Project Description

Nikolaj Sidorenco

January 28, 2020

1 Project

In this project I aim to formalise Sigma-protocols and commitment schemes within EasyCrypt with the help of existing formalisations. Moreover, I seek to understand the differeces between the available cryptographic proof assistents by comparing my formalisations to existings ones in the cryptHOL proof assistent.

When fomalising Sigma-protocols I also aim to prove general constructions, like the OR-construction, and proving them the be secure. Having formalised both Sigma-Protocols and Commitment schemes I will provide several concrete instantiations and prove their security in presence of passively corrupted parties.

Time permitting I will either prove the relation between Sigma protocols and Commitment schemes, the Fiat-Shamir protocol for non-interactive Sigma-protocols or other possible extensions.

2 Litterature

- Butler, D., Lochbihler, A., Aspinall, D., & Gascon, A. (2019). Formalising Σ-protocols and commitment schemes using cryptHOL.
- Metere, R., & Dong, C. (2017). Automated cryptographic analysis of the Pedersen commitment scheme. CoRR, abs/1705.05897(), .
- Damgård, I. (2011). On Σ-protocols.