QUANTUM KEY RECONCILIATION APPLICATION

Diogo Marto, **108298**

David Cobileac, **102409**

Tiago Pereira, **108546**

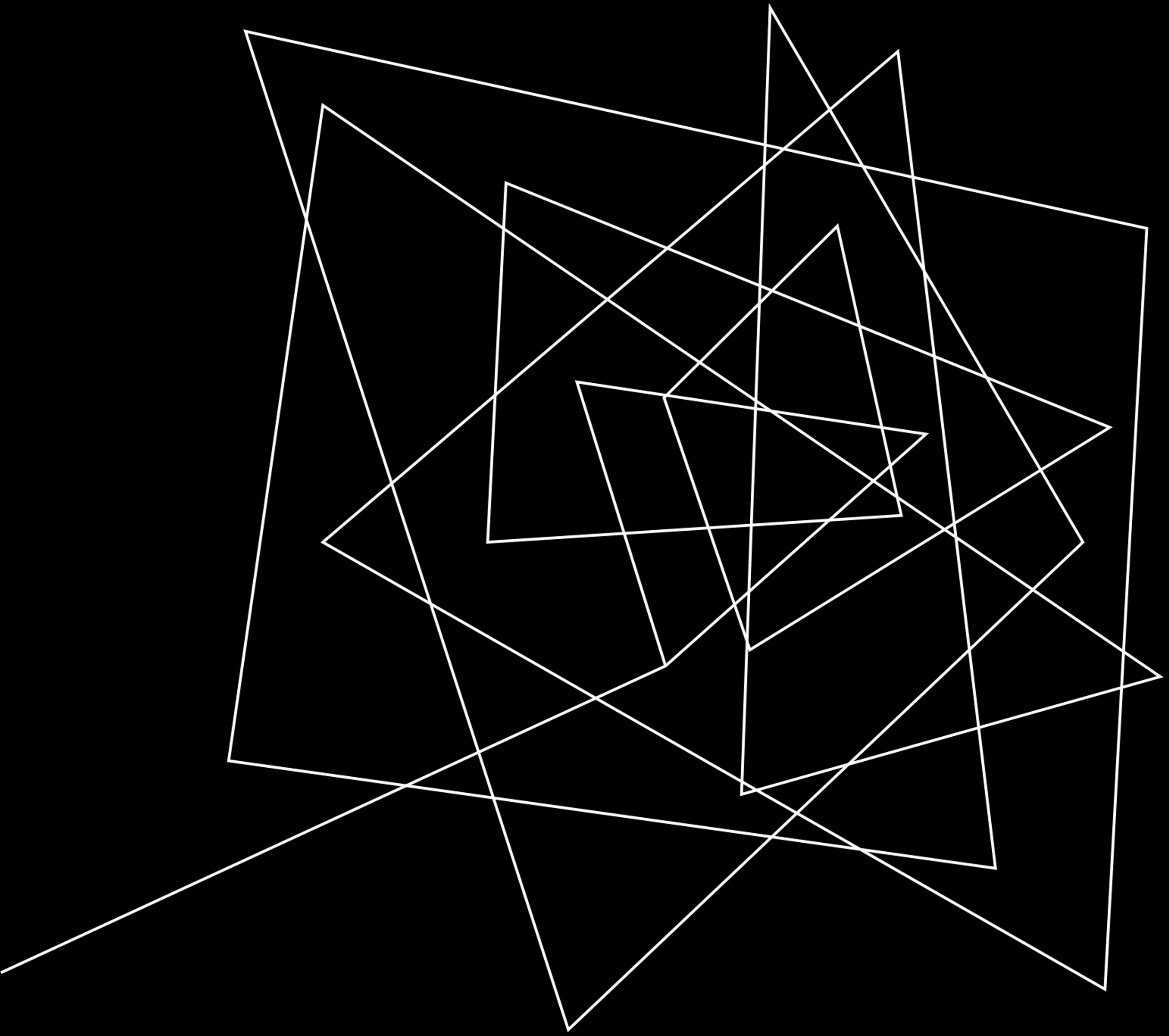
Tiago Portugal, **103931**

Vítor Santos, **107186**

Orientadores:

Armando Pinto (anp@ua.pt)

Diogo Matos (dftm@ua.pt)



