SQUIRREL

An Interactive Prover for Protocol Verification in the Computational Model

D. Baelde, S. Delaune, C. Jacomme, A. Koutsos & S. Moreau

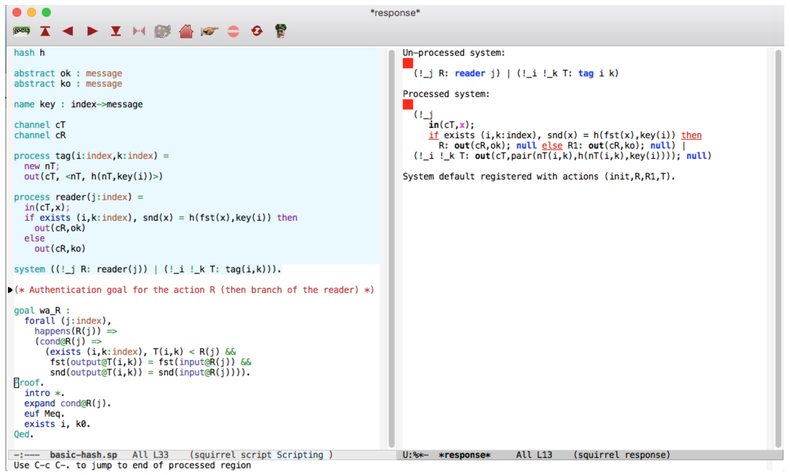
We illustrate our approach on the Basic Hash protocol which is an RFID protocol involving multiple tags and readers. Each tag stores a secret key that is never updated, and the readers have access to a shared database containing all these keys. The protocol is as follows:

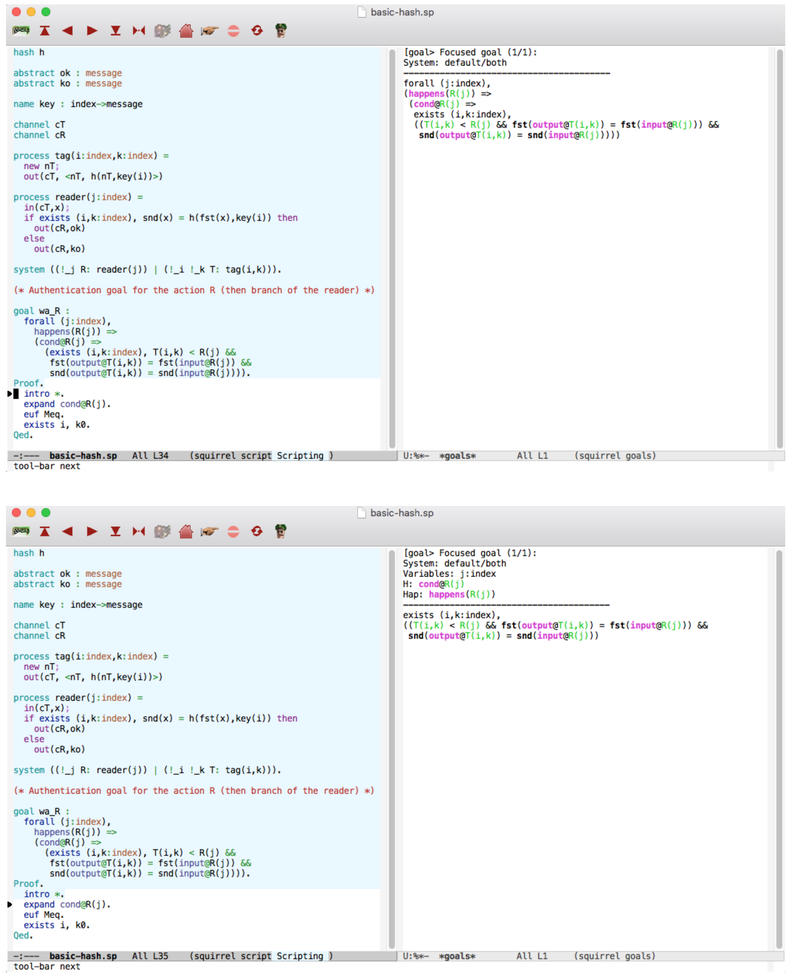
$$T \to R : \langle n, \mathsf{H}(n, key) \rangle$$

