

MS4: Final Presentation

# Quantum Key Reconciliation Application

Team:

Diogo Marto	108298
David Cobileac	102409
Tiago Pereira	108546
Vítor Santos	107186

Orientadores:

Armando Pinto, IT  
Diogo Matos, IT

# Index



## Context & Vision

---

### Reconciliation

- Motive
- Requirements
- Process
- Results & Outcomes

### QeeP

- Motive
  - Goals
  - Architecture
  - Results
- 

## Conclusions

# Context

***“At the end of the day, the goals are simple:  
Safety & Security***

*- Jodi Rell*

**”**

# Context



**Quantum computers represent a possible future threat for current asymmetric crypto schemes with disastrous consequences.**



**Quantum Key Distribution aims to solve this by using eavesdropper-proof quantum channels to exchange symmetric keys.**



**Reconciliation is the phase of this process that outputs useful encryption keys.**

# PART 1

# Reconciliation



**Motive**



**Requirements**



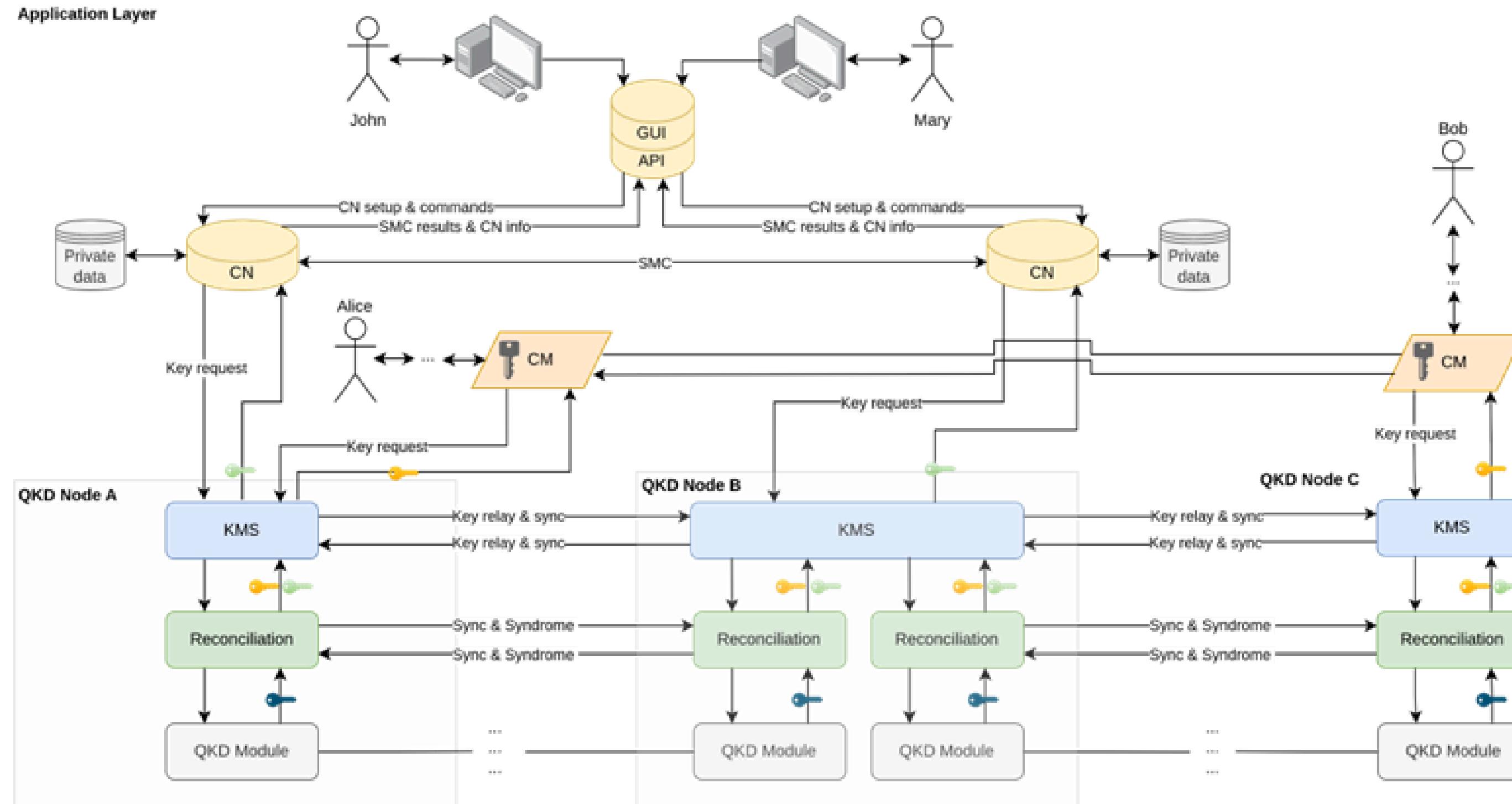
