Offline (Quantum) Key Distribution

Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

Master Thesis/ Bachelor Thesis

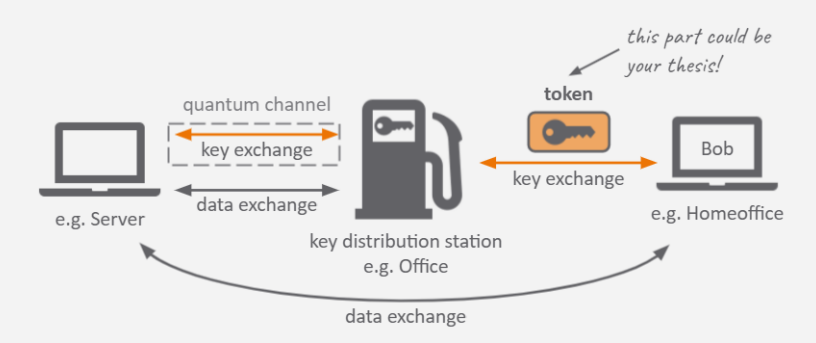
In the upcoming age of quantum computers, most common cryptographic techniques might become obsolete. It is, therefore, necessary to develop future-proof and resistant methods. Quantum Key Distribution (QKD) is a method that uses the physical properties of quantum mechanics to provide two or more parties 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 as 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. fiber):** This channel is used for the key distribution between Alice and Bob. The keys are sent 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-safe token. He could subsequently use the token at home and connect to the server. Hence, even outside the QKD context, the topic of offline distribution of cryptographic keys is interesting for researchers and practitioners alike.



Exemplary research questions:

- Which use cases for offline key distribution exist?
- How could this token look like (design, usability, and security)?
- How could the token be transported? Is there a possibility to detect unauthorized access to the token?
- How do humans interact with such a token?

Possible BA/MA thesis:

- conceptual considerations regarding offline (quantum) key distribution based on related literature, usability, or security analysis
- development and evaluation of a prototypical key distribution/transport token based on users' needs

Recommended Skills & Interests:

- interest in Usable Security (= creating usable security mechanisms)
- knowledge in the area of human-computer interaction & qualitative and/or quantitative research methods
- independent thinking and creative problem solving

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