

Launch of the Quantum Secure Networks Partnership (QSNP)

The new European Quantum Flagship project in quantum communications will aim to develop and deploy quantum cryptography technology that will permit the ultra-secure transmission of information through the network.

March 15, 2023

Digital communications have been key players in all connectivity advances society has experienced in these last decades. The increasingly astonishing number of devices and systems connected to the global networks and the information that is being transmitted amongst them is an indication that we are indeed in need to protect the information that can be considered sensitive.

We are aware that most networks are public and may be easy targets to attacks by hackers. Therefore, one of the major concerns for all users nowadays is security. There is an imperative need to secure our information as much as possible so no one can have access to it. But many current existing cryptography techniques that are used to secure our information are in fact based on methods that are becoming vulnerable to the constant

increase of computer processing capabilities.
March 1st, 2023, has been the official launch of the Quantum Secure Networks Partnership, or QSNP, a new project in the area of quantum communications of the Quantum Flagship. Coordinated by ICREA Prof. at ICFO, Valerio Pruneri, QSNP brings together more than 40 partners from all over Europe, ranging from academia, foundries and RTOs, SMEs and spin-offs, to network and cryptography integrators and telecom operators. In the time span of 3.5 years and with a budget of 25M?, these experts in the field of quantum technologies will seek to fulfil three main goals.
Firstly, they will develop advanced quantum technology for quantum secure communication networks against the ever-increasing power of computers and the sophistication of algorithms, even for quantum computers. That is, they will work on the development and deployment of next generation protocols based on Quantum Key Distribution (QKD) cryptography techniques, that can help reduce the security assumptions needed for the networks, extend the range of secure communication, and search for new functionalities that could beyond these techniques.
Secondly, they will aim to integrate this innovative quantum cryptography technology not only at the component, system and network levels, but also into existing classical telecommunication systems and post-quantum protocols, assuring an additional layer of ultra-secure communications in this hybrid classical-quantum network.
Finally, they will apply all the know-how and capabilities acquired, as well as the technology developed, into different use cases, mainly into delivering critical European technology for government infrastructures such as the European Quantum Communications Infrastructure (EuroQCI). In doing so, they are interested in identifying the potential users, be it authentication, long-term secure storage, critical infrastructure protection, clock synchronization or primitives beyond QKD, in order to provide robust and solutions to their needs. In addition, the project will be a launchpad for future applications, to exploit new capabilities, evaluate new cost/effective features, measure use/integration easiness levels, and explore new sectors where quantum technologies could take over markets that are not being reached by the current technology.
As Valerio Pruneri mentions, i¿½**We are thrilled to commence this innovative program. With QSNP, we are now moving out into the terrain where we will be able to develop further and most of all test the research development carried out in the first phase of the flagship. With the +40 entities within this gran consortium, we expect to achieve unprecedented performances and new designs for application-specific cryptography, covering the full chain from quantum fundamental to product development.**i¿
? As the official launch of the project has occurred, the first in person meeting with all t
e consortium partners will be held at ICFO premises in Barcelona, from 24-25 April, 202

List of the Consortium Partners

Participant

Institution

Country

Academic Partners

1

ICFO-The Institute of Photonic Sciences (Coordinator)

Spain

2

Centre National de la Recherche Scientifique

France

3

Institut Polytechnique de Paris

France

4

Technical University of Denmark

Denmark

5

Universidad Politecnica de Madrid

Spain

6

Friedrich-Alexander University Erlangen-Nuremberg

Germany

7

QuTech, at the Technical University Delft

Netherlands

8

Universita di Padova

Italy

9

AIT Austrian Institute of Technology

Austria

10

Palacky University Olomouc

Czech Rep.

11

Instituto Superior Tecnico

Portugal

12

Universidade de Vigo

Spain

13

Katholieke Universiteit Leuven

Belgium

14

Universitat Wien

Austria

15

Universite libre de Bruxelles

Belgium

16

University of Warsaw

Poland

17

University of Malta

Malta

18

Institute of Communications and Computer Systems

Greece

19

Universitat Paderborn

Germany

20

Inria

France

21

National and Kapodistrian University of Athens (NKUA)

Greece

22

Insitituto De Telecomunicacoes

Portugal

23

Politecnico di Bari

Italy

Foundries & RTOS

24

Fraunhofer Heinrich-Hertz-Institut

Germany

25

Commissariat a l'Energie Atomique et aux Energies Alternatives

France

26

Technische Universiteit Eindhoven

Netherland

27

Interuniversity Microelectronics Centre

Belgium

28

University College Cork

Ireland

Spin-offs and SMEs

29

QuSide

Spain

30

LuxQuanta

Spain

31

Micro Photon Devices

Italy

32

ThinkQuantum

Italy

33

VPIphotonics GmbH

Germany

34

Alea Quantum Technologies ApS

Denmark

35

Q*Bird

Nertherlands

Network & Crypto Integrators

36

Cryptonext Security

France

37

Nokia Bell Labs

Franc

38

Nextworks

Italy

Telecom Operators

39

Deutsche Telekom

Germany

40

Telefonica

Spain

41

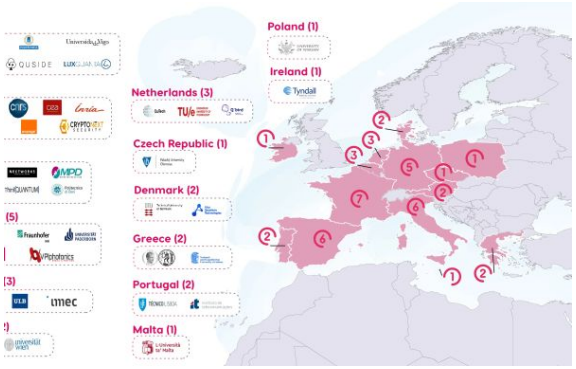
TIM S.p.A

Italy

42

Orange SA

France


Poland (1)
Ireland (1)
Netherlands (3)
Czech Republic (1)
Denmark (2)
Greece (2)
Portugal (2)
Malta (1)
imec