**Process**



**Results**

# Motive

## SYSTEM ARCHITECTURE

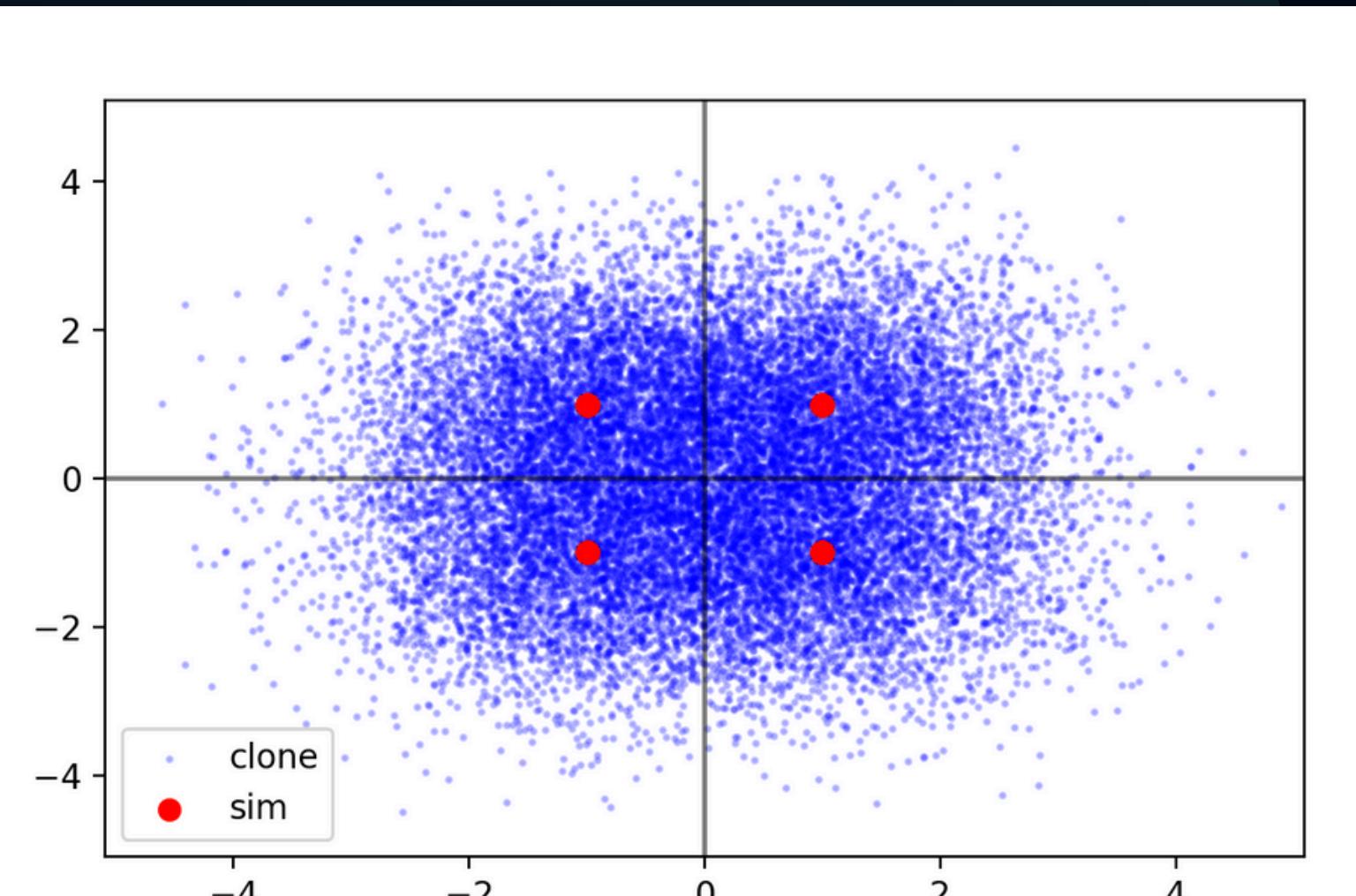


# Motive

## LAYER ARCHITECTURE

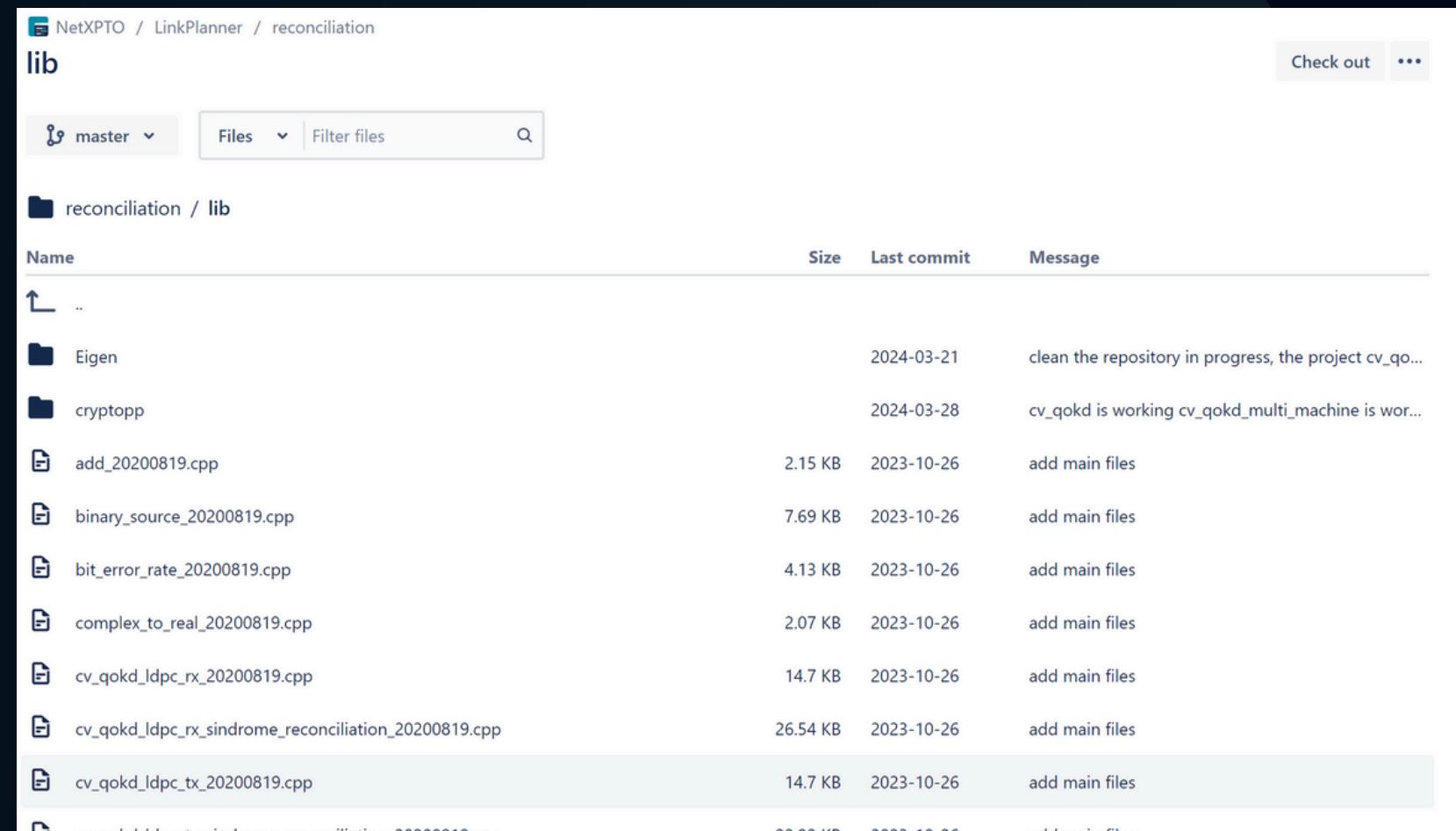
### Objectives

- Develop/Fix Solutions
- QKD Layer Emulation
- Communication Protocols
- Local Key Storage
- Comprehensible Docs



# State of the art

- Implementations of reconciliation already existed with different features
- Uses a library called netxpto written in C++
- Some implementations worked between 2 computers



The screenshot shows a GitHub repository interface for the 'reconciliation' branch of the 'lib' directory. The repository is named 'NetXPTO / LinkPlanner'. The table lists the following files:

Name	Size	Last commit	Message
..			