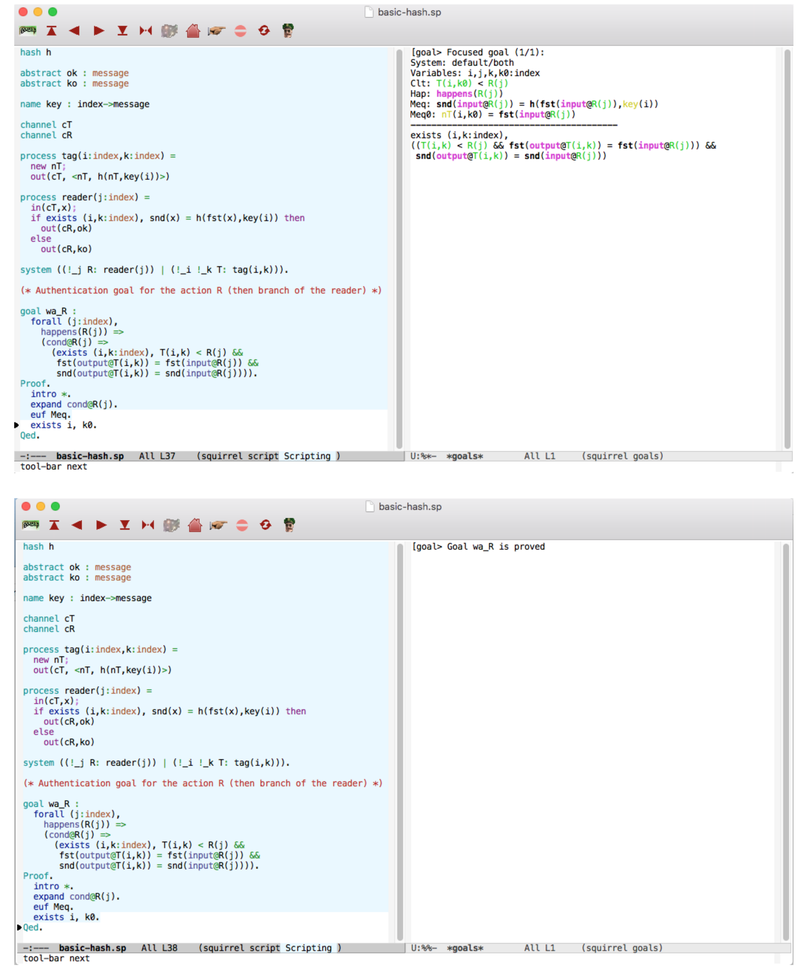
Here, n is a fresh name and key is the secret key. When receiving a message, the reader checks that it is a pair whose second component is a hash of the first component using one of the keys from the database. We illustrate how SQUIRREL works on a simple authentication goal. The screenshots below show how the proof can be done step by step.

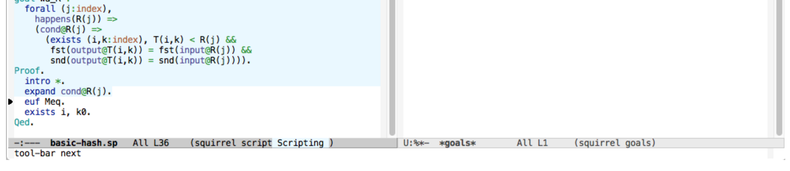
Poster Demo

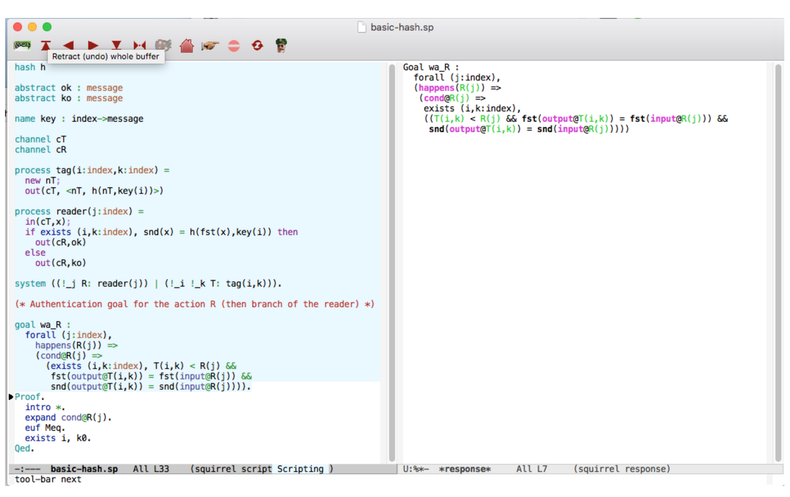
Hopefully, more online with the screen sharing feature!











erc
cnrs
UMR IRISA
université PARIS-SACLAY
LMF Laboratoire Méthodes Formelles
CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY
Inria