Formal verification of security protocols: the Squirrel prover

Stéphanie Delaune*[1]

[1]Institut de Recherche en Informatique et Systèmes Aléatoires (IRISA) – Université de Rennes, Institut National des Sciences Appliquées - Rennes, Université de Bretagne Sud, École normale supérieure - Rennes, Institut National de Recherche en Informatique et en Automatique, CentraleSupélec, Centre National de la Recherche Scientifique, IMT Atlantique – Avenue du général LeclercCampus de Beaulieu 35042 RENNES CEDEX, France

Résumé

Security protocols are widely used today to secure transactions that take place through public
channels like the Internet. Common applications involve the secure transfer of sensitive

information like credit card numbers or user authentication on a system.

Because of their increasing ubiquity in many

important applications (e.g. electronic commerce, smartphone, government-issued ID . . .),

a very important research challenge consists in developing methods and verification tools

to increase our trust on security protocols, and so on the applications that rely on them.

Formal methods have introduced various approaches to prove that

security protocols indeed guarantee the expected security properties.

Tools like ProVerif and Tamarin analyse protocols in the symbolic

model, leveraging techniques from model-checking, automated reasoning,

and concurrency theory.

However, it's essential to note that security in the symbolic model

doesn't necessarily imply security in the cryptographer's standard

model-the computational model-where attackers operate as

*Intervenant

probabilistic polynomial time Turing machines. Verification techniques for the computational model, though crucial, often exhibit less flexibility or automation compared to tools in the symbolic model.

In recent collaborative efforts, my colleagues and I have proposed a novel approach, building upon the CCSA logic introduced by Gergei Bana and Hubert Comon a few years ago. This approach has been implemented in a new proof assistant called Squirrel and its effectiveness has been validated across various case studies. In this presentation, I will outline the key aspects of the approach, highlight its advantages, and discuss some of the remaining challenges.