Two models for the verification of cryptographic protocols:

**Abstract Model; Automatic Proofs:**
- \(\text{sign}(M, sk)\)
- \(\text{enc}(M, k)\)
- \(\text{dec}\)
- \(\text{enc}\)
- \(\text{sign}\)

Our goal is to bridge the gap between these two models:
- **Computational Model:**
  - Probabilistic Turing machine
  - Example: 0101101110
  - Example: 01010100010

**Realistic Model; Manual Proofs:**
- Participants:
  - LIENS: Bruno Blanchet, David Pointcheval, David Monniaux
  - LSV: Jean Goubault-Larrecq, Mathieu Baudet, Steve Kremer
  - LORIA: Véronique Cortier, Mathieu Turuani, Bogdan Warinschi
- Scientific Advisor: Martin Abadi

**URL of the project:** http://www.di.ens.fr/~blanchet/formacrypt/

A logically sound prover

- **Goal:** Build a specialized, computationally sound, automatic prover.
- **Results already obtained:**
  - An automatic, computationally sound prover that
    - generates proofs by sequences of games, as in Shoup’s or Bellare and Rogaway’s method;
    - proves secrecy and that events are executed with negligible probability;
    - provides a generic treatment of cryptographic primitives, including shared- and public-key encryption, signatures, MACs, hash functions;
    - is sound in the presence of an active adversary, for a parametric number of sessions;
    - evaluates the probability of an attack (exact security).
- The user is allowed (but does not have) to interact with the prover to make it follow a specific sequence of games.

Examples handled:
- Many protocols: correct versions of Needham-Schroeder, Denning-Sacco, Otway-Rees, Yahalom,... protocols;
- Full Domain Hash signatures scheme;
- Encryptions schemes of Bellare and Rogaway, CCS’93.

Publications:
- B. Blanchet, IEEES&P, Oakland, 2006

**Planed extensions:**
- Authentication properties.
- Other primitives, such as Diffie-Hellman key agreements.
- Improvements in the proof strategy, for more automation.

A computationally sound logic

- **Goal:** Design a computationally sound logic for reasoning symbolically on protocols.
- **Results already obtained:**
  - Adaptation of the Protocol Composition Logic (PCL) to the computational model.
  - Soundness proof for a subset of PCL with positive tests.
  - Extension to prove more complex properties, such as secrecy of keys.
- This logic is compositional. For example, from the security of keysestablished using a key exchange protocol, one can prove the security of a secure channel application that uses these keys.

Publications:
- M. Backes, A. Datta, A. Derek, J. C. Mitchell, and M. Turuani, TCS.

**Planed extensions:**
- Soundness for any proof in PCL with computational tests.
- Make the semantics more direct and natural.

Case studies and comparison of the various approaches

**Goal:** Compare the results obtained by the three approaches above, on examples ranging from protocols of the literature to more complex, realistic protocols.

**Planed extensions:**
- Branching properties (e.g., fairness).
- Secrecy of keys.
- Primitives with more complex equational theories (Diffie-Hellman, XOR, CBC encryption).

Proofs in the formal model imply proofs in the computational model.

**Goal:** Obtain computational soundness results, i.e., show that security in the formal model implies security in the computational model.
- Computationalsoundness was shown for public-key encryption and signatures.
- Based on this result, we have implemented a tool that provides computational proofs of protocols, using the AVISPA formal protocol analyzer.
- We have extended computational soundness results to the case of hash functions.
- We have developed an equational theory for specifying cryptographic primitives, such that (symbolic) static equivalence is sound with respect to computational indistinguishability.

Publications:
- M. Abadi, M. Baudet, and B. Warinschi, FoSSaCS'06
- V. Cortier and E. Zalinescu, LPAR'06
- V. Cortier, H. Härdegen, and B. Warinschi, ICS'06
- V. Cortier, S. Kremer, R. Küsters, and B. Warinschi, FSTTCS'06

Software at http://www.loria.fr/~hordegen/avispa/