QuantaGENOMICS

NEWSLETTER - MAY, 2023

QUANTAGENOMICS GENERAL ASSEMBLY IN AVEIRO, PORTUGAL

Organised by the project coordinator, Instituto de Telecomunicações, the first in-person QuantaGenomics General Assembly was held on **22nd December 2022** and took place in Aveiro, at IT - Aveiro University, and was attended by the majority of the partners (IT, SU, CBR, ICFO, and UPM). The event aimed to join teammates and partners to **discuss the running tasks** and activities, in addition to defining the following steps according to the work plan for each stage.

Prof. Armando Pinto and Nelson Muga chaired the session that had several presentations, distributed over the different work packages: Nelson Muga, IT - WP1; Verena Yacoub, SU - WP2; Paula Alonso, ICFO, and Sara Mantey, IT - WP3; Laura Ortiz, UPM - WP4; Mário Grãos, CBR - WP5. During the session, it was possible to bring the results of the work is being done since the beginning of the project. The representatives had the opportunity to **share with their colleagues the work status, discuss new ideas, and plan further steps.**

The next in-person General Meeting will consolidate the first year of the project and will take place in **Paris, in May 2023.**

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.

In this issue:

PARTICIPATION IN THE "QUANTUM TECH DAY" IN AVEIRO, PORTUGAL

On the 13th of March, took place the **Quantum Tech Day** workshop, to discuss the present and future of quantum technologies. It was organized by the Quantum Communications Group. This event was integrated with the celebrations of the 50th anniversary of the Department of Electronics, Telecommunications, and Informatics (DETI). This workshop was attended by Paulo Jorge Ferreira, the Rector of the University of Aveiro, Mário Campolargo, the Secretary of State for Digitalisation and Administrative Modernisation, Government of Portugal, and Rear-Admiral António Gameiro Marques, the Director General of the Portuguese National Security Authority, which includes the National Cybersecurity Center.

PARTICIPATION IN "QKD DAYS" IN MADRID, SPAIN

Sponsored by the QuantaGENOMICS' partner Universidad Politécnica de Madrid, in collaboration with the Austrian Institute of Technology, and Telefónica, the event "QKD days in Madrid", hosting the latest meeting of the **OPENQKD project**, brought together leading QKD experts, as well as European equipment suppliers and policymakers on 14 and 15 December 2022.

The event was an opportunity to join contributions from companies, universities, and researchers from 38 members of a European consortium of the Quantum Flagship to pave the way towards a pan-European infrastructure for secure quantum communication.

SECURE MULTIPARTY COMPUTATION FOR HEALTH SERVICES

QUANTAGENOMICS PROJECT ROLL-UP

This roll-up was developed as a support material to present the QuantaGenomics project in presentations, events, and congresses. The main goal is to demonstrate the purpose of the project and the results obtained by the researches.

Quantum Enabled Secure Multiparty Computation for Genomic Medicine

instituto de telecomunicações

IQC

universidade de aveiro

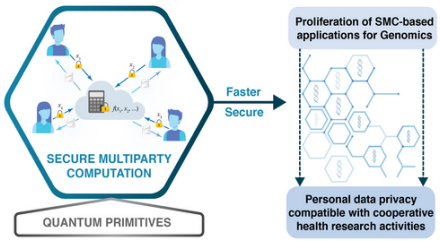
Quantum Communications Group

Instituto de Telecomunicações - Aveiro

Secure Multiparty Computation for Health Services

Quantum Enabled Secure Multiparty Computation for Genomic

Collaborative genomic medicine is on the verge to bring major advances to medical research and health care services

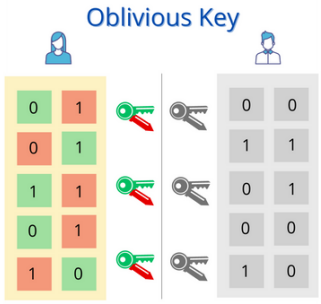


A generic and broadly available secure multiparty computation (SMC) framework, targeting genomic medicine applications, is explored by the laws of quantum mechanics. The developed quantum SMC framework provides unprecedented levels of security, without compromising the efficiency and availability of the system.
As a proof of concept, private data mining genomic medicine service, based on quantum SMC, is implemented in the laboratory and validated in a field trial.
In our approach, the classical oblivious transfer (OT) implementation is replaced by a quantum-enabled OT in a secure multiparty computation (SMC) protocol, leading to a solution that is both fast and secure, even against quantum computer attacks.

