PhD Thesis proposal
Formal verification of post-quantum secure messaging

Charlie Jacomme
charlie.jacomme@inria.fr
charlie.jacomme.fr

Steve Kremer
steve.kremer@inria.fr
members.loria.fr/SKremer/

City and country Nancy, France.

Research team Team PESTO at LORIA lab (Inria Nancy, CNRS and Université de Lorraine).

Thesis subject Secure messaging applications are among the most used and most sensitive applications around the globe. Whether it is simply to communicate with loved ones, or a journalist talking with a source, or activists organizing in countries prosecuting them, it is crucial that the exchanged messages remain secure for as long as possible. The Signal Messenger, a widely deployed secure messaging application, has already received a lot of scrutiny over the years, and strong guarantees have been obtained on the underlying protocols. However, with the threat of quantum computers breaking elliptic curve cryptography, those protocols need to be updated. Signal Messenger relies on two protocols, an initial key exchange dubbed PQXDH, and a subsequent per-message key update protocol, the Double Ratchet. As its name indicates, the former is already a post-quantum (PQ) resistant version, but the latter remains to be updated.

This thesis will aim to verify recent proposals of Key Encapsulation Mechanism (KEM) based double ratchets, using a mechanized prover for cryptographic proofs of protocols, the Squirrel Prover [1] (`squirrel-prover.github.io`). At first, the KEM double ratchet would be analyzed in isolation, and then ideally in the full setting of PQXDH and the elliptic curve double ratchet.

Working environment The thesis will take place in the PESTO team at LORIA. The team focuses on developing formal methods for proving the security of protocols, and has participated in the development of many tools for this, such as ProVerif, Tamarin, Jasmin, DeepSec, Sapic+, and of course, the Squirrel Prover. On the more applied side, the team as participated in the analysis of widely deployed standards of security protocols (5G-AKA, SSH, TLS, OPC-UA, ...), and already as experience in secure messaging.

Expected ability The student should have either a strong background in theoretical computer science (with a focus on logic) or provable cryptography. Some experience in using a mechanized prover such as Rocq, Isabelle, ... is a bonus.

References

[1] David Baelde, Stéphanie Delaune, Charlie Jacomme, Adrien Koutsos, and Solène Moreau. An Interactive Prover for Protocol Verification in the Computational Model. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 537–554, May 2021. ISSN: 2375-1207.