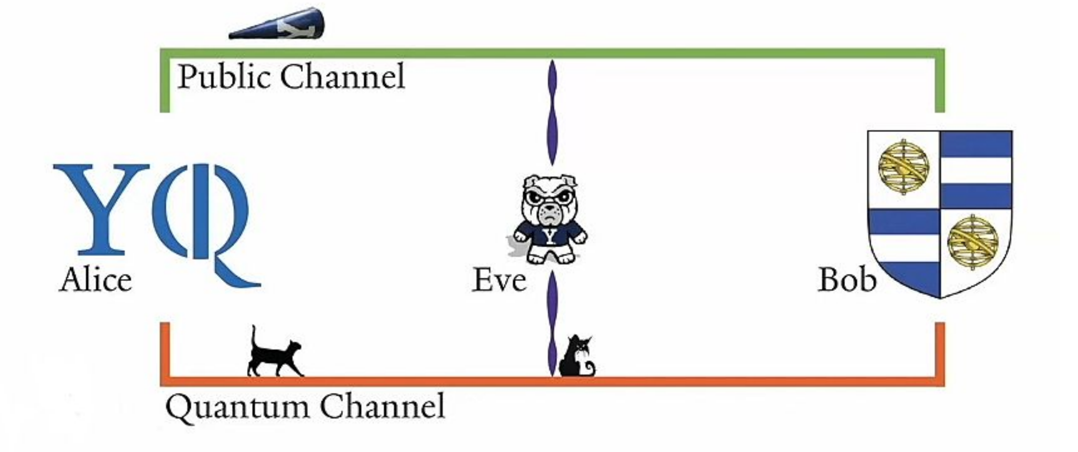
CONTEXT

2ND QUANTUM REVOLUTION

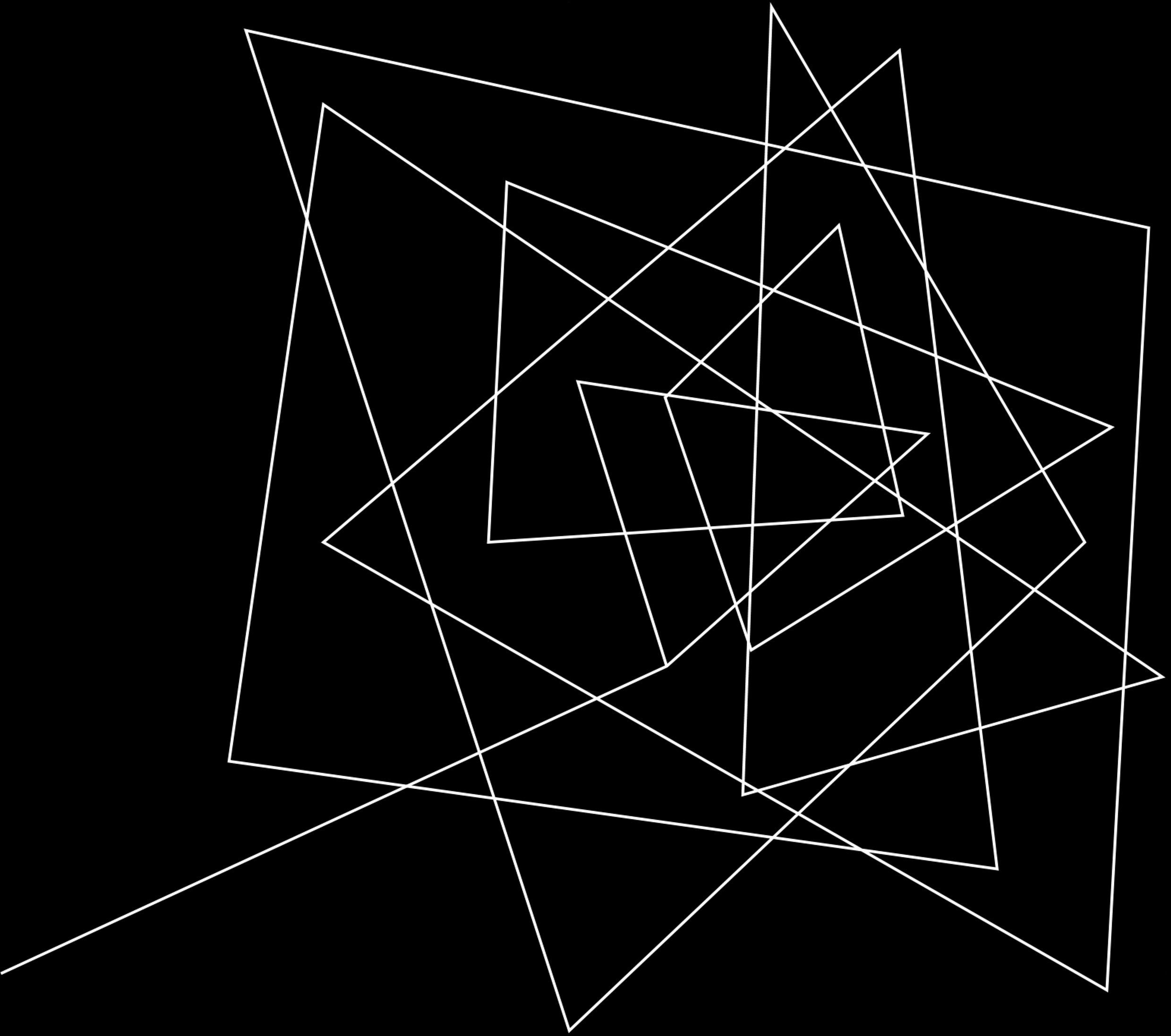
- **Quantum Computers**
- **Impossibly hard** decryption algorithms can be made **possible** (Shor's algorithm)
- Current **public key** distribution schemes potentially **compromised**

