Verification of cryptographic protocols: techniques and link to cryptanalysis

Véronique Cortier

Verification of cryptographic protocols: techniques and link to cryptanalysis

Véronique Cortier[1]

CNRS — LORIA
Nancy, France

Abstract

Security protocols are short programs aiming at securing communications over a network. They are widely used in our everyday life. Their verification using symbolic models has shown its interest for detecting attacks and proving security properties. In particular, several automatic tools have been developed. However, the guarantees that the symbolic approach offers have been quite unclear compared to the computational approach that considers issues of complexity and probability. This later approach captures a strong notion of security, guaranteed against all probabilistic polynomial-time attacks.
In this talk, we present several techniques used for symbolically verifying security protocols and we show that it is possible to obtain the best of both worlds: fully automated proofs and strong, clear security guarantees. For example, for the case of protocols that use signatures and asymmetric encryption, we establish that symbolic integrity and secrecy proofs are sound with respect to the computational model against an active adversary.

[1] Email: Veronique.Cortier@loria.fr

Abstract of an invited talk given at AVoCS 2006
URL: avocs06.loria.fr