Subversion-resilient Key-exchange in the Post-quantum World

Charlie Jacomme*[1]

[1]Inria – Inria Nancy - Grand Est – France

Abstract

Subversion-resilient Authenticated key-exchange (AKE) aims to achieve the guarantees of secure AKE even in the presence of an adversary that has tampered with parts of the protocol's implementation. One way to achieve subversion-resilient AKE is the use of Reverse Firewalls (RFs), an untrusted third-party that can restore security. In this presentation, we will present security definitions for AKE in this setting, and discuss the challenges toward providing such post-quantum subversion-resilient AKE. To overcome them, we will introduce a novel kind of Key Encapsulation Mechanism for which public keys are re-randomizable, provide an instantiation for it based on Kyber, as well as propose a final AKE based on it. Our subversion resilient AKE was proved secure both on paper as well as using CryptoVerif, a mechanized prover, and we will highlight the benefits of this approach.

*Speaker