QUANTUM CRYPTOGRAPHY

- **Quantum Key Distribution** (QKD)
- **Protect** cryptographic keys from **eavesdroppers**
- Exploits **uncertainty** of quantum mechanics with "qubits"
- Simply seeing changes the state, detects eavesdropping
- No cloning theorem



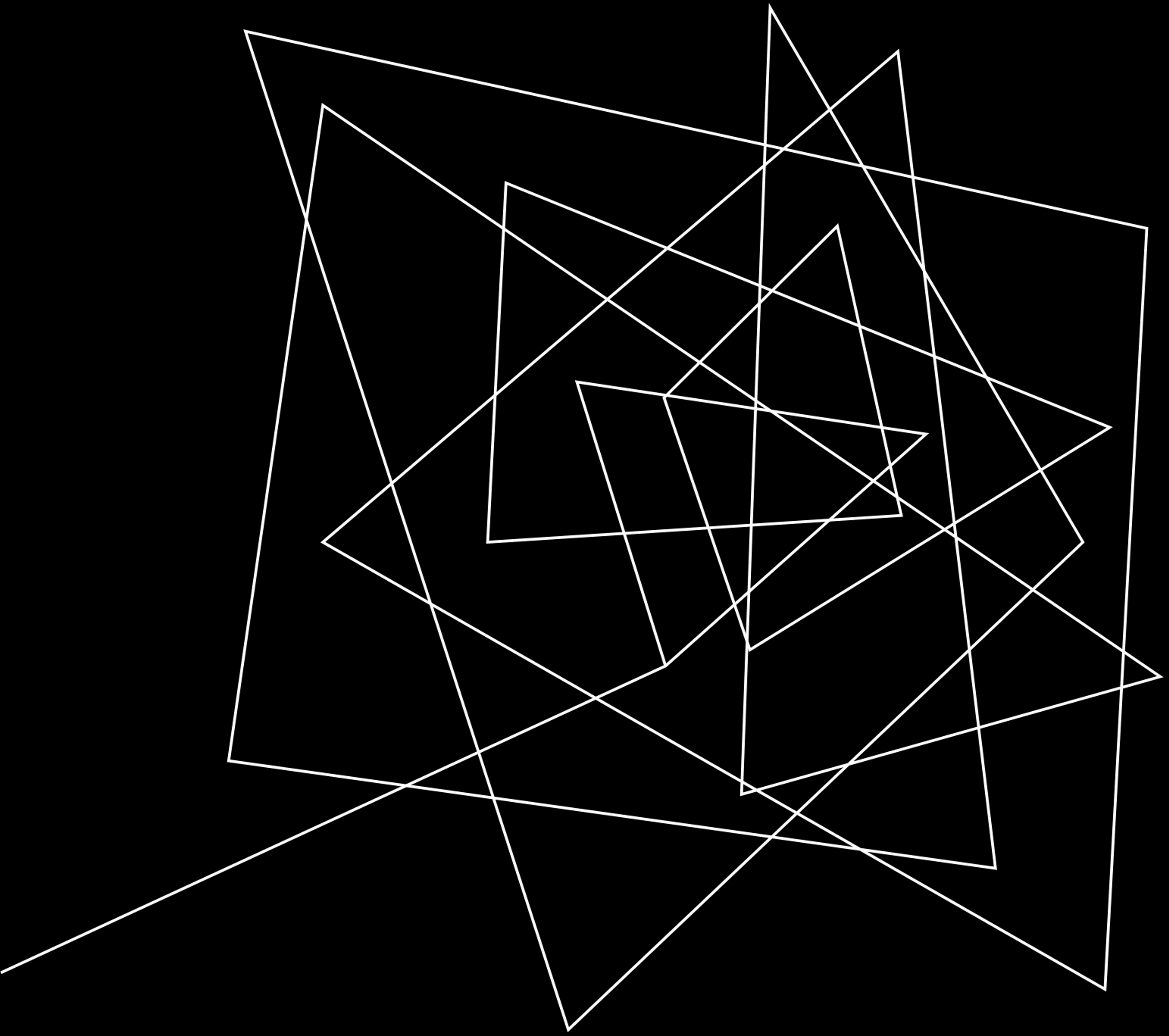
https://www.youtube.com/watch?v=PZFp_JTERRk