Eigen		2024-03-21	clean the repository in progress, the project cv_qo...
cryptopp		2024-03-28	cv_qokd is working cv_qokd_multi_machine is wor...
add_20200819.cpp	2.15 KB	2023-10-26	add main files
binary_source_20200819.cpp	7.69 KB	2023-10-26	add main files
bit_error_rate_20200819.cpp	4.13 KB	2023-10-26	add main files
complex_to_real_20200819.cpp	2.07 KB	2023-10-26	add main files
cv_qokd_ldpc_rx_20200819.cpp	14.7 KB	2023-10-26	add main files
cv_qokd_ldpc_rx_sindrome_reconciliation_20200819.cpp	26.54 KB	2023-10-26	add main files
cv_qokd_ldpc_tx_20200819.cpp	14.7 KB	2023-10-26	add main files
cv_qokd_ldpc_tx_sindrome_reconciliation_20200819.cpp	22.92 KB	2023-10-26	add main files

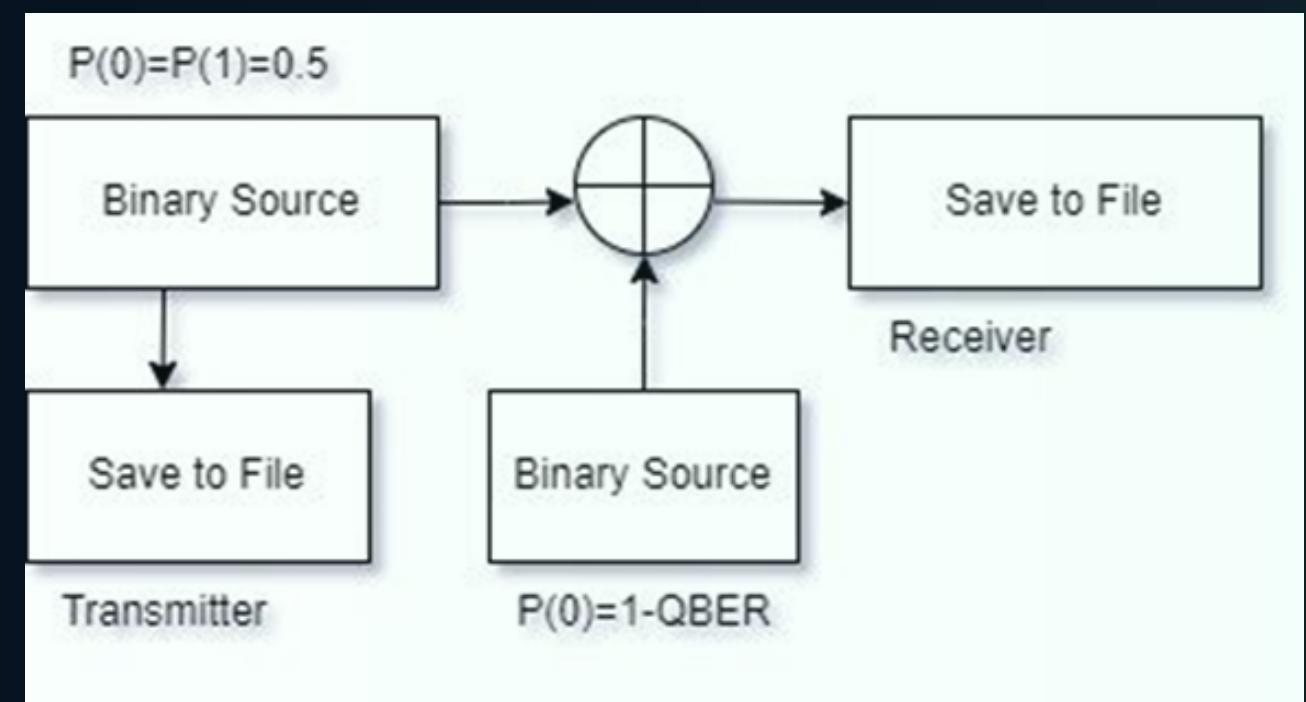
  


The screenshot shows a GitHub repository interface for the 'cv\_qokd\_ldpc' directory. The repository is named 'NetXPTO / LinkPlanner'. The table lists the following files:

