CryptoVerif: Mechanising Game-Based Proofs

Wrapping up

Benjamin Lipp & Charlie Jacomme

June 06, 2023

Max Planck Institute for Security and Privacy & Inria Paris

Exercise solution

- Who managed to get some security proved automatically?
- Any intuition about the final security bound?
- Any feedback for us? Too fast? Too slow? Too boring?

CryptoVerif, `https://cryptoverif.inria.fr/`

CryptoVerif

- generates **proofs by sequences of games**.
- proves **secrecy**, **authentication**, and **indistinguishability** properties.
- provides a **generic** method for specifying properties of **cryptographic primitives** which handles MACs (message authentication codes), symmetric encryption, public-key encryption, signatures, hash functions, Diffie-Hellman key agreements, ...
- works for N **sessions** (polynomial in the security parameter), with an **active adversary**.
- gives a bound on the **probability** of an attack (exact security).
- has an **automatic** proof strategy and can also be **manually guided**.

What We Covered Today

- Introduction to the syntax and semantics of games
- Model simple primitives and protocols
- Use macros from the default library: symmetric encryption, MAC, signature, random oracle, basic Diffie-Hellman
- Basic interactive interaction with CryptoVerif
- Prove secrecy and correspondence properties
- Read the final result

Next Steps with CryptoVerif

- Work on the additional exercices
  - syntax highlighting is available for Vim and Emacs
- The reference manual is online
  `https://bblanche.gitlabpages.inria.fr/CryptoVerif/`
- More examples are in the directory `examples` of the archive
  - beware, spoilers for the exercices
  - look for `.ocv` files, they use the oracle syntax presented in this tutorial. (`.pcv` and `.cv` use the *channel* frontend)
  - HPKE is the most recent work aiming to be close to the style of pen-and-paper security notions
- Subscribe to the mailinglist (low activity)
  `https://sympa.inria.fr/sympa/subscribe/cryptoverif`

On going work

- Interactions with EasyCrypt and F*
- Post-quantum sound version of CryptoVerif
- many ongoing extensions and proofs

References

- References for how CryptoVerif proves (titles are clickable links)
  - Secrecy:

    [1] Bruno Blanchet. A Computationally Sound Mechanized Prover for Security Protocols. IEEE Transactions on Dependable and Secure Computing, 5(4):193-207, October-December 2008. Special issue IEEE Symposium on Security and Privacy 2006.
  - Correspondence:

    [2] Bruno Blanchet. Computationally Sound Mechanized Proofs of Correspondence Assertions. Cryptology ePrint Archive, Report 2007/128.