CryptoVerif: a computationally-sound security protocol verifier

Bruno Blanchet*[1]

[1]Inria – Inria Paris Saclay – France

Résumé

CryptoVerif is a security protocol verifier sound in the computational model of cryptography. It produces proofs by sequences of games, like those done manually by cryptographers. It has an automatic proof strategy and can also be guided by the user. It provides a generic method for specifying security assumptions on many cryptographic primitives, and can prove secrecy, authentication, and indistinguishability properties. A successful proof guarantees asymptotic security, in the presence of polynomial-time adversaries, and also provides an exact security bound of the probability of success of an attack as a function of the probability of breaking the primitives. This talk will present a general introduction to CryptoVerif and will briefly mention a few recent results: post-quantum CryptoVerif, CV2EC, CV2F*.
Bio:
Bruno Blanchet is senior researcher at Inria Paris and head of the project-team Prosecco. His research focuses on the development of tools for verification of security protocols. He was the main developer of the symbolic protocol verifier ProVerif and is now the main developer of CryptoVerif.

*Intervenant