PROBLEM

RECONCILIATION

- Communication over the quantum channel is **random** (prone to errors)
- How to correct them? **Reconciliation**.
- Uses the **public channel** (not quantum, but still safe to use)



PRIMARY GOALS

GOALS

- 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.

it 30 YEARS instituto de telecomunicações

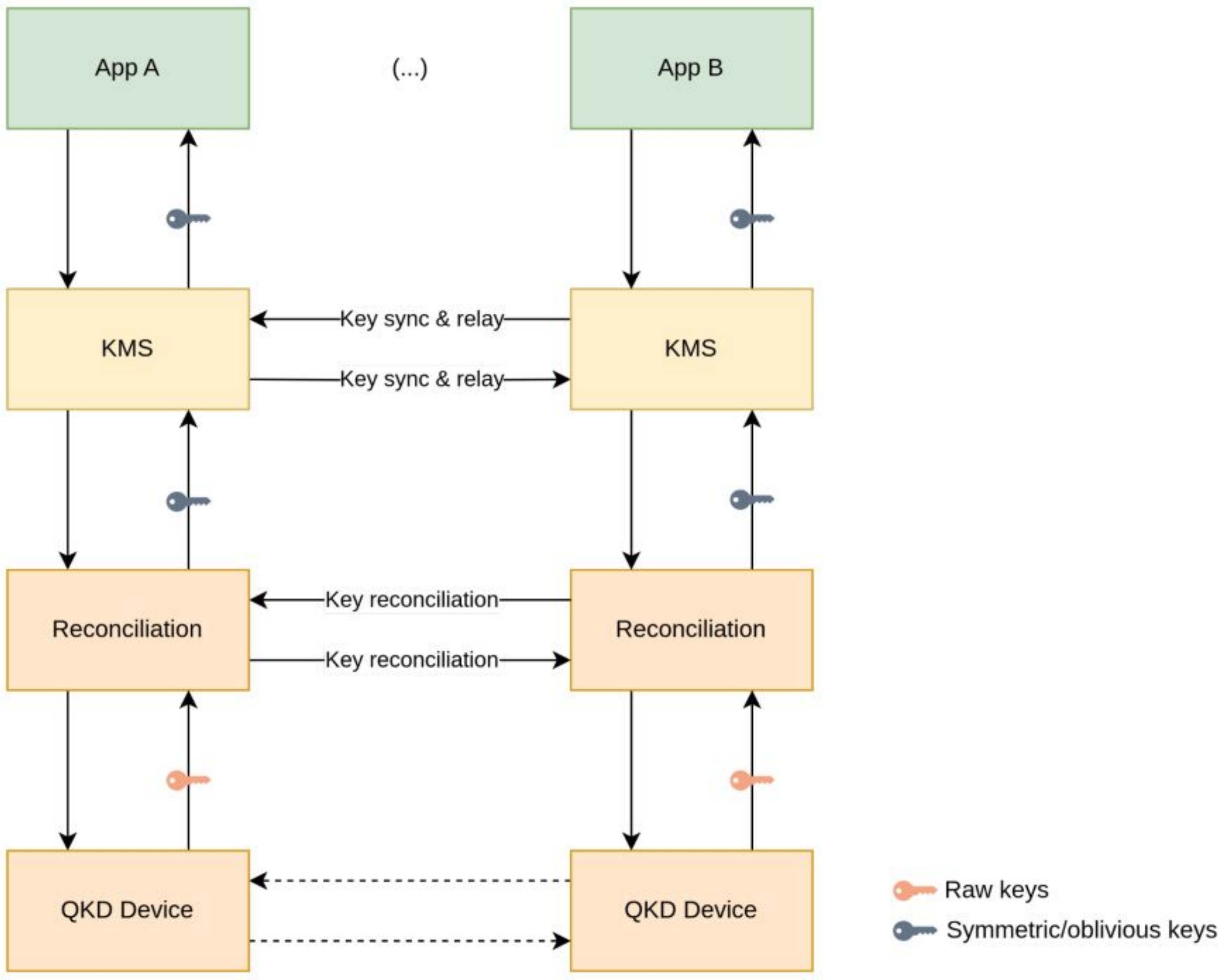
RELATED WORKS

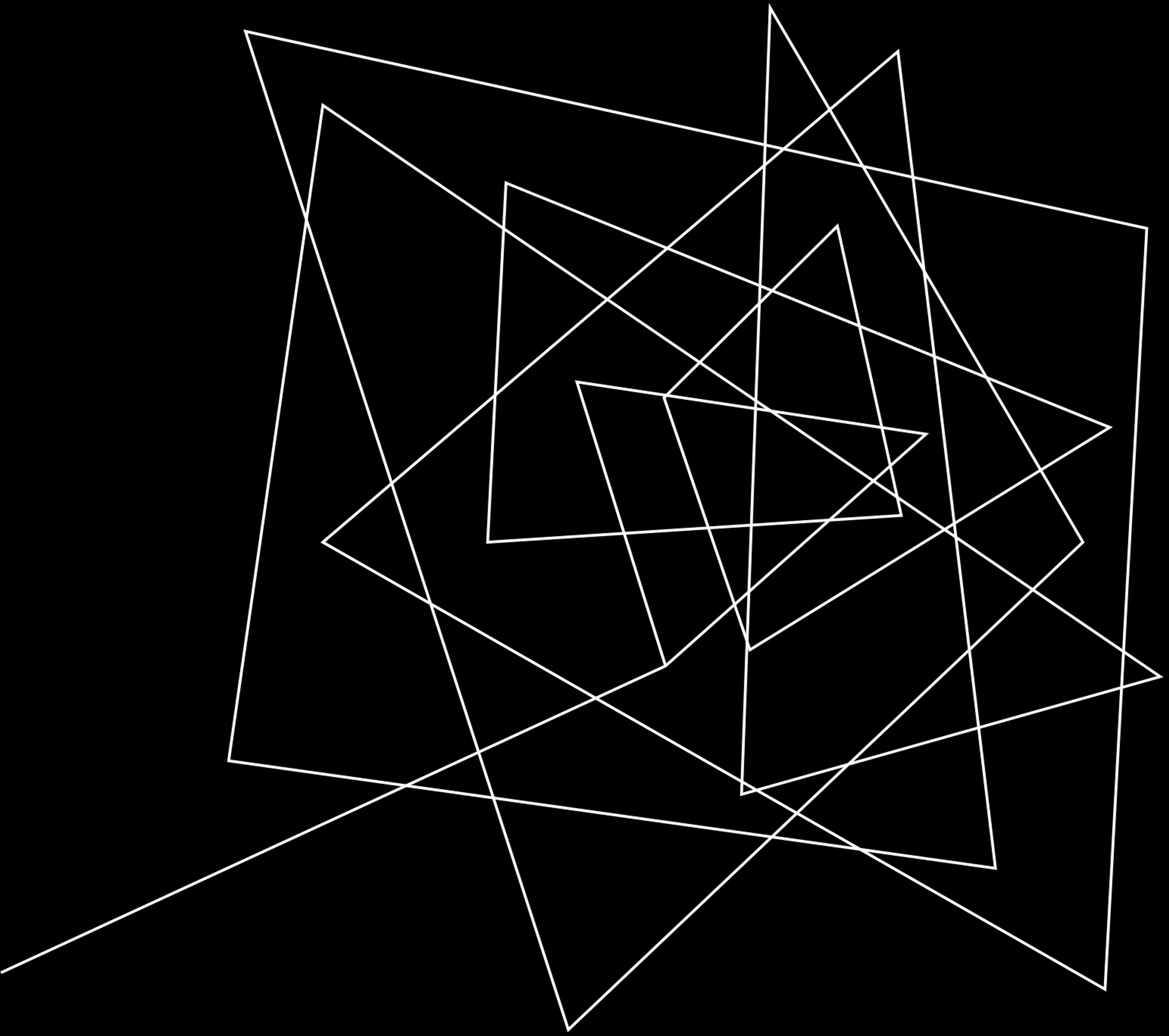
