Quantum Key Reconciliation Application

Supervisor: Armando Pinto (anp@ua.pt)
Collaborator: Diogo Matos (dftm@ua.pt)
Keywords: Quantum technologies, Cryptographic keys, Key reconciliation
Number of team elements: 4 to 5

Context

With the surge of quantum computers current public cryptographic schemes are potentially compromised. Quantum Key Distribution (QKD) have been emerging as a technology able to generate cryptographic keys in a secure way. QKD enables the negotiation of cryptographic keys in a secure manner without relying on computational complexity to achieve its security. In a QKD Network (QKDN), raw keys are first generated by the physical quantum layer; then the raw material goes through a post-processing phase (the reconciliation) to generate the cryptographic keys that are going to be stored in the Key Management System (KMS) which, ultimately, provide them to the applications that need them. For such a system to correctly operate, in the reconciliation phase, a pair of nodes must cooperate to distillate cryptographic keys from the raw key material received from the quantum layer.

Proposed objectives

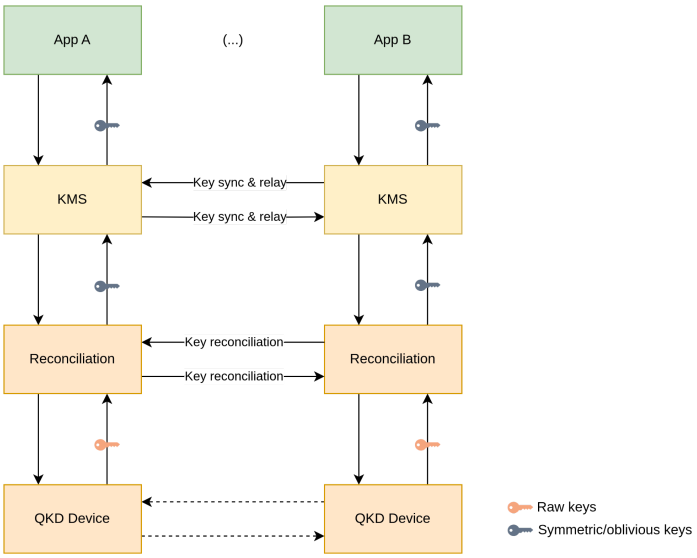

Fig. 1 - High-level two node QKDN architecture.

This proposal aims at contributing actively to the development of a quantum key reconciliation application. This application must:

- Retrieve raw key material from the QKD devices.
- Distillate both symmetric and oblivious keys in a coordinated protocol with another peer reconciliation application. Assuring correctness, security and efficiency.
- Provide the generated keys to the KML.

- Follow international and EU standards specified by institutions such as ETSI[1] and ITU-T[2].

The work done in this project will complement the work that is being done by IT in the scope of multiple projects, such as Discretion[3], QuantaGenomics[4] and PTQCI[5].

We expect the group to work on these major topics:

- Study the main standards and protocols related with quantum key reconciliation and management;
- Implement the reconciliation application starting from a simple proof-of-concept implementation;
- Document all developed work;
- Integrate and validate the developed solution in a test QKDN available at IT's laboratories.

Milestones

1. Study all essential background.
2. Analyze the work done previously by IT in the scope of the project.
3. Implement all the communication interfaces ensuring robustness and standard specifications.
4. Further develop and extend the reconciliation algorithms and protocols.
5. Benchmark the solution.
6. Test the solution in the lab.

[1] https://www.etsi.org/
[2] https://www.itu.int/
[3] https://discretion-eu.com/
[4] https://quantagenomics.av.it.pt/
[5] https://ptqci.av.it.pt/