cv_qokd_ldpc	2024-04-16	add a README.MD file
cv_qokd_ldpc_etsi_qkd_004	2024-03-29	trivial
cv_qokd_ldpc_multi_machine	2024-04-16	Complete README.md file
cv_qokd_ldpc_multi_machine_etsi_004	2024-04-16	Complete README.md file
cv_qokd_ldpc_multi_machine_messageHandler	2024-03-21	clean the repository in progress, the project cv_qokd_l...
cv_qokd_ldpc_multi_machine_messageHandler_etsi004	2024-03-21	clean the repository in progress, the project cv_qokd_l...

# Goals

- Create emulators capable of simulating QKD Devices
- Integrate emulators with reconciliation
- Integrate reconciliation with KMS



# Outcomes

The slide features the IQC logo at the top left. Below it is the title "Quantum Key Reconciliation Application". A list of associated institutions follows, including TÉCNICO LISBOA, universidade de aveiro, Escola Superior de Ciências, KTH Royal Institute of Technology, NOKIA, UNIVERSIDADE SÉRGIO MORAES, POLELO, ISCTE IUL, and IPL. To the right is a photograph of a quantum optics experimental setup with various optical components and monitors. Below the photo is a logo for the Instituto de Telecomunicações and the Universidade de Aveiro.

IQC quantum communications

Quantum Key Reconciliation Application

INSTITUIÇÕES ASSOCIADAS

TÉCNICO LISBOA  
universidade de aveiro  
Escola Superior de Ciências  
KTH Royal Institute of Technology  
NOKIA  
UNIVERSIDADE SÉRGIO MORAES  
POLELO  
ISCTE IUL  
IPL

Name(s): Diogo Marto, Vítor Santos, Tiago Pereira, Diogo Cobileac, Tiago Portugal  
Research Team: Reconciliation  
Role: 3<sup>rd</sup> Year project  
UA Course: LEI - PI  
Supervisors:  
Armando Nolasco Pinto  
Diogo Matos

