QuantaGENOMICS

Quantum Enabled Secure Multiparty Computation for Genomic Medicine

Deliverable: D5.2.8

Deliverable Title: Newsletter #8

Due date of deliverable: 30-04-2026
Actual submission date: 30-04-2026
Dissemination level: Public
Version: 1.0
Lead beneficiary of D5.2.8: **IT**
Contributing beneficiaries: All

Table of Contents

Introduction

This deliverable corresponds to the eighth newsletter and presents the main activities carried out during the previous semester. The newsletter will be disseminated through different vias, including the QuantaGENOMICS project 'website, and can be found attached to this document.

Conclusion

The deliverable was accomplished.

QuantaGENOMICS

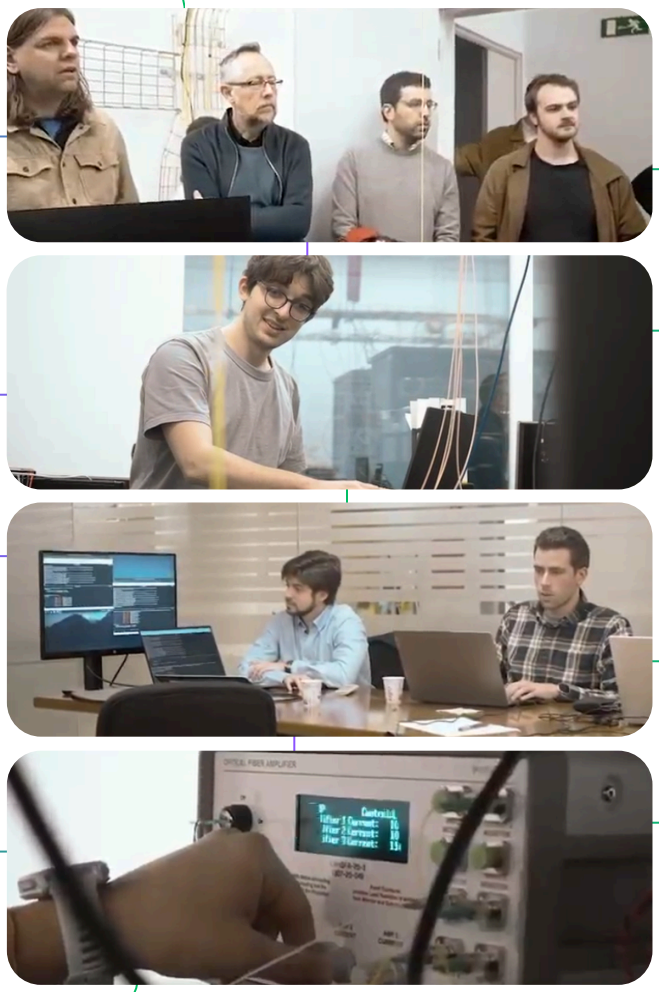
NEWSLETTER - APRIL, 2026

8TH EDITION

THE 7TH QUANTAGENOMICS GENERAL ASSEMBLY

The **seventh QuantaGenomics General Assembly** was held at the Universidad Politécnica de Madrid (UPM) on the 24th of March. The meeting gathered representatives from all partner institutions (IT, SU, ICFO, INRIA, Ophiomics, and UPM) to review the progress of ongoing tasks and activities, to outline the final steps according to the project's work plan, and to plan the last deliverables and potential publications. Participants had the opportunity to demonstrate devices and to present updates on their respective work packages, exchange ideas, and coordinate upcoming actions to ensure smooth progress toward the project's objectives.

DEMONSTRATION



Background:

During March, three quantum communication devices designed to implement the oblivious transfer cryptographic primitive were integrated into the Universidad Politécnica de Madrid (UPM)'s quantum communications infrastructure in Madrid.

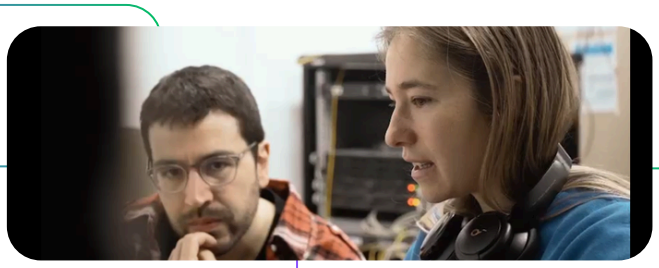
One was developed by the Sorbonne University (SU), another by the Instituto de Ciencias Fotónicas (ICFO) in Barcelona, and the third by the Instituto de Telecomunicações (IT) - Aveiro.

To demonstrate the integration of these technologies, the IT designed three applications of oblivious transfer within the Secure Multiparty Computation (SMC) framework for the field of genomic medicine: anomaly detection, calculation of genomic evolutionary distances, and machine learning inference.

