Computer-aided cryptography: status and perspectives

Gilles Barthe

IMDEA Software Institute, Madrid, Spain

Computer-aided cryptography is an emerging discipline which advocates the use of computer tools for building and mechanically verifying the security of cryptographic constructions. Computer-aided cryptography builds on the code-based game-based approach to cryptographic proofs, and adopts a program verification approach to justify common patterns of reasoning, such as equivalence up to bad, lazy sampling, or simply program equivalence. Technically, tools like EasyCrypt use a program verification method based on probabilistic couplings for reasoning about the relationship between two probabilistic programs, and standard tools to reason about the probability of events in a single probabilistic program. The combination of these tools, together with general mechanisms to instantiate or combine proofs, can be used to verify many examples from the literature.

Recent developments in computer-aided cryptography have explored two different directions. On the one hand, several groups have developed fully automated techniques to analyze cryptographic constructions in the standard model or hardness assumptions in the generic group model. In turn, these tools have been used for synthesizing new cryptographic constructions. *Transformational* synthesis tools take as input a cryptographic construction, for instance a signature in Type I setting and outputs another construction, for instance a batch signature or a signature in Type III setting. In contrast, *generative* synthesis tools take as input some size constraints and output a list of secure cryptographic constructions, for instance padding-based encryption schemes, modes of operations, or tweakable blockciphers, meeting the size constraints. On the other hand, several groups are working on carrying security proofs to (assembly-level) implementations, building on advances in programming languages, notably verified compilers. These works open the possibility to reason formally about mitigations used by cryptography implementers and to deliver strong mathematical guarantees, in the style of provable security, for cryptographic code against more realistic adversaries.

For further background information, please consult:`www.easycrypt.info`.