V platforms is desirable but not required.
- Previous attendance to the course is desirable, but not required.

Contact

Fabrizio De Santis
fabrizio.desantis@siemens.com

Advisors

Fabrizio De Santis