ABOUT THE PROJECT

QuantaGenomics is a QuantERA ERA-NET Cofund in Quantum Technologies project with a focus on the development of a quantum-enabled secure multiparty computation service for collaborative genomic medicine.
https://quantagenomics.av.it.pt/

In this issue:



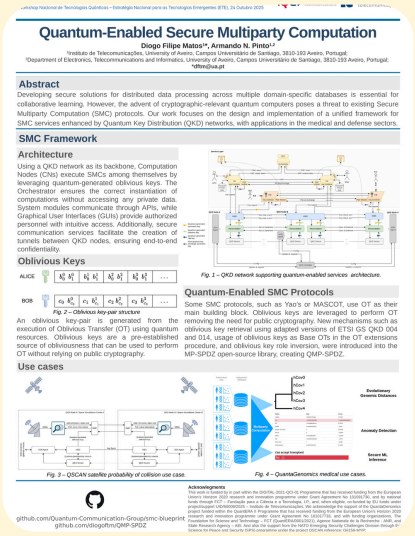
Description:

During the GA, the deployed devices were used to implement the use cases in genomic medicine described above. The devices were used according to their maturity: the device managed by the IT was used with the protocol to generate real-time data; the ICFO device was used with the data generated by the protocol over the previous few days; and for the SU device, the groundwork was laid for an integration that will be reflected in the final deliverable (although this could not be carried out in real time).

In addition, the operation and deployment status of the three experimental devices were explained, and the laboratories housing part of the deployed equipment from the SU and IT were shown.

PARTICIPATION IN THE "NATIONAL WORKSHOP ON QUANTUM TECHNOLOGIES" IN PORTUGAL

Diogo Matos (IT).


Quantum-Enabled Secure Multiparty Computation

Diogo Filipe Matos[1*], Armando N. Pinto[1,2]

[1]Instituto de Telecomunicações, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal.
[2]Department of Electronics, Telecommunications and Informatics, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal.
*difmm@ua.pt

Abstract

Developing secure solutions for distributed data processing across multiple domain-specific databases is essential for collaborative learning. However, the advent of cryptographic-relevant quantum computers poses a threat to existing Secure Multiparty Computation (SMC) protocols. Our work focuses on the design and implementation of a unified framework for SMC services enhanced by Quantum Key Distribution (QKD) networks, with applications in the medical and defense sectors.

SMC Framework

Architecture

Using a QKD network as its backbone, Computation Nodes (CNs) execute SMCs among themselves by leveraging quantum-generated oblivious keys. The Orchestrator ensures the correct instantiation of computations without accessing any private data. System modules communicate through APIs, while Graphical User Interfaces (GUIs) provide authorized personnel with intuitive access. Additionally, secure communication services facilitate the creation of tunnels between QKD nodes, ensuring end-to-end confidentiality.

Fig. 1 – QKD network supporting quantum-enabled services architecture.

Oblivious Keys

Fig. 2 – Oblivious key-pair structure

An oblivious key-pair is generated from the execution of Oblivious Transfer (OT) using quantum resources. Oblivious keys are a pre-established source of obliviousness that can be used to perform OT without relying on public cryptography.

Quantum-Enabled SMC Protocols

Some SMC protocols, such as Yao's or MASCOT, use OT as their main building block. Oblivious keys are leveraged to perform OT removing the need for public cryptography. New mechanisms such as oblivious key retrieval using adapted versions of ETSI GS QKD 004 and 014, usage of oblivious keys as Base OTs in the OT extensions procedure, and oblivious key role inversion, were introduced into the MP-SPDZ open-source library, creating QMP-SPDZ.

Use cases

Fig. 3 – QSCAN satellite probability of collision use case.

Fig. 4 – QuantaGenomics medical use cases.

github.com/Quantum-Communication-Group/smc-blueprint
github.com/diogofmr/QMP-SPDZ

Acknowledgments

Quantum-Enable Secure Multiparty Computation poster.

On October 24, 2025, Diogo Matos, a researcher at Instituto de Telecomunicações, presented the poster "Quantum-Enabled Secure Multiparty Computation" at the National Workshop on **Quantum Technologies – National Strategy for Emerging Technologie**s, held in Coimbra.

The initiative was jointly organized by the Quantum@UC Group at the Universidade de Coimbra and the Quantum Communications Group (Instituto de Telecomunicações – Aveiro).

"BEST STUDENT PAPER AWARD"
SPIE SENSORS+IMAGE: QUANTUM TECHNOLOGIES FOR DEFENCE AND SECURITY II

Best Student Paper Award/
Íris Guilherme (IT) at SPIE Sensors + Imaging 2025.