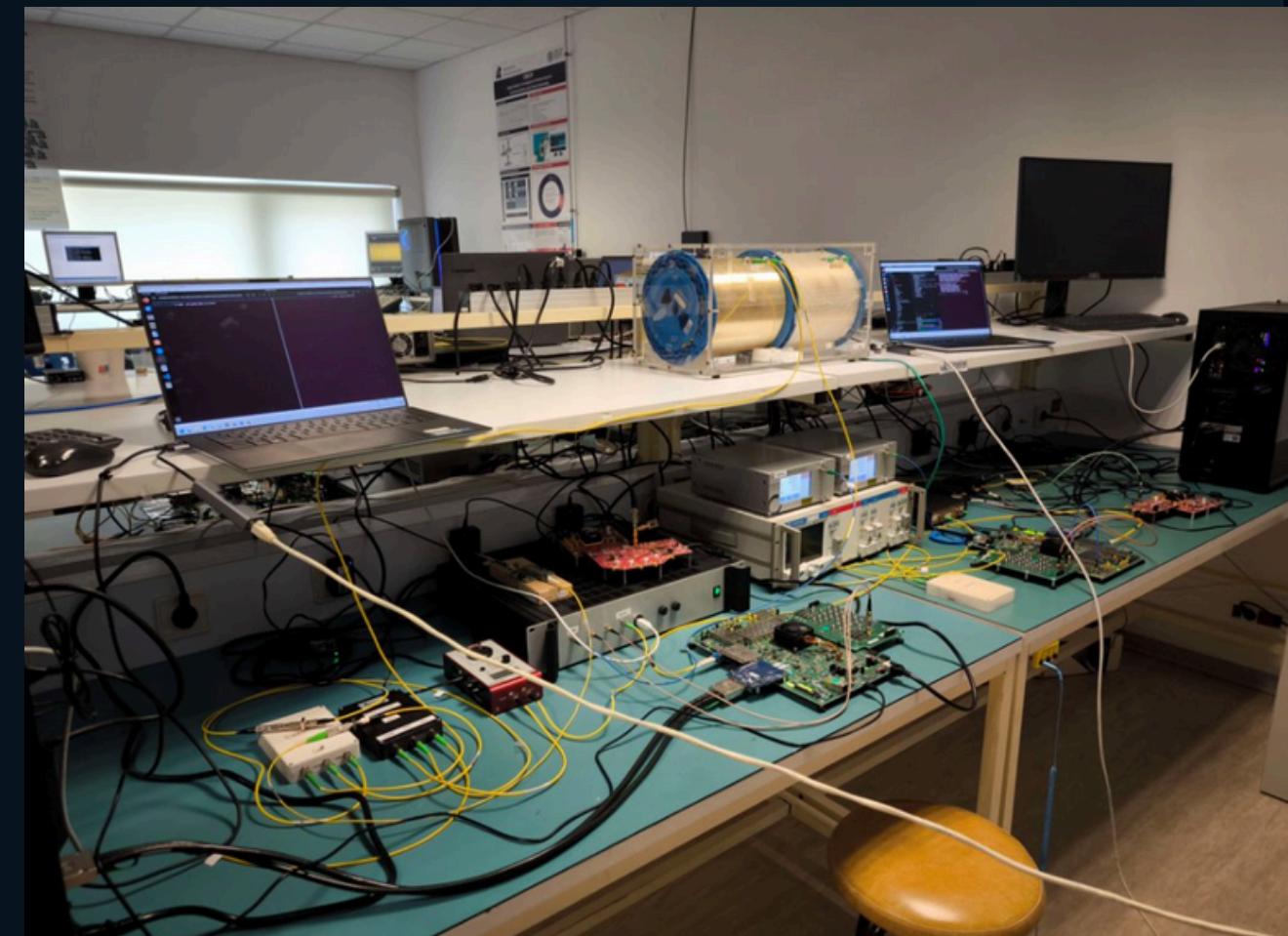
Group Meeting  
24 April

© 2012, Instituto de Telecomunicações

it instituto de telecomunicações

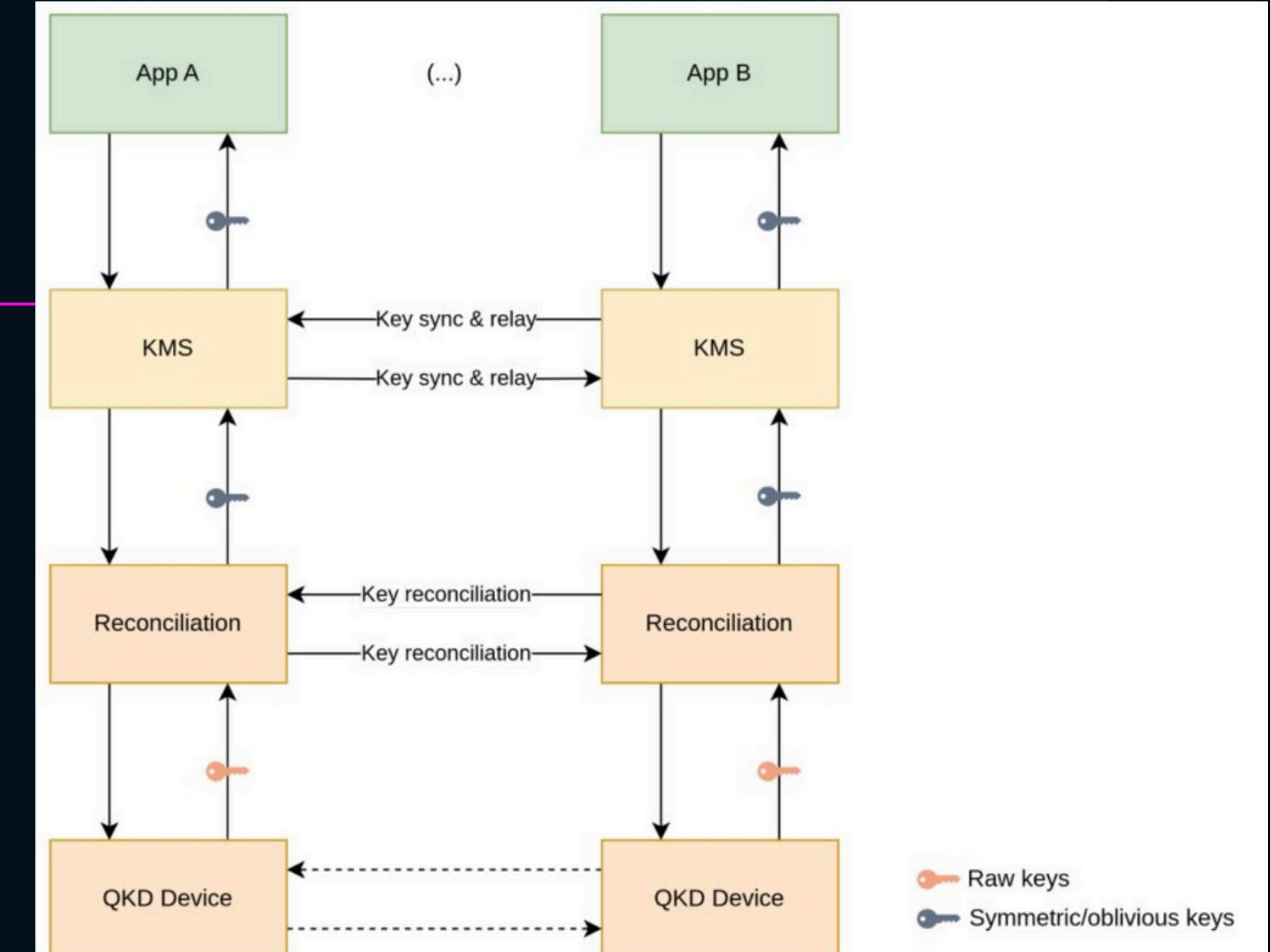
universidade de aveiro

- The actual source code and application
- Documentation of our work
- Demonstration
- Presentation



# Demonstration

- 4 computers in total, 2 on reconciliation and another 2 on KMS
- Was successful in processing raw keys into symmetric keys and storing them on KMS.



## PART 2



qEEP

? Motive

 Goals

 Architecture

 Results

# Motive

---

- Secrets management apps are pretty safe in their classical sense.
- QKD physical networking products already exist, but are too low-level.



