Formal certification of code-based cryptographic proofs.

Gilles Barthe

17/03/2009

Abstract

As cryptographic proofs have become essentially unverifiable, cryptographers have argued in favor of systematically structuring proofs as sequences of games. Code-based techniques form an instance of this approach that takes a code-centric view of games, and that relies on programming language theory to justify steps in the proof---transitions between games. While these techniques contribute to increase confidence in the security of cryptographic systems, code-based proofs involve such a large palette of concepts from different fields that machine-verified proofs seem necessary to achieve the highest degree of confidence. In an inspiring paper, Halevi convincingly argued that a tool assisting in the construction and verification of proofs is necessary to solve the crisis with cryptographic proofs.

CertiCrypt is a framework to construct machine-checked code-based proofs in the Coq proof assistant. CertiCrypt achieves many goals of Halevi's ideal tool. At the same time, it brings a formal semanticist perspective on the design of the tool, and in particular ensures the highest guarantees with the smallest trusted base. The main characteristics of CertiCrypt are:
* Direct and faithful encoding of code-based techniques.
* Support for code-based proofs.
* Complete and independently verifiable proofs.
The talk shall describe the design of CertiCrypt and its applications to machine-checked proofs of encryption and signature schemes.