Secrecy by typing in the computational model

Clément Herouard*[1]

[1]Institut de Recherche en Informatique et Systèmes Aléatoires – Institut National de Recherche en Informatique et en Automatique – France

Abstract

In this presentation, we propose a way to automate proofs of cryptographic protocols in the computational setting. We focus on weak secrecy and we aim to use type systems. Techniques based on typing have been used in symbolic models, and we show how these techniques can be adapted to the CCSA framework to obtain computational guarantees.
First, we only consider for now a limited set of primitives: symmetric encryption and decryption, and pairing (i.e. concatenation). However, our approach has the usual benefit of type systems of being modular, and could be extended to other primitives without excessive difficulties, as shown with asymmetric encryption. We aim to integrate it into the SQUIRREL proof assistant so that users may show some weak secrecy properties by typing and use them as part of larger SQUIRREL developments. This is still ongoing work. Index Terms-Security protocols, automated reasoning, typing, computational model, CCSA

*Speaker