Effects of PQC on Wireguard protocol

Qiguang Wang, Master of Science in Computer Science

University of Dublin, Trinity College, 2023

Supervisor: Stephen Farrell

This paper introduces KEM-WireGuard, a post quantum secure instantiation. This study is based on the KEMTLS protocol (ACM CCS 2020), which uses key-encapsulation mechanisms (KEMs) instead of post quantum signatures to authenticate communication parties. It brings both the TLS and the traditional post-quantum TLS into a more efficient protocol. Notably, this variant does not merely put focus on few aspects of security such as authentication and forward secrecy, as commonly pursued by earlier research at designing post-quantum protocols. Instead, it also offer bilateral post-quantum authentication with moderate cost of computation and communication. To accomplish this, we substitute the existing Elliptic Curve Diffie-Hellman key exchange with a new asymmetric crypto primitive, namely KEM. This thesis explores various combinations of different KEMs to alter existing WireGuard implementations. We propose three incremental modifications, each providing different level of security against quantum threats.