**qEEP**



qEEP

# QeeP's Vision

---

- Why not both?
- Quantum-proof secrets management for both users and organizations
- Quantum-proof messaging platform

# State-of-the-Art

---

Password/secrets management - Bitwarden

- E2EE for all data, both in transit and at rest.
- Relies on a master password known by the end-user to derive an encryption key.
- Reliance on asymmetric cryptography for authenticity



# State-of-the-Art

---

Secure messaging - WhatsApp

- E2EE for all data, both in transit and at rest.
- Historical data backups using aforementioned master password mechanism.
- Modern Signal protocol for all messaging.



# State-of-the-Art

---

## Main takeaways

- SoA of secure storage and messaging platforms are NOT quantum-proof.
- Reference for E2EE data handling & new messaging protocol design.



# Requirements

## Analysis

Finding ways to achieve results

# Methodology

---

## **Unified Process' Requirement Analysis:**

- Domain & documentation research on QKD and secure protocols (Done)
- Interviewing target users and stakeholders (Done)
- Extensive research on critical system design and standards (Not done)

# Actors

---

- **Individual user** - QeeP's most basic secret management and messaging features
- **Organizational user** - QeeP's more advanced features, tailored for organizations
- **Organizational admin** - Advanced organization vault management features
- **QeeP admin** - website management

# Use cases

---

## Secrets management package

- **Authentication** - logging in, signing up... - all actors
- **Secrets management** - storing, retrieving, deleting - all actors
- **Organization management** - vault ops, inviting users - organizational admin

## Messaging package

- **Messaging** - sending simple text with attached media - all actors
- **Device linking** - loading message history onto different devices - all actors

# Non-functional

---

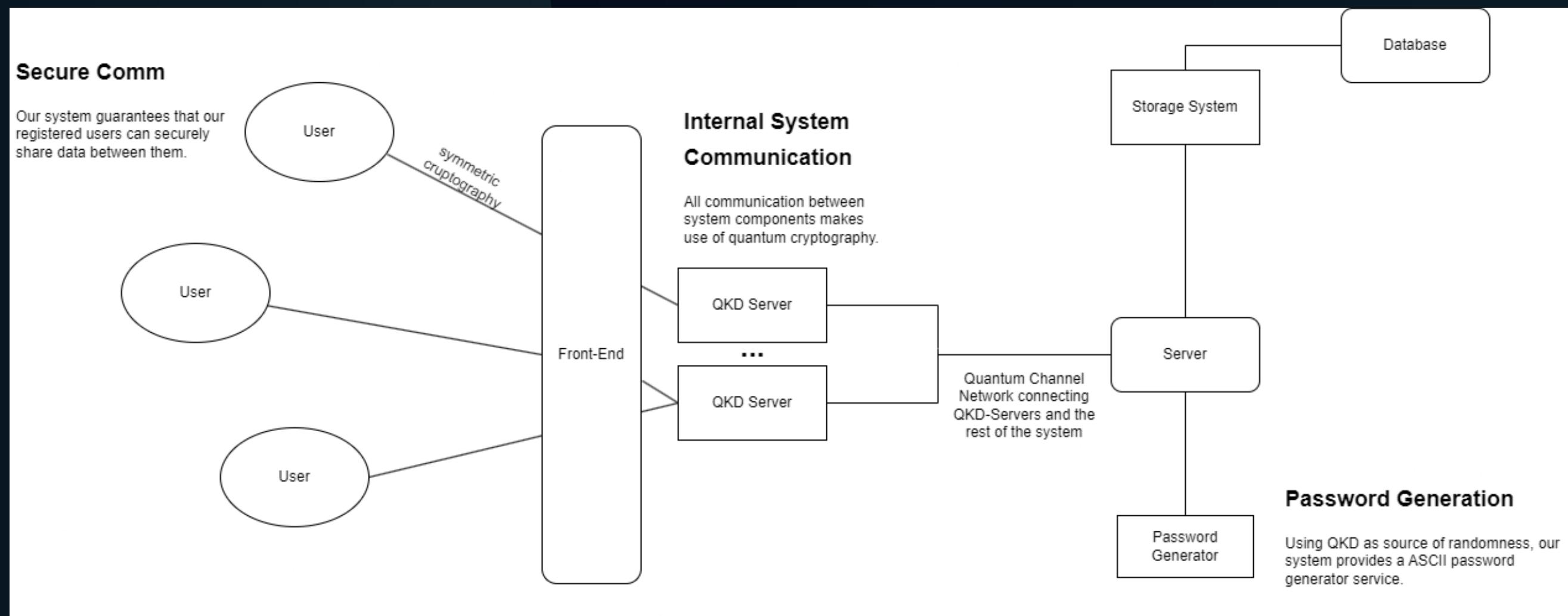
## Of note:

- **Security**: Elephant in the room
  - Focus of the project and extremely critical given the context
- **Usability**: A lesson from WhatsApp vs Signal
  - The less cumbersome one wins. Balance with the previous point.
- **Reliability**: High usage rates

