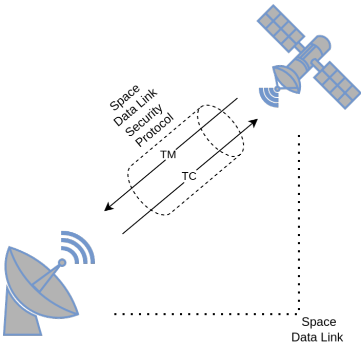
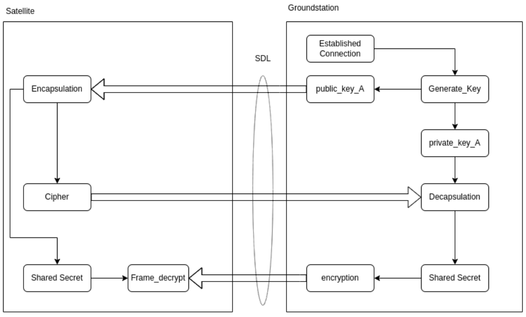
A Quantum Safe Space Data Link

With the advances in the field of quantum computation also comes the drawback of new security issues in traditional encryption protocols. New Protocols have already been found and are in the process of ratification. The Problem now lies in the implementation of said protocols.



Space Data Link



Kyber Implementation in the Project

The Problem

The Space Data Link Security Protocol (SDLS) is currently not secured against Quantum computer attacks. However, this can be changed by using the Kyber encapsulation algorithm. But before the Kyber could be implemented, another public key protocol was used to create a proof of concept. For this, a simple Server/Client TCP connection has been established as a host for the SDLS.

ECDH

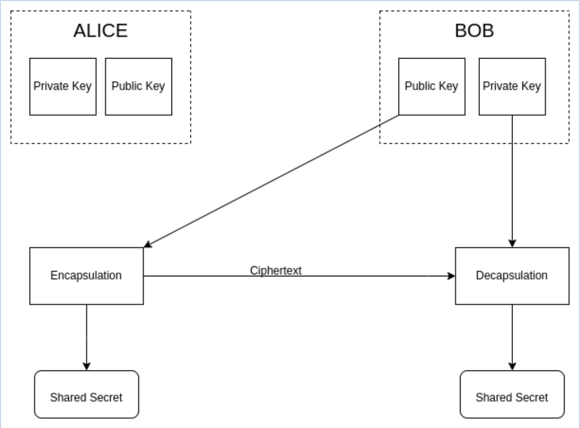
To achieve the proof of concept, that a public key exchange protocol could be used with the SDLS, the ECDH is added to the protocol. However as the existing SDLS protocol only supports rekeying over an encrypted connection, a new method for storing the session key had to be implemented. With this, the ECDH was added to the SDLS and the proof of concept was functioning.

Kyber

With this proof of concept now the post-quantum encryption can be added. To establish this implementation, the ECDH is replaced with the Kyber. As the algorithm for the key exchange (not the encryption algorithm) is quite similar, there are only a few things that need to be changed to have a working Kyber implementation.

What is the Kyber?

The Kyber is a post-quantum key exchange protocol, that uses the Learning-with-Errors problem to generate a public and a private key for one of the two parties. This public key is then sent over an insecure connection to the opposite party where a shared secret is created and encapsulated. This is then sent back, where it is decapsulated using the public key. Now both parties have the same shared secret.



Project Team:
Matthias Bhend

Client:
Ateleris GmbH, Brugg

Coaches:
Prof. Dr. Christoph Wildfeuer,
Prof. Dr. Willi Meier

Repository:
`https://github.com/fhnw-ise-qcrypt/CCSDS-SDLC`