Title

Future-proofing Key Exchange Protocols: Hybrids and Beyond

Abstract

By now, the fact that quantum computers will have serious implications on the security of currently deployed cryptographic protocols is widely acknowledged and research into developing quantum-resistant solutions is well under way.

However, history shows that the biggest hurdle is often not in the development of new, more secure algorithms, but in the widespread deployment of these algorithms. Backwards compatibility must be ensured while, at the same time, downgrade-attacks must be avoided at all costs. This makes the transition to new cryptographic primitives or protocol versions a highly non-trivial and daunting task.

In this talk, we will explore ways how to best transition existing applications in the realm of key exchange and secure messaging in light of this predicament.