Thesis Proposal

José Bacelar Almeida*

CCTC-UM
December 2010

1 Title

Tool Support for Security Proofs

2 Context

Formal verification of security proofs have attracted much attention in recent years. A security proof of a cryptographic scheme consists of an argument that reduces a successful attack to the scheme in a probabilistic algorithm for solving a presumably intractable problem — a *computational assumption*. These proofs are often organized as sequences of probabilistic games describing the interaction of the scheme with an adversary. However these proofs are inherently complex, which makes them difficult to verify. In fact, several published proofs have been shown to be incorrect. As a result, the need for tool support as been claimed as essential to turn cryptographic proofs less prone to errors.

This thesis proposal addresses the construction of such a tool, build around the Coq proof assistant. This work is proposed in the context of the research project *SMART - Secure Memories and Applications Related Technologies* (European Nanoelectronics Initiative Advisory Council). The mission of the SMART project is to define and develop new hardware and firmware technologies for the secure storage and communication of large and multi-form data.

3 Formalization of Security Proofs

The use of theorem provers for the verification of security proofs is an area of active research during the last couple of years. In particular, the HasLab/CCTC research group have collaborated with the research groups that have proposed the most significant approaches in this context, namely:

*Email: jba@di.uminho.pt

- *Certicrypt* – a framework based on the Coq proof system, by Gilles Barthe and his colleagues at IMDEA, Spain.
- *David Nowak's toolbox* – a toolbox also developed in Coq at AIST Institute, Japan, by David Nowak.

These tools are representative of distinct approaches for modeling an application domain in a theorem prover: Certicrypt is based on what is called a *deep-embedding*, where a domain specific language is formalized in the system, together with the corresponding semantic interpretation. On the other hand, David Nowak's tolbox is an example of a *shallow-embedding*, where Coq's own specification language is used for directly modeling the target semantic domain (security games are modelled directly as functions in Coq's language). Each approach has its own merits. By one side, a shallow-embedding is considerably lighter, being more flexible in fitting new application scenarios. On the other side, a deep-embedding increases the possibilities of automation, and is capable of expressing relevant notions such as complexity issues.

4 Goals

The first main objective of the project is to define a set of basic components that will provide support for expressing security proofs (probabilistic reasoning, algebraic reasoning, complexity constraints). These components are expected to be tightly coupled with both `ssreflect` (an extension of Coq that includes an extensive library of algebraic results), and the Certicrypt tool (or, more precisely, to the second generation of the tool which is currently under development, and where this project is expected to provide active contribution). During this task, a close collaboration with Certicrypt group at IMDEA is anticipated.

The second main goal is to investigate concrete cryptographic solutions proposed in the context of the SMART project. To this end, the framework should be extended with support for "leakage-resilient cryptography", and be integrated with other tools developed in the context of the project.