Recent advances in CryptoVerif

Bruno Blanchet

INRIA Paris
Bruno.Blanchet@inria.fr

April 2024
CryptoVerif is a mechanized prover that:
- works in the computational model.
- generates proofs by sequences of games.
- proves secrecy, correspondence, and indistinguishability properties.
Dealing with dynamic key compromise in CryptoVerif
[to appear at CSF’24]

Extensions:

- Proof of secrecy, when part of an array is secret, and part is public.
- New commands and game transformations:
  - `focus q_1, \ldots, q_m` tells CryptoVerif to prove only the properties $q_1, \ldots, q_m$.
  - `success simplify` removes parts of the game such that the adversary cannot break the desired properties when they are executed.
  - `guess` the tested session, the value of a variable, which branch of a test is taken.
Proof strategy:

1. Insert events $e_i$ executed when some authentication properties are broken (and the key is not compromised).

2. **focus** on proving $\text{event}(e_i) \Rightarrow \text{false}$.

3. **success simplify** removes the compromise of the key.

4. We prove queries $\text{event}(e_i) \Rightarrow \text{false}$.

5. We go back to before **focus** and prove the other properties (implicitly using the authentication properties already proved).
Example application:

- Forward secrecy with respect to the compromise of the pre-shared key in TLS 1.3 and WireGuard.
CV2EC: Getting the Best of Both Worlds

Translate CryptoVerif security assumptions to EasyCrypt.

Applications:

- 1-to-$N$-query IND-CCA2 public-key encryption
- CDH and GDH with random self-reducibility
- $N$-user IND-CCA2 authenticated KEM