QuantaGENOMICS

DISCRETION

PTQCI

EXPECTED RESULTS





TASK LIST

TASK LIST

Module: Communication (**David Cobileac, Tiago Portugal, Tiago Pereira, Diogo Marto**)

- Task 1 (**David Cobileac & Tiago Portugal**): Develop and manage the project's website, reports and presentations and roles definition.
- Task 2 (**David Cobileac & Tiago Portugal**): Manage the project's Git repository.
- Task 3 (**Tiago Pereira**): Manage project’s Jira page.
- Task 4 (**Tiago Pereira & Diogo Marto**): Design and create the project's poster for presentations

Module: Research (**Team**)

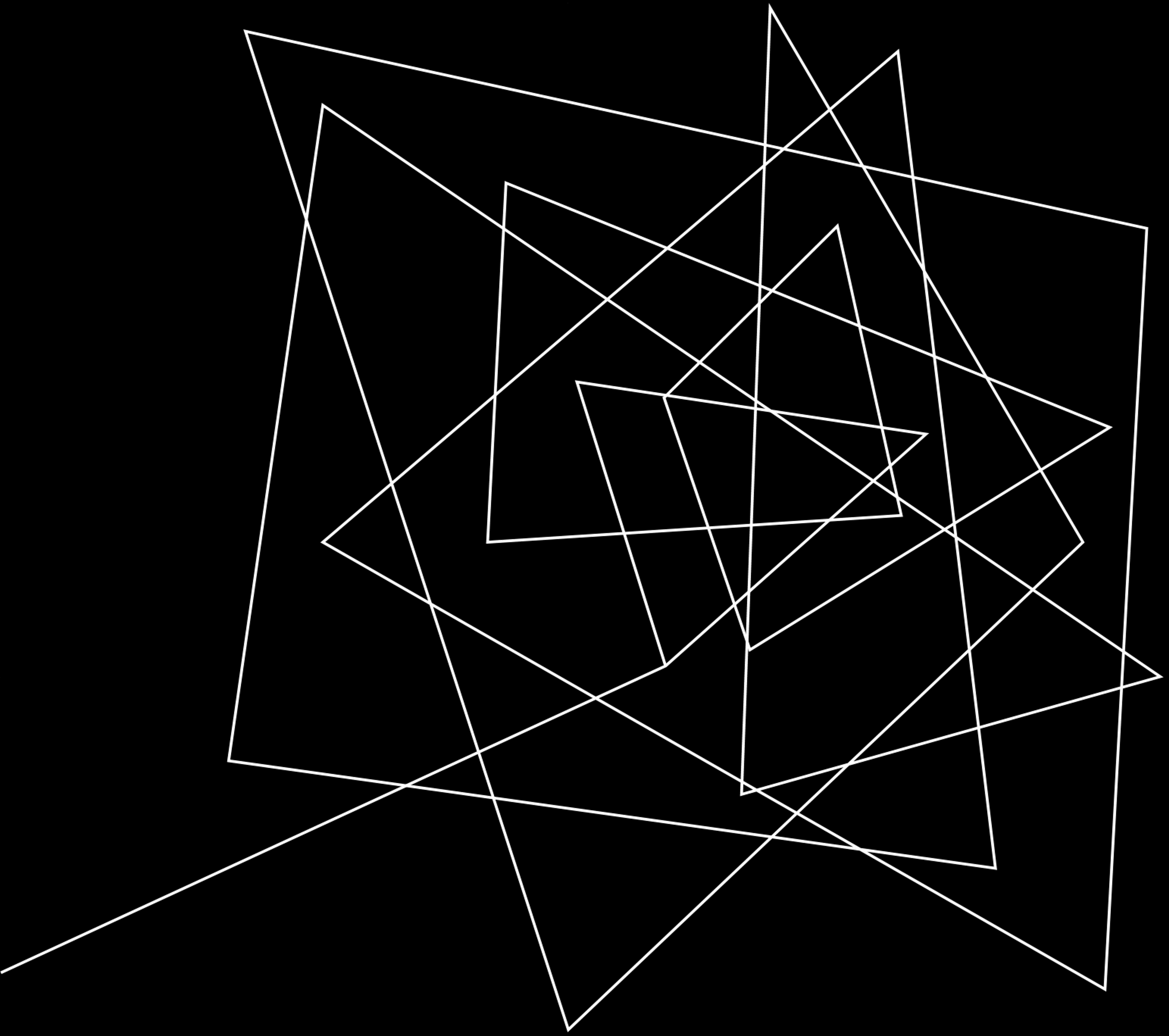
- Task 1 (**Team**): Conduct a thorough review of literature and background information on quantum key reconciliation techniques.
- Task 2 (**Vítor Santos & Tiago Pereira**): Analyze the architecture of the systems done by IT.