QuantaGENOMICS

The QuantaGENOMICS project will demonstrate the proof that quantum technologies can play a major role in solving the conflict between privacy and utility of collecting and mining huge quantities of individuals' data

To construct this quantum SMC framework, a practical secure random oblivious transfer protocol based on classical and quantum cryptographic primitives is being developed, implemented, and validated.
The obtained random oblivious transfer protocol will be practically secure, even in the presence of a quantum computer. Several quantum resources, namely single-photon, coherent and entangled quantum states, are going to be used together with classical cryptographic resources to ensure that the system offers the desired level of security.
Based on this hybrid random oblivious transfer protocol, a generic, fast, and secure SMC framework will be achieved. On top of the quantum SMC framework, a collaborative genomic medicine service is going to be implemented.



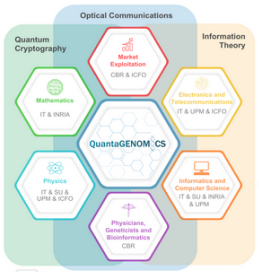
Quantum Enabled Secure Multiparty Computation for Genomic Medicine

Project Coordinator
Instituto de Telecomunicações
Universidade de Aveiro
Quantum Communications Group
Armando Nolasco Pinto – anp@av.it.pt

Project Duration
May 2022 – April 2025

Website
https://quantagenomics.av.it.pt/

Project funded within the QuantERA II Programme (EU 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.



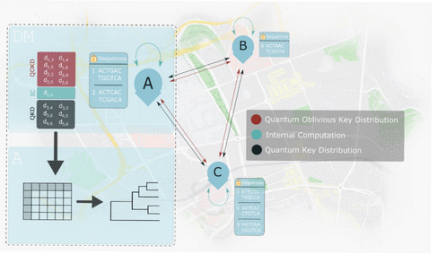
QuGenome

Quantum Enabled Private Recognition of Composite Signals in Genome

QuGenome was a research project focused on secure multiparty computation service supported by quantum technologies to provide a secure and fast multiparty private analyses of genome databases to construct Phylogenetic Trees. This project focused on the implementation of a private recognition of composite signals in a genome use case.
The proposed secure multiparty computation service performed genome database analysis with unprecedented levels of security, which represented a truly innovative approach in the field of healthcare research.
The experiment involved three machines with the same VPN, placed in different locations: IT-Aveiro, the Polytechnic University of Madrid and CBR Genomics.

The experiment demonstrated the computation of a phylogenetic tree using DNA sequences from three different entities. The machines extracted random and symmetric keys and then switched to use the raw keys to compute oblivious keys. In this way, all machines could transfer data and make unconscious transfers safely. The demonstration resulted in the generation of a phylogenetic tree.

Partners



Secure Multiparty Computation solution for private recognition of composite signals in genomes to construct phylogenetic trees

Project Coordinator
Instituto de Telecomunicações
Universidade de Aveiro
Quantum Communications Group
Armando Nolasco Pinto
anp@av.it.pt

Project Duration
Dec 2020 – Jan 2022

Website
https://qugenome.av.it.pt/

Funding Agencies

This work is funded by AIT Austrian Institute of Technology GmbH and 37 further beneficiaries of OpenQKD (project number: 857156, action QuGenome).

