Normal attacks on security protocols

Hubert Comon

LSV, ENS Cachan, 61, av. du Président Wilson 94235 Cachan Cedex, France

We consider the problem of automatically verifying security protocols. The specification of such protocols come in three parts:

- ⋆ A finite set of processes called roles. They rely on some cryptographic primitives such as (a)symetric encryption, one way functions etc.
- ⋆ Hypotheses on the deductive capabilities of an intruder, which we assume given as a set of inference rules.
- ⋆ The (assumed) algebraic properties of cryptographic primitives, which we assume given by a convergent rewrite system, possibly modulo associativity and commutativity.

In this talk, our goal is to give sufficient conditions on both the intruder capabilities and the algebraic properties, which allow to derive a normalization result on possible attacks. This yields complete strategies in general and decision procedures when the number of sessions is fixed.