Quantum Key Reconciliation Application

Tiago Pereira, David Cobileac, Diogo Marto, Vítor Santos
Orientador: Prof. Armando Pinto

Projeto em Informática, 3º ano, LEI.

2024

Introduction

Classical asymmetric cryptograpy is vulnerable to quantum algorithms. Our projects takes part in a solution to this problem: **Quantum Key Distribution**. By using quantum channels to exchange key material, current eavesdropping methods won't be effective.

Our project revolves around the reconciliation layer, designed to obtain usable cryptographic keys from raw material.

QKD & Reconciliation

This project uses continuous variable quantum key distribution (**CV-QKD**), which, like most QKD schemes, uses a quantum channel to generate raw key material and a public channel to then obtain usable cryptographic keys. To extract usable cryptographic keys, reconciliation is performed over an authenticated public channel with classical post-processing methods. Information transmitted over this channel isn't enough for a potential eavesdropper to discover the final keys.

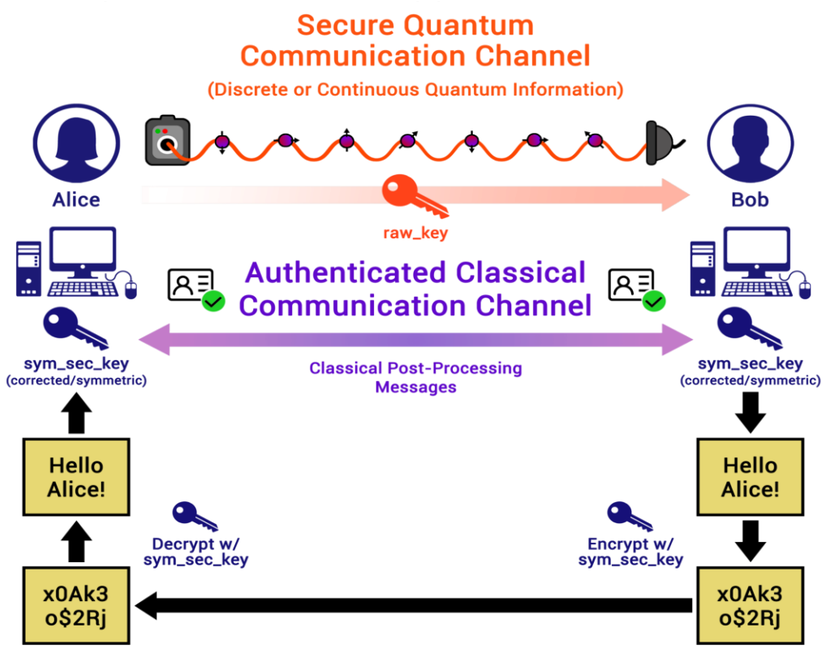

Fig 1- Quantum Key Distribution Overview.

Qeep - quantum-secure secret vaults

To demonstrate how QKD can be applied to real applications and use-cases, we developed **QeeP**, a platform for organizations to manage and exchange data using digital vaults and messaging systems, all secure with a quantum-secure communications system that uses **QKD** and **Reconciliation** to stave off eavesdroppers by using encrypted storage and communication, with quantum-generated keys.

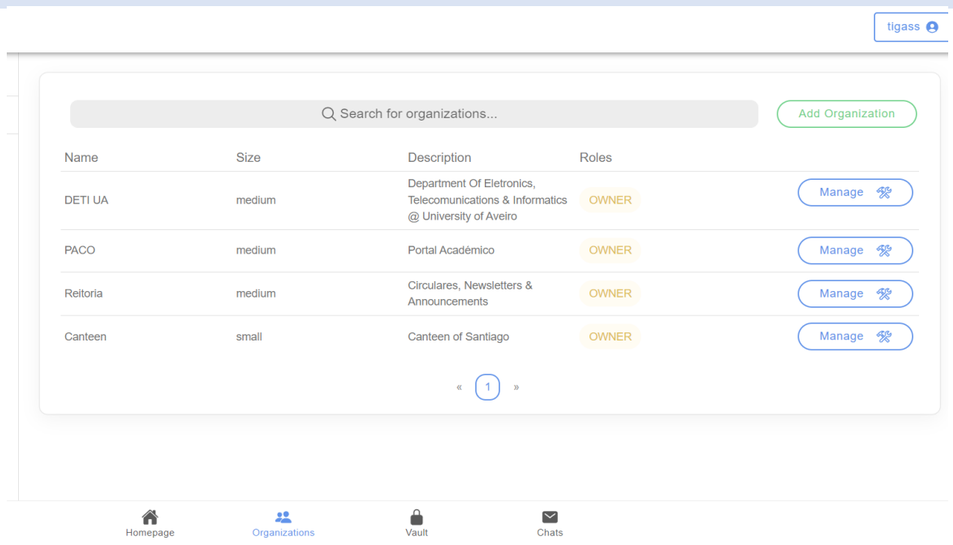

Fig 2- Part of Qeep Organizations Dashboard.

For **Qeep** & the QKD **Reconciliation** layer to effectively cooperate, we created a communication protocol to be implemented over the IP network.

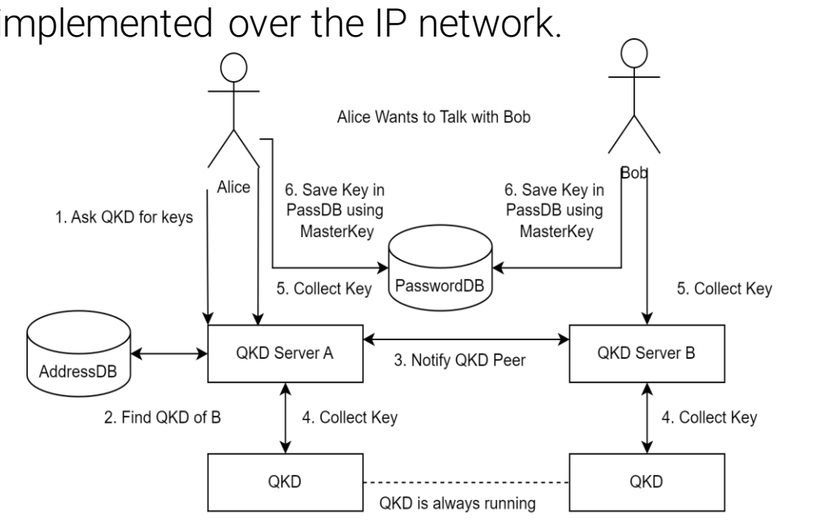

Fig 3- Project Expansion Communication Cycle.

Conclusion

More than ever, Privacy and Data Security are sought after and, more than ever, they're subject to complex threats & exploits. Our System, **using recent technological innovations,** provides the mean to protect sensible data from preying eyes while still promoting commodity and efficiency.

References

https://www.sioproject.pt/
https://ptqci.pt/
https://discretion-eu.com/
https://quantagenomics.av.it.pt/
https://www.it.pt/ITSites/Index/3

instituto de telecomunicações

universidade de aveiro
theoria poiesis praxis

deti departamento de electrónica, telecomunicações e informática