Scientific Outputs

- Manuel B. Santos, Ana C. Gomes, Armando N. Pinto, and Paulo Mateus, "Private Computation of Phylogenetic Trees based on Quantum Technologies", IEEE Access, vol. 10, pp. 38065 - 38088, (2021).
- Manuel B. Santos, Paulo Mateus and Armando N. Pinto, "Quantum Oblivious Transfer: a Short Review", Entropy (2022), 24, 945. DOI: 10.3390/e24070945
- Armando N. Pinto, and Vicente Martin, "QKD combined with secure multiparty computation", ITU-T FG QIT4N D2.2: Quantum information technology for networks use cases: QKDN, Use case ID: UC-1-2 (2021).
- Daniel Pereira, Margarida Almeida, Margarida Facão, Armando N. Pinto, and Nuno A. Silva, "Probabilistic shaped 128-APSK CV-QKD transmission system over optical fibres", Optics Letters, vol. 47, pp. 4938 (2022). DOI: 10.1364/OL.456333.
- Daniel Pereira, Armando N. Pinto, and Nuno A. Silva, "Polarization Diverse True Heterodyne Receiver Architecture for Continuous Variable Quantum Key Distribution", IEEE Journal of Lightwave Technology Vol. 41 , pp. 432 - 439 (2023). DOI: 10.1109/JLT.2022.3216754.
- Daniel Pereira, Margarida Almeida, Margarida Facão, Armando N. Pinto, and Nuno A. Silva, "Probabilistic shaped 128-APSK CV-QKD transmission system over optical fibres", Optics Letters, vol. 47, pp. 4938 (2022). DOI: 10.1364/OL.456333.
- Mauricio J. Ferreira, Nuno A. Silva, and Nelson J. Muga, "Quantum-Noise Based True Random Number Generation", Iberic Meeting of Optics Students (IMOS), 20-22 June 2022, Aveiro, Portugal.
- Margarida Almeida, Armando N. Pinto, and Nuno Silva, "CV-QKD Imperfections Impact on Shot-Noise Measurement", Iberic Meeting of Optics Students (IMOS), 20-22 June 2022, Aveiro, Portugal.

CURRENT SCIENTIFIC ACTIVITIES

To the current date, two non-technical and two technical work packages (WPs) have been executed by the consortium: WP1 - Project Management, WP5 - Dissemination and Exploitation, WP2 - Quantum Foundation for SMC, and WP3 - Laboratory Validation. The WP7, Laboratory Validation, started in month 7 of the project.

WP1 is providing the proper administrative and scientific management of the project, e.g. day-to-day operational administrative and contractual tasks of the project and establishing the interface and interaction with the QuantERA office.

WP5 has ensured the dissemination of the project, including the presentation of the project activities, objectives, and results in scientific events and national and international conferences, as well as journal publications.

WP2 has started through the activities of Task 2.1, whose main goal is to identify a set of quantum resources and cryptographic primitives to support fast and practical secure multiparty computation (SMC). This Task is led by SU and has the participation of three more partners, IT, INRIA and ICFO.

WP3 is the most recent initiated workspace, and it is related with the laboratory validation of protocols. . There were three main tasks to be implemented: protocols based on DVs, CVs and quantum entanglement. This task is led by ICFO and has the participation of more two partners, IT and SU.

PUBLICATIONS

"Quantum Oblivious Transfer: A Short Review"

The Quantum Communication Group, from the IT partners, has published a review paper on Quantum Oblivious Transfer.
Manuel Santos, Paulo Mateus, and Armando N. Pinto, "Quantum Oblivious Transfer: A Short Review",
Entropy Vol. 24, pp. 1-35 , 2022.

Other publications:

- B. Mera, P. Mateus, A. M. Carvalho, Model complexity in statistical manifolds: the role of curvature, IEEE Transactions on Information Theory, Vol. 68, No. 9, pp. 5619 - 5636, September, 2022.
- Daniel Pereira, Armando N. Pinto, and Nuno A. Silva, Polarization Diverse True Heterodyne Receiver Architecture for Continuous Variable Quantum Key Distribution, Journal of Lightwave Technology, Vol. 41, No. 2, pp. 432 - 439, October, 2022.

Conferences:

- S. T. Mantey, M. F. Ramos, N. A. Silva, A. N. Pinto, N. J. Muga, Frame Synchronization for Quantum Key Distribution Systems, IEEE Global Communications Conference - GLOBECOM, Rio de Janeiro, Brazil, December, 2022.
- Daniel Pereira, Margarida Almeida, Armando Pinto, and Nuno A. Silva "Optimization of continuous variables quantum key distribution using discrete modulation", SPIE Security + Defense, Berlin, Germany, September, 2022.

QuantaGENOMICS

quantum communications

instituto de telecomunicações

cbrgenomics
genetically informed medicine

SORBONNE UNIVERSITÉ

Inria

POLITÉCNICA

UNIVERSIDAD POLITÉCNICA DE MADRID

ICFO

European Commission

QUANTERA

FCT
Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

anr
agence nationale de la recherche

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

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.