Paper Title

Diego Lupi, Pedro Nieto, and Huaira Gómez

FaMAF - Universidad Nacional de Córdoba, Córdoba, Argentina

Resumen Easycrypt[1] es una herramienta automatizada que soporta la construcción y verificación de pruebas de seguridad de sistemas criptográficos. Permite mejorar la confianza en sistemas criptográficos mediante la entrega de pruebas verificadas formalmente que resultan en sus metas propuestas. Provee una plataforma versátil que soporta pruebas automatizadas pero también permite al usuario realizar puebas complejas de manera interactiva entrelazando la verificación del programa con la formalización de las matemáticas, hecho fundamental al formalizar pruebas criptográficas.

Keywords: Easycrypt · Game-based cryptographic proofs · Probabilistic.

1. Introducción

Desde siempre las pruebas fueron propensas a errores, lo que naturalmente las puede llevar a ser erróneas. En particular las pruebas de seguridad criptograficas la correctitud es critica para mejorar la confianza en el sistema criptografico. Actualmente se tiede a generar mas pruebas de seguridad de las que se pueden verificar, se omiten detalles finos desde un analisis formal que pueden tener grandes efectos en la practica. Teniendo en cuenta que los sistemas criptograficos en el mundo real pueden ser vulnerados, es necesario hacer las verificaciones sobre los pruebas de los sistemas criptograficos para evitar un desastre en el area de la seguridad.

Easycrypt es una herramienta que permite de manera interactiva buscar, construir, y realizar comprobaciones en maquina a pruebas de seguridad de construicciones criptograficas usando la secuencialidad del codigo con un enfoque de juego. El enfoque de juego consiste en la interaccion de un retador y un adversario, donde se especifica explicitamente la meta que adversario intenta alcanzar, como por ejemplo suponer de manera correcta una porcion de informacion oculta. Usando este enfoque podemos definir seguridad[2] como

Definition 1. *Para todo adversario, la probabilidad de que se alcance la meta no exceda un umbral fijo.*

En Easycrypt los juegos cryptograficos se modelan como modulos, que consisten en procedimientos escritos en lenguaje imperativo. Por otra parte los adversarios se modelan como modulos abstractos, modulos cuyo codigo es desconocido y puede cuantificarse.

EasyCrypt [BDG + 14, BGHZ11] is a framework for interactively finding, constructing, and machine-checking security proofs of cryptographic constructions and protocols using the code- based sequence of games approach [BR04, BR06, Sho04]. In EasyCrypt, cryptographic games and algorithms are modeled as modules, which consist of procedures written in a simple user- extensible imperative language featuring while loops and random sampling operations. Adversaries are modeled by abstract modules—modules whose code is not known and can be quantified over. Modules may be parameterized by abstract modules. EasyCrypt has four logics: a probabilistic, relational Hoare logic (pRHL), relating pairs of procedures; a probabilistic Hoare logic (pHL) allowing one to carry out proofs about the probability of a procedure's execution resulting in a post-condition holding; an ordinary (possibilistic) Hoare logic (HL); and an ambient higher-order logic for proving general mathematical facts and connecting judgments in the other logics. Once lemmas are expressed, proofs are carried out using tactics, logical rules embodying general reasoning principles, and which transform the current lemma (or goal) into zero or more subgoals—sufficient conditions for the original lemma to hold. Simple ambient logic goals may be automatically proved using SMT solvers. Proofs may be structured as sequences of lemmas, and EasyCrypt's theories may be used to group together related types, predicates, operators, modules, axioms and lemmas. Theory parameters that may be left abstract when proving its lemmas—types, operators and predicates—may be instantiated via a cloning process, allowing the development of generic proofs that can later be instantiated with concrete parameters.

Referencias

1. Gilles Barthe, Juan Manuel Crespo, Benjamin Gregoire, Cesar Kunz, Santiago Zanella Beguelin. Computer-Aided Cryptographic Proofs. Third International Conference, 2012.
2. Jonathan Katz, Yehuda Lindell: Introduction to modern cryptography. 2nd edn. CHAPMAN & HALL/CRC, Boca Raton, FL (2008).