Quantum Secure Multiparty Computation to Support Genomic Medicine

Armando Nolasco Pinto[1,2], N. J. Muga[1], N. A. Silva[1], M. B. Santos[1,3], P. Mateus[1,3], Ana C. Gomes[4], M. Grãos[4], J. P. Brito[5], L. Ortiz[5], and V. Martin[5]

[1]*Instituto de Telecomunicações, Portugal*
[2]*Department of Telecommunications, Electronics, and Informatics, University of Aveiro, Aveiro, Portugal*
[3]*Instituto Superior Técnico, Universidade de Lisboa, Portugal*
[4]*CBR Genomics, Cantanhede, Portugal.*
[5]*Universidade Politecnica de Madrid, Madrid, Spain*
anp@ua.pt

Data mining and analysis over large Genomic databases promise major advances in medicine. Protecting the privacy of the data owners demands the use of adequate and sophisticated cryptographic primitives and protocols [1]. Nevertheless, to make the genomic data useful we must ensure large-scale interaction between data owners that do not trust each other. This trade-off between data privacy and data mining can be reached by implementing secure multiparty computation (SMC) functionalities [1]. The cryptographic primitive oblivious transfer (OT) plays a central role since it allows for the implementation of any SMC functionality [2]. However, classical implementations of OT are computationally very demanding, requiring a strong relaxation in the security. To overcome these constraints, we design, test, and implement in a real quantum network, a SMC service capable of compute a public phylogenetic tree from private genomic database. To implement that functionality, we develop a quantum oblivious key distribution (QOKD) protocol from which we generate OTs [2].

In this work we present recent results of the implementation of a SMC service involving three private genome databases. We test our SMC in the Madrid quantum network, see Figure 1. The three nodes ran a quantum-enabled SMC procedure to jointly compute the matrix distance of the genome sequences. This without revealing their private genome sequences. Each node pair consumed oblivious keys, generated through the implementation of a QOKD protocol, as well quantum key distribution protocol. The final output, shared by the three nodes, was the phylogenetic tree corresponding to the genome sequences belonging to the three private genome databases.

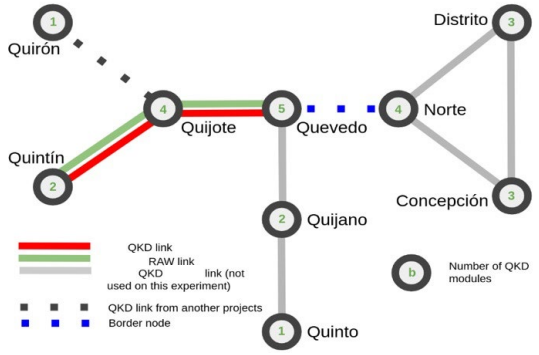

Figure 1: Madrid quantum network.

References

[1] 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)

[2] M. Lemus, M. F. Ramos, P. Yadav, N. A. Silva, N. J. Muga, A. Souto, N. Paunković, P. Mateus and A. N. Pinto, "Generation and distribution of quantum oblivious keys for secure multiparty computation", Applied Sciences, vol. 10, pp. 4080, (2020)

Acknowledgements

This work was supported by OpenQKD (project number: 857156, action QuGenome), and by the QuantERA II Programme funded by the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101017733, and with funding from The Foundation for Science and Technology – FCT (QuantERA/0001/2021), Agence Nationale de la Recherche - ANR, and State Research Agency – AEI. We also acknowledge MCIN with funding from European Union NextGenerationEU (PRTR-C17.I1) and funding from the Comunidad de Madrid. Programa de Acciones Complementarias. Madrid Quantum.