Quantum Enabled Private Recognition of Composite Signals in Genome

Nuno A Silva[1], Nelson J Muga[1], Manuel Santos[2], Paulo Mateus[2] and Armando N Pinto[1, 3]

Genomic data must be handled and examined with extremely secure privacy-preserving procedures to comply with people's rights to privacy and legal requirements. In this use case, we implemented a quantum-enabled secure multiparty computation (SMC) service involving three private genome databases placed at three distinct nodes in the Madrid Quantum Network. The three nodes ran a quantum-enabled SMC procedure to jointly compute the matrix distance of the genome sequences present in the private databases. The final objective was to compute a phylogenetic tree without revealing private genome sequences. Each node pair consumed oblivious keys generated through the implemented QODK protocol, which was supported by a Continuous-Variable Quantum Raw Key Distribution (CV-QRKD) link and symmetric keys generated by the QKD systems. The final output, shared by the three nodes, was the phylogenetic tree corresponding to the genome sequences belonging to the three private genome databases. The consortium was comprised of Instituto de Telecomunicações (PT), who coordinated the project and contributed with two research groups (Optical Quantum Communications and Security and Quantum Information), CBR Genomics, a genomics as a service SME that brings genetic information to the physician's practice, and Huawei Technologies Duesseldorf GmbH, a leading global information and communications technology solutions provider. The project benefited from the support of the OpenQKD partners IDQuantique, UPM, RedIMadrid.

Acknowledgements

This work was supported in part 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 organisations, FCT (QuantERA/0001/2021), ANR, and AEI, and by AIT Austrian Institute of Technology GmbH and 37 further beneficiaries of OpenQKD (project number: 857156, action QuGenome).

Figure 1 and 2

The QuGenome project (http://qugenome.av.it.pt/) implemented a secure multiparty computation (SMC) of phylogenetic trees involving three private genome databases placed at three distinct nodes in the Madrid quantum network (see Figure 1): Quintin – Node A, Quijote – Node B, Quevedo (CSIC node on RM Network) – Node C. This SMC service enables distributed parties in a network to jointly compute arbitrary genome analysis without revealing their private genome sequences. The three nodes run a quantum-enabled SMC procedure to jointly compute the SARS-CoV-2 genome sequences' matrix distance over the private databases. After the computation of the matrix distance entries corresponding to the sequences from the same database, the three nodes shared the missing matrix distance entries via encrypted messages, whose cryptography keys were generated by the QKD systems. Once the full matrix distance was reached, the three nodes iteratively grouped the genes with the fewest differences between them. The final output, shared by the three nodes, was the phylogenetic tree (see Figure 2) corresponding to the genome sequences belonging to the three private genome databases.

1 – Institute of Telecommunications & University of Aveiro.
2 – Institute of Telecommunications & Instituto Superior Técnico.
3 – Department of Electronics, Telecommunications and Informatics & IT, University of Aveiro.

FIGURE 1
Madrid quantum network left) links used; right) three computation diagrams.

FIGURE 2
Computed phylogenetic tree.