

Advanced Anonymity Protecting Technologies for Embedded Systems

Motivation:

Transactions of electronic devices can be easily traced e.g. tracking of cars via road pricing systems, tracking of people's movement via access control systems or monitoring access logs of web servers.

Project description:

The goal of the project is to design and implement the basic cryptographic building blocks for anonymous credential systems. In contrast to common PKIs where RSA or ECC signature schemes are used, our anonymous credential system uses group signatures to achieve anonymity.

The implementation should result in a library which has to be integrated in TLS/SSL implementations such as Matrix SSL or IAIK SSL. The resulting implementation should work on an embedded microcontroller or on a mobile phone.

Tasks:

- Get familiar with anonymizing crypto algorithms
- Design a library containing basic support for anonymizing algorithms
- Integrate the library in one selected trusted channel implementation
- Develop the required core services for group management and revocation



MCB 2130 controller board

Master Project

Participants: 1-2 Students

Prerequisites:

- Experience with C & Java software development
- Crypto 1 & Crypto 2 Lectures

Contact: Kurt.Dietrich@iaik.tugraz.at

Studies: INF SEW TEL Master Thesis

The master project can be continued as master thesis.