Witness Encryption

Advisor(s): David Derler and Daniel Slamanig

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

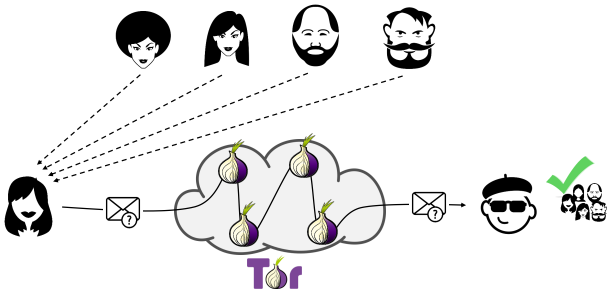
Motivation

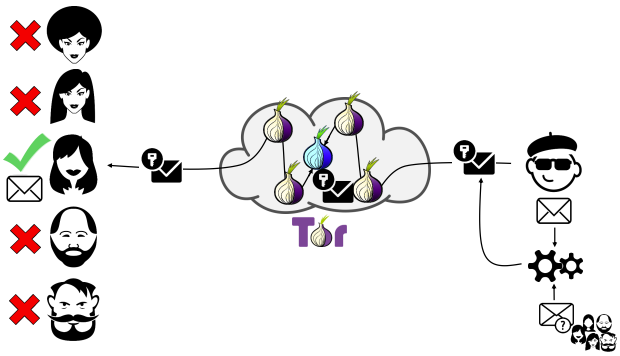
Witness encryption is an interesting encryption paradigm, which allows to encrypt a message with respect to the description of a (hard) problem so that everyone who knows a solution to this problem can later decrypt.

We have proposed a fully ad-hoc solution, which employs witness encryption to confidentially reply to an anonymous whistleblower and are interested in a practical implementation.

Goals and Tasks

- Get familiar with the concept of witness encryption.
- Understand the scheme to be implemented.
- Implement the scheme.
- Write a simple demonstrator application.





Literature

- D. Derler and D. Slamanig
  Practical Witness Encryption for Algebraic Languages Or How to Encrypt Under Groth-Sahai Proofs
  IACR Cryptology ePrint Archive 2015
  http://eprint.iacr.org/2015/1073

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.