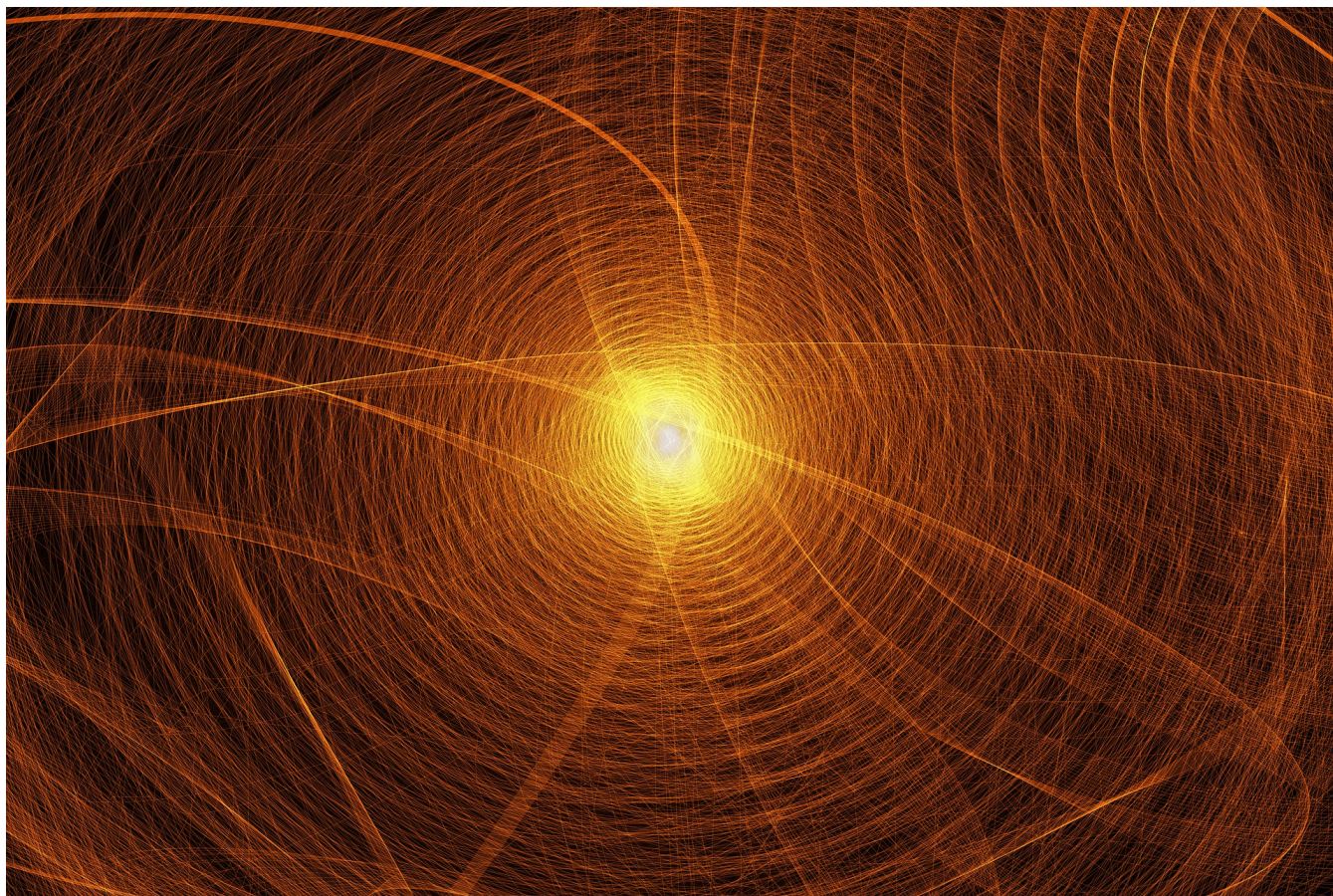


Madrid Quantum Network

Boosting Europe's capabilities in quantum technologies, cybersecurity and industrial competitiveness.



Contact information

Address: CeSViMa i Parque Científico y Tecnológico de la UPM
Campus de Montegancedo
28223, Pozuelo de Alarcón, Madrid
Website: cesvima.upm.es
Email: jose Luis.rosales@upm.es

Technological Offers type

[Technological solutions](#)

Research and innovation areas

- [Digital Technologies, Artificial Intelligence, Cybersecurity, 5G, Robotics](#)

ODS



Where?

Computer Simulation Research Centre Quantum Information and Computing Research Group (GIICC)

Keywords: | [cyber security](#) | [quantum technology](#)

Brief description of the solution and the added value it delivers

Solution to provide quantum key distribution (QKD) as a service.

Description of the technological basis

Quantum communication infrastructure (QCI) will help Europe to protect its critical infrastructure and its encryption systems from cyber threats, protecting smart energy networks, air traffic control, banks, healthcare facilities and more from piracy. It will also enable data centres to store and exchange information securely and will preserve the long-term privacy of government information. The long-term plan is for QCI infrastructure to become the backbone of Europe's quantum internet, connecting quantum computers, simulators and sensors over quantum networks, in order to distribute information and resources securely throughout Europe.

'QKD, a hardware technology whose level of security will not be affected by the calculation capacities of any future quantum computer'

Business needs / application

- The best methods known at present require an amount of computing power that makes them completely unviable.
- Classic cryptography cannot cope with the power of a quantum computer.
- Opportunity cost associated with not using QKD services.

'The QKD market will grow by 19.9% per year over the next five years'

Competitive advantages

- Quantum key distribution infrastructure is fully compatible with existing cryptographic and encryption methods. AES, DES and Triple DES (market standards) through transport layers ETSI 004 and ETSI 014.
 - Coexistence of post-quantum cryptographic algorithms in the services network.
-

References

- OpenQKD Consortium European Flagship (2018-2022) Testbed
- Consortium with AIT, Max Planck Institute, RediMad, Telefónica, Cambridge University, IdQuantique, Toshiba and UniGe
- CiViQ European Flagship (2017-2021)
- Quantum Secure Net (ITALTEL) e-health project (2021-2022)
- OpenCall Up&Running +UPM (2021)

Stage of development

CONCEPT

RESEARCH

LAB PROTOTYPE

**INDUSTRIAL
PROTOTYPE**

PRODUCTION

Contact

Madrid Quantum Network contact

José Luis Rosales, Juan Pedro Brito, Vicente Martín

Centro de Supercomputación y Visualización de Madrid, CeSViMa | UPM

e: joseluis.rosales@upm.es

UPM contact

I&E

Technological Innovation Support Centre (CAIT) - UPM

e: innovacion.tecnologica@upm.es