Offline (Quantum) Key Distribution II – Security Analysis

FI CODE Forschungsinstitut Cyber Defence Universität der Bundeswehr München

Master Thesis/ Bachelor Thesis

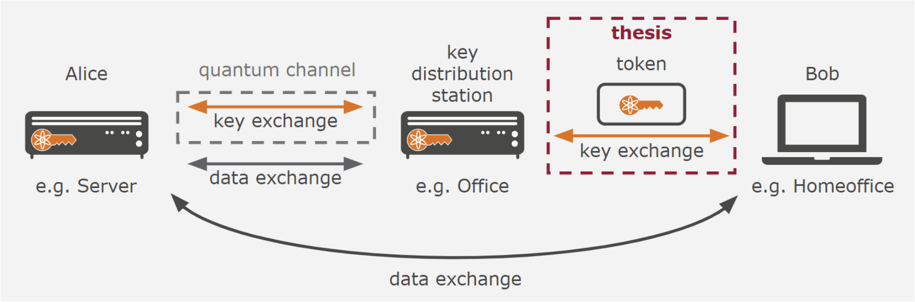
In the upcoming age of quantum computers, most common cryptographic techniques might become obsolete. It is, therefore, necessary to develop future-proof and resistant methods. Quantum Key Distribution (QKD) is such a method that uses the physical properties of quantum mechanics to provide two or more parties with a common, physically secure key for communication.

However, since direct fiber links and expensive QKD-hardware are required to exchange these keys, the question arises to whether cryptographic keys can also be transported offline. The following scenario describes the present problem in an exemplary manner.

Imagine Bob's office is connected via a quantum-encrypted connection to a server. This means, that there are two channels connecting the server and Bob's office:

1. **Quantum channel (via. fibre):** This channel is used for the key distribution between Alice and Bob. The keys are send as qbits, meaning that interceptions can be recognized (e.g., whether someone read the key). Once a key reaches its destination it is translated to "normal" bits.
2. **Classical channel:** This channel is used to exchange data that is encrypted with the previously exchanged keys.

But how does Bob access the server from his home office if he has no direct fiber connection and also no QKD hardware at home? Well, Bob could get keys in his office and save them on his personal key-transport token. He could subsequently use the token at home and use the stored key to encrypt his communication with the server. We, therefore, recently conducted a first master thesis on how such a hardware token could look like, while largely focusing on usability aspects and user perception. Even outside the QKD context, the topic of "offline distribution of cryptographic keys" is interesting for researchers and practitioners alike.



Possible BA/MA thesis: Your thesis would evolve around the evaluation of already existing consumer devices that could be used to store and transport QKD-keys (or symmetric cryptographic keys in general).

Research questions:

- State of the Art: Which devices for "offline key distribution" exist and are they appropriate for this application?
- Security: Which security features, but also vulnerabilities have these devices in common? Are there attack vectors specific to token-based transport of cryptographic keys?

Recommended Skills & Interests:

- interest in IT-Security and Usable Security (= creating usable security mechanisms)
- knowledge/interest in the area of vulnerability analysis
- independent thinking and creative problem solving

Contact: Sarah Delgado Rodriguez (sarah.delgado@unibw.de)