

**PROJECT / SI I&DT Copromoção Nr.
039728 - Distributed Quantum
Oblivious Transfer**

Q.DOT

Cofinanciado por:



UNIÃO EUROPEIA
Fundo Europeu
de Desenvolvimento Regional

Main Objective:

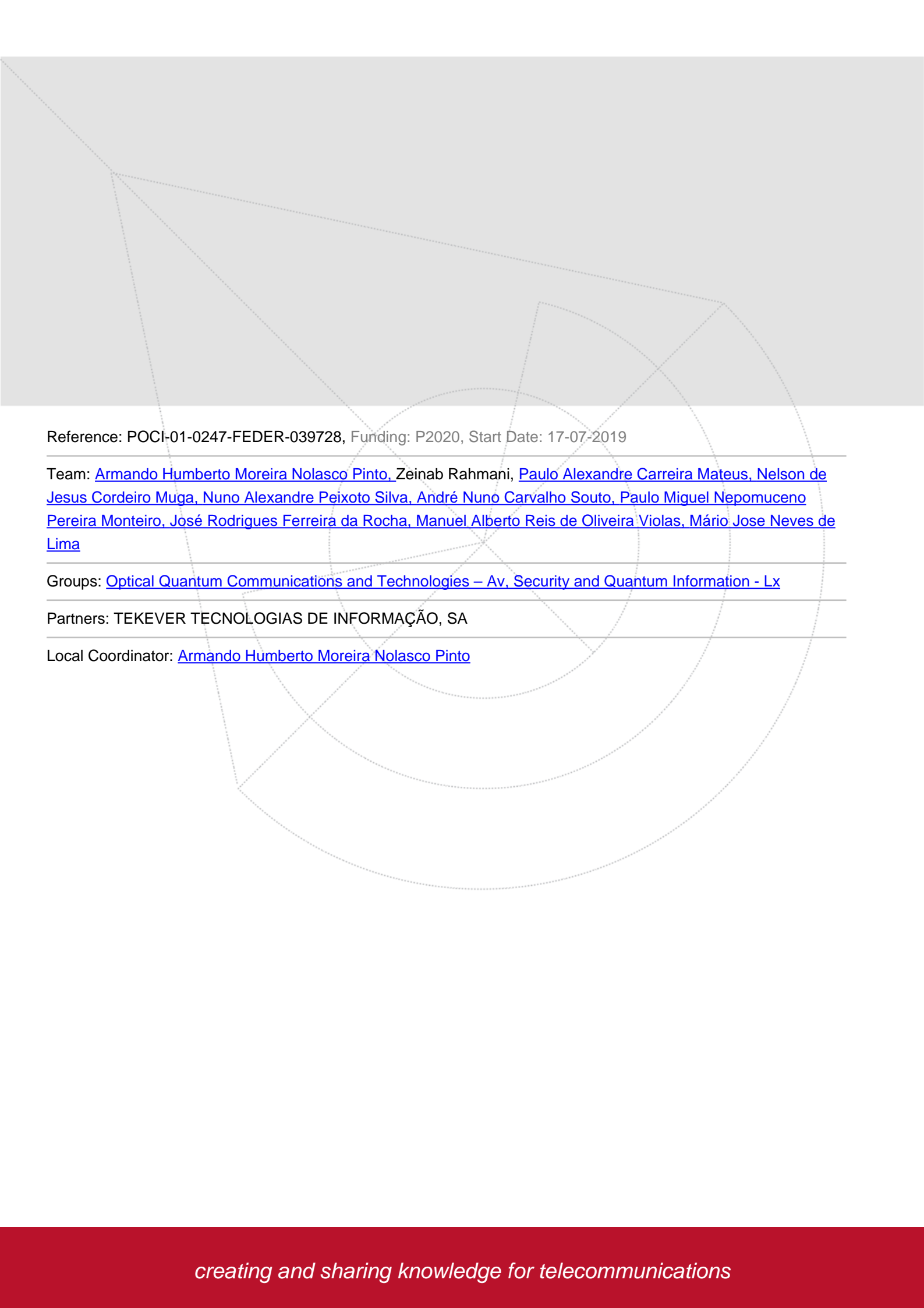
Reinforce research, technological development and innovation

Synthesis: The need to protect the privacy of sensitive data collected by third parties has driven several measures in order to prevent the information from being analyzed and/or shared between different entities. Therefore, even though actions like the General Data Protection Regulation bear evident advantages, the added-value that arises from the study and cooperative processing of this information is lost. In order to extract the benefit that is inherent to this cooperative processing, it is necessary to come up with a solution that allows the analysis of the information without compromising the privacy of whom this issue affects. This can be achieved through Secure Multiparty Computation (SMC), which is based on operating data transfers through the use of a fundamental primitive called Oblivious Transfer (OT).

Still, in order to make SMC a viable common practice, it is necessary that it has the capacity to process millions of OTs per second and thus, the efficient and secure development of each OT becomes imperative – two characteristics that aren't compatible with current classic cryptographic protocols. To address this problem, the Q.DOT project capitalizes from previously established synergies between TEKEVER and IT Aveiro in order to present a practical and scalable solution based on the integration of quantum technology for the production of OT for the statistical analysis of private databases - Privacy Preserving Data Mining (PPDM).

Eligible Costs: 609 544,21 € (Total) / 285 567,71 € (IT)

Funding (FEDER - COMPETE 2020): 391 941,95 € (Total) / 214 175,79 € (IT)



Reference: POCI-01-0247-FEDER-039728, Funding: P2020, Start Date: 17-07-2019

Team: [Armando Humberto Moreira Nolasco Pinto](#), Zeinab Rahmani, [Paulo Alexandre Carreira Mateus](#), [Nelson de Jesus Cordeiro Muga](#), [Nuno Alexandre Peixoto Silva](#), [André Nuno Carvalho Souto](#), [Paulo Miguel Nepomuceno Pereira Monteiro](#), [José Rodrigues Ferreira da Rocha](#), [Manuel Alberto Reis de Oliveira Violas](#), [Mário Jose Neves de Lima](#)

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

Partners: TEKEVER TECNOLOGIAS DE INFORMAÇÃO, SA

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