Internship project
Security Analysis of the Signal Messenger application - focus on key reuse

Charlie Jacomme

September 10, 2024

Keywords Cryptographic analysis, Signal Messenger, CryptoVerif, Post-Quantum

General Context To obtain formal guarantees over security protocols, we often rely on computer-aided cryptography, where a program will hep us to the proof.

We recently analyzed PQXDH, the initial key exchange of Signal, by using CryptoVerif[1], a prover that enables us to make with a computer classical cryptographic proofs based on game-hops. Yet, our analysis [1] suffers from some limitation.

The project PQXDH, and more generally Signal, uses an identity key to identify each agent. While most theoretical protocols and their analysis are often made with the assumption that a given key is used for a single purpose in real life (e.g., only to produce encryptions, or only to produce signatures), this assumption is often not met in practice, and in the case of Signal, the identity key is used in multiple fashions. Our work as well as all previous analysis of Signal (e.g., [2]) have ignored this issue and came up with approximations.

The goal of this project will be to build over our previous CryptoVerif models, and include all the possible the identity key reuse. This may require designing new joint security notions for the corresponding primitives, as classical ones are not met under key reuse, and existing joint security notion (e.g., [3]) do not directly apply to PQXDH.

As a first step, we will start by including the fact that the identity key is directly used within PQXDH both for an xEdDSA signature and a X25519 shared key computation. Then, if successful, we will track down in the open source code all the real life additional reuse of the identity key, and try to derive a global result.

Importantly, existing proofs consider both a classical and a quantum attacker, and the general result should also cover both cases.

[1] `https://bblanche.gitlabpages.inria.fr/CryptoVerif/`

References

[1] Karthikeyan Bhargavan, Charlie Jacomme, Franziskus Kiefer, and Rolfe Schmidt. Formal verification of the pqxdh post-quantum key agreement protocol for end-to-end secure messaging. In *33rd USENIX Security Symposium*, 2024.

[2] Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, and Douglas Stebila. A formal security analysis of the signal messaging protocol. *Journal of Cryptology*, 33:1914–1983, 2020.

[3] Erik Thormarker. On using the same key pair for ed25519 and an x25519 based kem. *Cryptology ePrint Archive*, 2021.