Quantum Secure Key Exchange for IEEE 802.1AE (MACSec)

In the last 40 years, quantum computing developed from an exclusively theoretical description of a quantum Turing machine to real-world implementations with various technologies and capabilities. Linking this development to the rapid development of the digital computer in the 20th century, a quantum computer with practical implications on industry and everyone's daily life seems within reachable bounds. There are many reasons to seek such a practical implementation. From algorithmic improvements to completely new technical possibilities like quantum teleportation, a quantum computer promises to solve certain tasks faster than it would be possible with a classical digital computer.

Besides the benefits such a computer could provide it would also have a significant impact on the field of cryptography. Modern cryptography protocols in general and especially the field of public-key cryptography relies on mathematical problems that are believed to be intractable. Famous examples of such algorithms are the RSA and the Diffie-Hellman (DH) key exchange protocol and its variant, Elliptic Curve Diffie-Hellman (ECDH). As of today, nearly all encrypted messages in the modern Web are bootstrapped by either one of these protocols. A serious flaw in these cryptosystems would have a massive impact on the confidentiality of user data. This is where quantum computing comes into play. In 1999 Peter Shor published his famous algorithm, which uses a quantum computer to break both, the RSA and the DH problem. Since Shor was able to show that both algorithms run in polynomial time, the foundation of modern cryptography is questioned.

Luckily, even more than 20 years later, there is no implementation of a quantum computer available that could be used to break cryptographic keys of reasonable size. While this may not be true in a more distant future, an ever-growing effort was introduced to find alternative, quantum-safe, cryptosystems for which no such attack exists.

A common downside in these systems is the rather large amount of traffic or computational overhead these algorithms introduce when compared to the existing RSA or DH-based implementations. For this reason and to get a better understanding of the requirements, another important task is the adaptation of quantum-safe algorithms in existing cryptographic protocols like IEEE 802.1X and 802.1AE.

IEEE 802.1X focuses on the mutual authentication of clients in IEEE 802.1 Ethernet LAN networks. For this purpose, the EAP protocol is used with asynchronous, certificate-based approaches of authentication that are directly affected by Shor's algorithm. Furthermore, 802.1X makes use of public-key cryptography and key exchanges to agree on a symmetric key between the clients and the connected network equipment, which is further used by IEEE 802.1AE to encrypt ethernet frames and provide confidential communication in a LAN segment. The symmetric primitives used in IEEE 802.1AE are also subject to another attack first described by Lov Grover, which reduces the effective key space of these primitives by a quadratic factor. Other than Shor's algorithm the implications are not as drastic, since they

can be relatively easily mitigated by increasing the key space accordingly. Both protocols are of special interest for a quantum-safe implementation for two reasons:

1. The wide adoption of these protocols in enterprise-grade networks makes them an important security measure in modern computer networks. They allow to control access to a network and prevent eavesdropping of local communication.
2. Both protocols are specified for generic IEEE 802.1 LAN networks and cover a broad range of environments. A quantum-safe implementation of these protocols could yield interesting insights into requirements on quantum-safe algorithms and protocols in general.

Goals of this work:

- Study of the IEEE 802.1X and 802.1AE protocols to identify components that are vulnerable to an attacker with access to a practical quantum computer.
- Isolation of requirements for a quantum-safe design of this protocols
- A proposal for a quantum-safe design that takes the requirements into account and an implementation of this design in an experimental setting
- A extensive experimental evaluation of the provided design and comparison with their classical counterpart.