Automated Proofs for the Post-quantum Extensions of IKEv2

Sophia Grundner-Culemann

Ludwig-Maximilian-Universität

Since classical cryptography is under threat from the advances in quantum computing, the IETF and other standard bodies are taking measures to try and secure the standard internet protocols against future attacks. They mainly achieve this by extending the legacy protocols, which alters the protocol's state machines. Automated Theorem Proving (ATP) has become a valuable tool for the formal analysis of new network protocols (e.g., TLS 1.3 and MLS). The IKE_INTERMEDIATE-extension of the IPsec key exchange protocol IKEv2 has already been analysed using the Automated Prover "Tamarin"; however, there are other post-quantum-extensions that still need to be addressed. We will therefore outline the next steps in formally verifying the remaining IKEv2-protocol changes.

Keywords: IKEv2, IPsec, formal verification, network protocols, post-quantum cryptography