Module: Documentation (**Team**)

- Task 1 (**Team**): Collaboratively write technical documentation detailing project specifications, requirements, and implementation guidelines.
- Task 2 (**Diogo Marto & Vítor Santos**): Write benchmark report.
- Task 3 **(David Cobileac**): Create a demo video showcasing the project.
  Task 4 (**Vítor Santos & Diogo Marto**): Write a technical report.

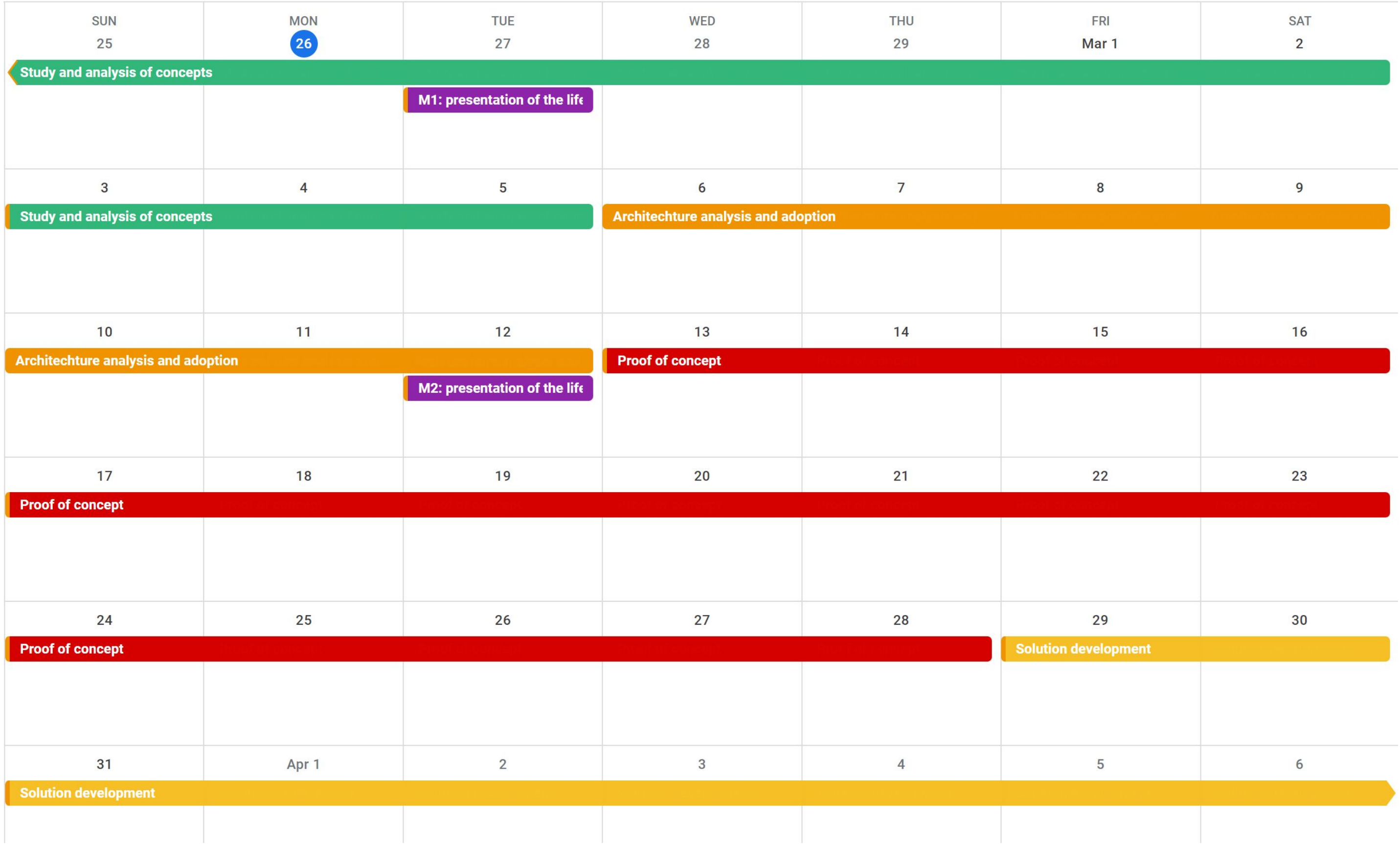
Module: Development

- Task 1 (**TBD**): Retrieve raw key material from the QKD devices.
- Task 2 (**TBD**): Distillate both symmetric and oblivious keys in a coordinated protocol with another peer reconciliation application. Assuring correctness, security and efficiency.
- Task 3 (**TBD**): Provide the generated keys to the KML.
- Task 4 (**TBD**): Verify international and EU standards specified by institutions such as ETSI 1 and ITU-T.
- Task 5 (**TBD**): Benchmark.
- Task 6 (**TBD**): Lab Testing.



PROJECT SCHEDULE

PROJECT SCHEDULE



SUN	MON	TUE	WED	THU	FRI	SAT
25	26	27	28	29	Mar 1	2
Study and analysis of concepts						
		M1: presentation of the life				
3	4	5	6	7	8	9
Study and analysis of concepts			Architechture analysis and adoption			
10	11	12	13	14	15	16
Architechture analysis and adoption			Proof of concept			
		M2: presentation of the life				
17	18	19	20	21	22	23
Proof of concept						
24	25	26	27	28	29	30
Proof of concept					Solution development	
31	Apr 1	2	3	4	5	6
Solution development						