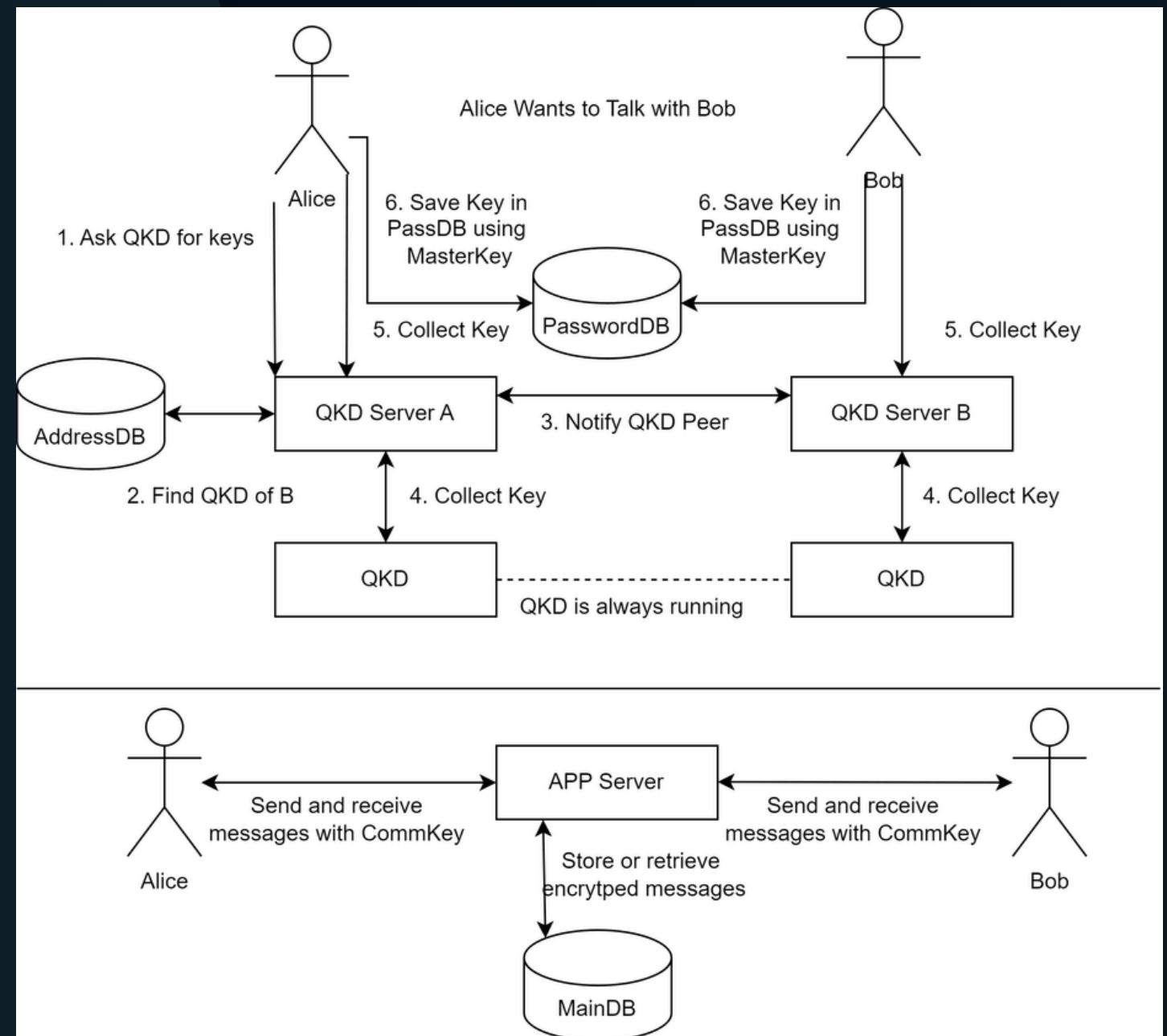
# Architecture Analysis

Finding ways to better results

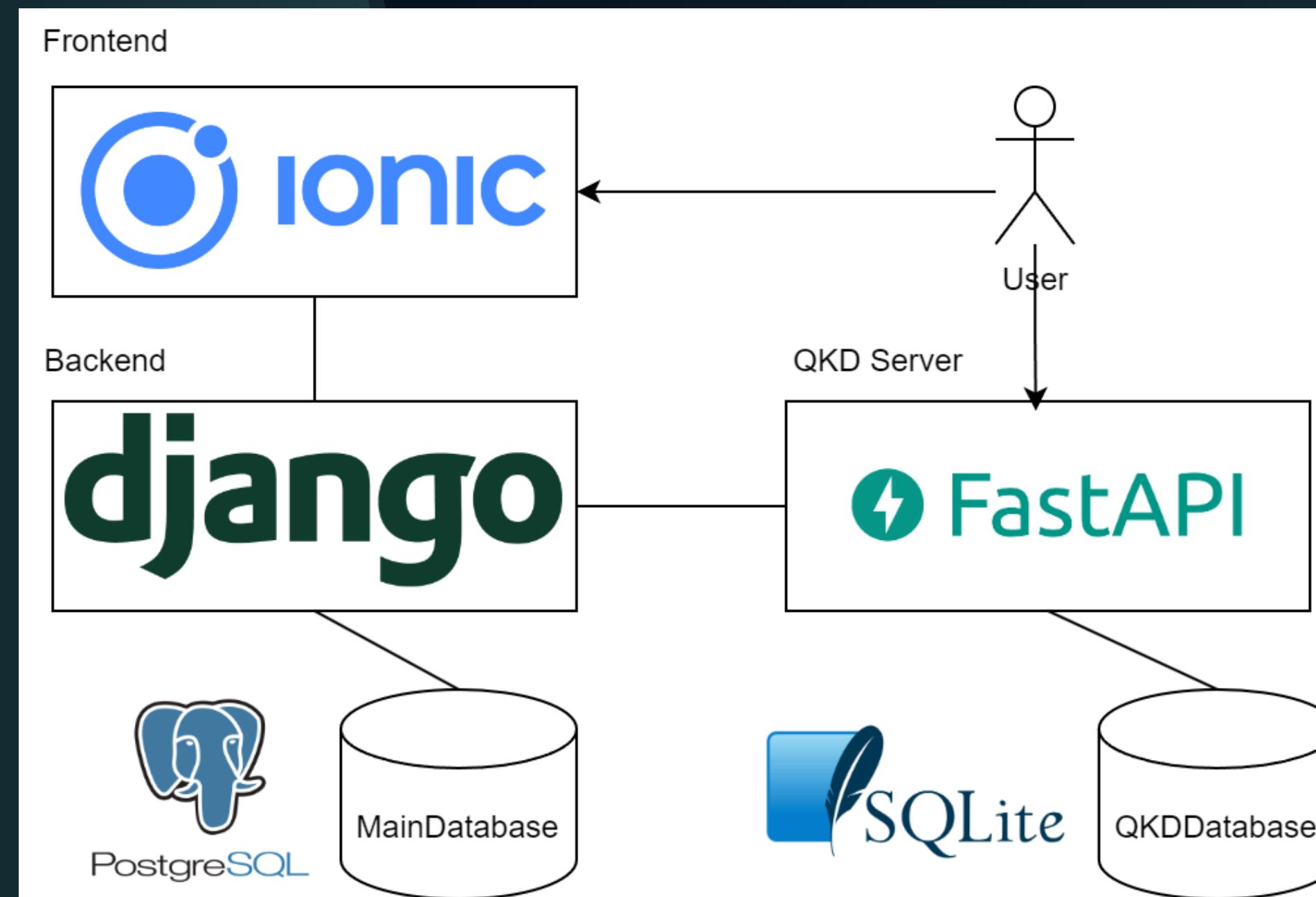
# Communication



# Architecture



# Implementation

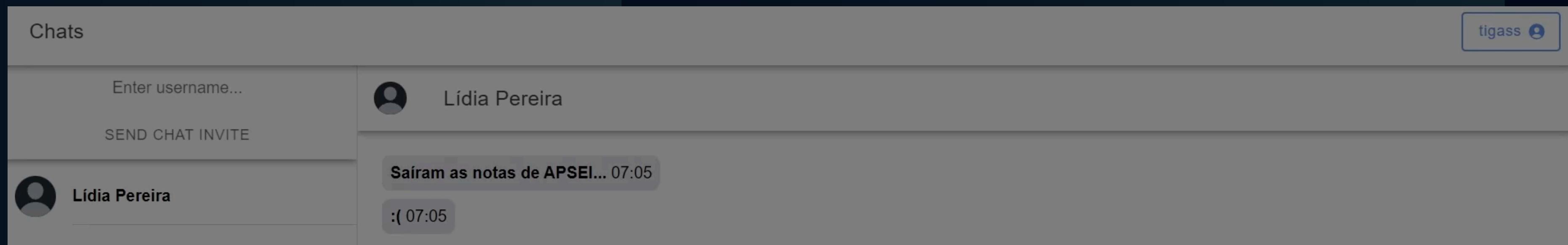


# Results & Outcomes

# Results & Outcomes

---

- Quantum Chat System



# Results & Outcomes

- Quantum Vaults
- Highly-Modular Secret Data Management Ecosystem

The screenshot shows a user interface for managing organizations. At the top right, there is a user profile icon labeled "tigass". Below the header, there is a search bar with the placeholder "Search for organizations..." and a green "Add Organization" button. The main content area displays a table with four rows of organization data:

Name	Size	Description	Roles	Action
DETI UA	medium	Department Of Eletronics, Telecommunications & Informatics @ University of Aveiro	OWNER	<a href="#">Manage</a> <a href="#"></a>
PACO	medium	Portal Académico	OWNER	<a href="#">Manage</a> <a href="#"></a>
Reitoria	medium	Circulares, Newsletters & Announcements	OWNER	<a href="#">Manage</a> <a href="#"></a>
Canteen	small	Canteen of Santiago	OWNER	<a href="#">Manage</a> <a href="#"></a>

