

PROJECT / Quantum Primitives for Privacy Preserving Data Mining

QuantumMining



Main Objective:

QuantumMining project is going to pave the way on the development of a radically new generation of cryptographic technologies, based on the realization of both highspeed and secure quantum oblivious transfer (QOT) cryptographic primitive. QOT is a basic cryptographic primitive which can be used to construct any secure multiparty computation protocol, including privacy preserving data mining. We are going to design and implement a QOT protocol over optical fibers, and we are going to integrate this quantum primitive with a privacy preserving Genome data mining service. Privacy preserving data mining cryptographic tools associated to genome databases can enable a revolution in health care services, enabling personalized medicine, and helping on the discovery of novel genome-phenome associations. However, this major breakthrough has had limited impact due to the inefficiency of the privacy algorithms used for data mining in very large Genome data sets.

Reference: POCI-01-0145-FEDER-031826, Funding: FCT, Start Date: 01-09-2018

Team: [Armando Humberto Moreira Nolasco Pinto](#), [Rogério Nunes Nogueira](#), [Paulo Alexandre Carreira Mateus](#), [Nuno Alexandre Peixoto Silva](#), [Nelson de Jesus Cordeiro Muga](#), [André Nuno Carvalho Souto](#), [Nikola Paunkovic](#), [Celestino Sanches Martins](#), Margarida Facão, [Somayeh Ziaie](#), Preeti Yadav



Groups: [Optical Quantum Communications and Technologies – Av, Security and Quantum Information - Lx](#)

Partners: CBRA GENOMICS, S.A.

Local Coordinator: [Armando Humberto Moreira Nolasco Pinto](#)