Íris Guilherme, MSc student, received a prestigious award at the SPIE **Sensors + Imaging 2025 Conference**, held on 15-18 September 2025 in Madrid, Spain.

She was honored with the "Best Student Paper Award" for the paper entitled "Polarization Multiplexing **CV-QKD** with Polarization Drift Post-Compensation".

The SPIE Sensors + Imaging 2025 conference showcases the latest advances in sensor and photonic technologies for imaging and environmental monitoring, as well as innovations addressing homeland security, defence, and counterterrorism challenges.

The paper is available here.

OUTPUTS

Publication:

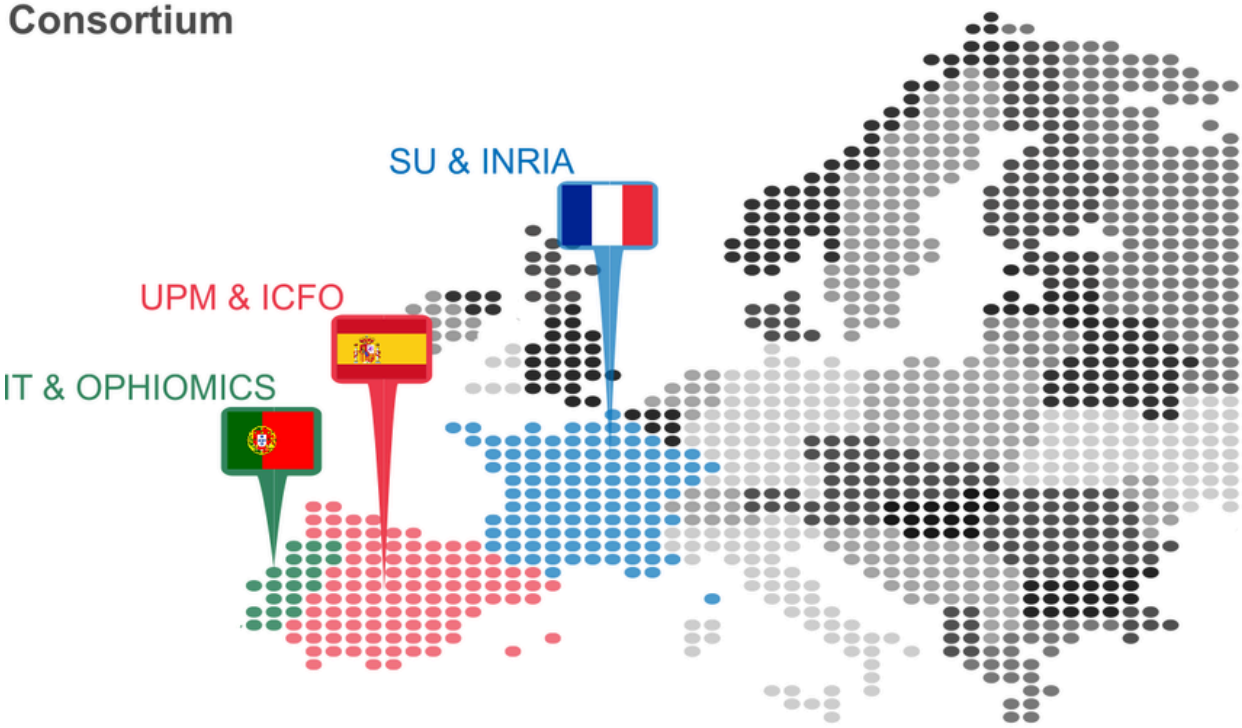
- Almeida, M., Pinto, A. N., & Silva, N. A. (2025). Robustness of continuous variable quantum key distribution under strong polarization drift. *EPJ Quantum Technology*, *12*, 118. https://doi.org/10.1140/epjqt/s40507-025-00417-3

Conference Proceedings:

- Guilherme, Í. G., Almeida, M., Pinto, A. N., & Silva, N. A. (2025). Polarization multiplexing CV-QKD with polarization drift post-compensation. In Proceedings of SPIE Security + Defence (Vol. 13676, Article 1367608). SPIE. https://doi.org/10.1117/12.3069806
- Matos, D. F., Romero, J. J., Ortiz, L., Martín, V., & Pinto, A. N. (2025). Quantum-enabled secure computation medical service. In Proceedings of the 2nd Workshop on Quantum Networks and Distributed Quantum Computing (QuNet '25) (pp. 42–48). Association for Computing Machinery. https://doi.org/10.1145/3749096.3750036

QuantaGENOMICS

Consortium



QuantaGenomics project was funded within the QuantERA II Programme that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101017733, and with funding organisations, The Foundation for Science and Technology – FCT (QuantERA/0001/2021), Agence Nationale de la Recherche – ANR, and State Research Agency – AEI.