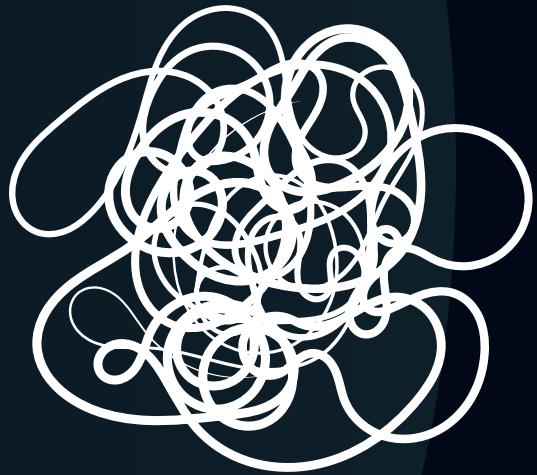
At the bottom center of the table, there is a page number "1" inside a blue circle, indicating the current page. Below the table, there is a navigation bar with four items: "Homepage" (home icon), "Organizations" (people icon), "Vault" (padlock icon), and "Chats" (envelope icon).

# Main Challenges

---

Project management issues:

- **Insufficient** and **inefficient** communication with advisor during initial phase – significant delay in development.
- Consensus on design issues was **turbulent** up until the end.
- In this time-sensitive, rapidly shifting scenario, the UP methodology started to **fall short**.
- Missing member...



# Conclusions

---

- Real project value was started too late -> Increased Challenge
- Implementing and testing novel security mechanisms is a time-consuming and constantly shifting venture.
- Fundamental takeaway: the value of communication and negotiation.

MS4: Final Presentation

# Quantum Key Reconciliation Application

Team:

Diogo Marto	108298
David Cobileac	102409
Tiago Pereira	108546
Vítor Santos	107186

Orientadores:

Armando Pinto, IT  
Diogo Matos, IT