Privacy-Friendly Parking

Advisor(s): David Derler and Daniel Slamanig

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

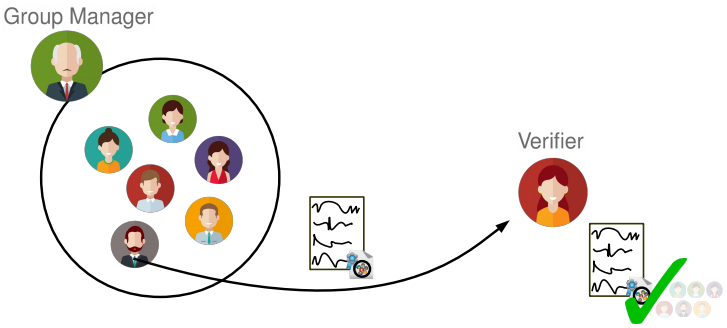
Motivation

Group signatures are an important tool in privacy enhancing crypto. They allow to set up a group so that every member of this group can anonymously sign messages on behalf of the group.

We are currently working on an application for privacy-friendly parking. We already have a plan how to employ group signatures in our use case and need help with the implementation.

Goals and Tasks

- Get familiar with the concept of group signatures.
- Understand the protocols to be implemented.
- Implement a group signature scheme.
- Write a simple demonstrator application.



Literature

- D. Derler and D. Slamanig
  Fully-Anonymous Short Dynamic Group Signatures Without Encryption
  IACR Cryptology ePrint Archive 2016
  http://eprint.iacr.org/2016/154
- O. Blazy et al.
  Non-Interactive Plaintext (In-)Equality Proofs and Group Signatures with Verifiable Controllable Linkability
  CT-RSA 2016
  http://eprint.iacr.org/2016/082

Deliverables

- Project files (zip, cleaned)
- Documentation (pdf)
- Presentation (pdf)

Schedule

- Start Immediately
- Month 1 Reading literature
- Month 2 Implementing
- Month 3 Final deliverables

Studies

☒ INF ☒ TEL ☒ SW

Prerequisites

- Interest in crypto
- Java programming

Advisor / Contact

david.derler@iaik.tugraz.at.