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 criptograficas la correctitud de las pruebas es critico para mejorar la confianza en el sistema criptografico. Actualmente se tiede a generar mas pruebas 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.

Desde siempre las pruebas fueron propensas a errores, lo que naturalmente las puede llevar a ser erróneas. En particular las pruebas criptograficas la correctitud de las pruebas es critico para mejorar la confianza en el sistema criptografico. Actualmente se tiede a generar mas pruebas 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.

Referencias

1. Gilles Barthe, Juan Manuel Crespo, Benjamin Gregoire, Cesar Kunz, Santiago Zanella Beguelin. Computer-Aided Cryptographic Proofs. Third International Conference, 2012.