Proposal for a Master’s thesis

Formalizing Constructive Security Statements in Isabelle

Supervisors: Dr. Andreas Lochbihler, Christian Badertscher, Manu Drijvers, Daniel Jost
Professor: Prof. David Basin, Prof. Ueli Maurer
Issue date:

Prerequisites

- Good foundations in cryptography and security
- Good knowledge about logic and the $\lambda$-calculus
- Interest in getting to know state-of-the-art theorem prover technology

Introduction

A formal proof is the main tool to express that a cryptographic protocol is secure under certain hardness assumptions. A typical technique is to show that any attacker breaking the claimed security goal of the protocol can be transformed into an attacker against the hardness assumption.

One way of expressing the security goal of a cryptographic protocol is to specify a game between an attacker and an instance of the protocol. For example, the IND-CPA security game allows an attacker to obtain ciphertexts for chosen plaintexts, and the game is won if the attacker can successfully distinguish ciphertexts for different plaintexts (of equal length). A problem with game-based security definitions is that they only capture specific attack-scenarios (e.g., obtaining only ciphertexts) and thus fall short of providing guarantees that hold in any possible application of the scheme. To capture what a cryptographic scheme achieves in any possible application, one has to formulate its security in a universally composable security framework such as Canetti’s UC framework [3], reactive simulatability by Backes, Pfitzmann, and Waidner [1], or constructive cryptography by Maurer and Renner [7]. For example, the central idea of constructive cryptography is that the resources available to the parties, such as communication channels or randomness, are made explicit. The goal of a cryptographic protocol is then to securely construct, from certain assumed resources, for example a secret key and an insecure channel (the “real world”), another, more desirable resource, for example a secure channel (the “ideal world”). A construction is secure
if the real world is as useful to an adversary as the ideal world, the latter world being secure by definition. Formally, one has to describe a simulator in the ideal world that generates a view for the adversary that is (computationally) indistinguishable from the real-world view. A constructed resource can then again be used by higher-level protocols or applications and thanks to the composition theorem, one can safely replace this resource by the protocol achieving it.

Due to the inherent complexity, many cryptographic proofs unfortunately lack formal rigor. This applies especially to composable security statements. As a consequence, Halevi [5], and Bellare and Rogaway [2] proposed that such security proofs should be checked mechanically by a computer. At ETH, we have developed a framework for formalising such cryptographic arguments in the proof assistant Isabelle/HOL [6]. We used it successfully to mechanically check indistinguishability statements of some cryptographic protocols.

### Objectives

The goal of this thesis is to formalize constructive security statements and their proofs in the Isabelle/HOL framework. Constructive cryptography [7, 4], which is being developed at ETH as well, is a suitable candidate for this task and offers an elegant basis to start with.

The goal can be achieved in three steps: First, identify how the notions of constructive cryptography can be expressed in Isabelle. We will focus on the so-called Alice-Bob-Eve setting (where Alice and Bob denote two honest parties and Eve the adversary). Second, formalize important proof steps for constructive security statements within the proof assistant. Third, proof constructive security statements using your Isabelle framework.

### Tasks

This project can be subdivided into the following tasks:

1. Make yourself familiar with Isabelle/HOL and the framework for formalising cryptographic arguments (e.g., by working through the relevant tutorials [8] and existing proofs).

2. Find a way to represent the main concepts of constructive cryptography in Isabelle. This includes the notion of a distinguisher, a resource, and a converter, as well as their interaction. Phrase repeating proof steps for constructive security statements, such as composition-order invariance, as lemmata in Isabelle.

3. Pick a cryptographic construction from the literature, we recommend [4], and prove the soundness of this construction using the reasoning principles from step 2.

4. **(optional)** The project can be extended to further cryptographic constructions or investigate the applicability of your formalization to models other than constructive cryptography.

5. Write the final report and prepare the presentation.
**Deliverables**

The following deliverables are due at the end of the project:

- **Final report** The final report should consist of an introduction; a theoretical background section; one or more sections describing the challenges in Isabelle/HOL, the implementation, and the test cases; and a conclusion. The language of the report is English.

- **Isabelle/HOL theories** Complete Isabelle/HOL development that runs with the latest release or a recent developer’s version.

- **Presentation** At the end of the project, a presentation of 30 minutes must be given during an InfSec group seminar. It should give an overview and discuss the most important highlights of the work.

**References**