23 Feb - 5 Mar Study and Analysis of concept **6 Mar - 28 Mar** Architecture Analysis and Adoption

13 Apr - 28 Apr Proof Of Concept

29 Mar - 16 Apr Solution Development

17 Apr - 20 Apr Iterate Over Feedback

21 Apr - 26 Apr Further Development and Polish

27 Apr - ? Benchmark date to be determined

MILESTONES

M1 27/02/2023

- Presentation of the lifecycle objectives and calendar for the project.

M2 - 12/03/2024

- Study all essential background
- Analyze the work done previously by IT in the scope of the project.

M3 - 16/04/2024

- Implement all the communication interfaces ensuring robustness and standard specifications.

M4 - 04/06/2024

- Further develop and extend the reconciliation algorithms and protocols.
- Benchmark the solution.
- Test the solution in the lab.

DELIVERABLES

- Proof of concept (Implement the reconciliation application starting from a simple proof-of-concept implementation)
- Final Solution
- Documentation
- Benchmarks
- Technical report
- Project website
- Demo & Poster

REFERENCES

- https://discretion-eu.com/
- https://quantagenomics.av.it.pt/
- https://discretion-eu.com/
- https://www.itu.int/
- https://ptqci.av.it.pt/
- https://www.projectsmart.co.uk/project-planning/project-planning-step-by-step.php

THANK YOU!

Diogo Marto, 108298, diogo.marto@ua.pt

David Cobileac, 102409, cobileacd@ua.pt

Tiago Pereira, 108546, tfgp@ua.pt

Tiago Portugal, 103931, tiago.portugal@ua.pt

Vítor Santos, 107186, vitor.mtsantos@ua.pt