QUANTUM COMMUNICATION

Technologies at a Glance

June 2025

"TECHNOLOGIES AT A GLANCE" REPORT

ANALYSING KEY TRENDS FOR INFORMED DECISION-MAKING

Funded by the European Union

NATIONAL COMPETENCE CENTRE
SUPERCOMPUTING LUXEMBOURG

EURO

LUXINNOVATION
#MakingInnovationHappen

Agenda

01 Quantum Communication

In a nutshell

What is quantum communication?

Quantum communication is a cutting-edge field that uses the principles of quantum mechanics to securely transmit information. Unlike classical communication, which encodes data using bits (0s and 1s), quantum communication uses **quantum bits (qubits),** whose properties (like superposition and entanglement) allow for **fundamentally secure communication**.

Why now?

The growing interest in quantum communication stems from the **looming threat of quantum computing**. Once sufficiently advanced, quantum computers could break widely used encryption algorithms**, compromising financial systems, government communications, critical infrastructure and private data**.

This has spurred governments and companies worldwide to invest in quantum-safe technologies. Two key paths are emerging: **post-quantum cryptography (PQC)**, new classical algorithms that resist quantum attacks; and **quantum key distribution (QKD),** a physical-layer defence that works even against future quantum computers.

For what?

Quantum communication represents a strategic imperative for **long-term confidentiality, for information protection and sovereign control over critical communications infrastructures**, and for a future quantum internet infrastructure.

02 Quantum Communication

Introduction

Quantum communication is an emerging field that harnesses the unique properties of quantum mechanics, enabling fundamentally secure and efficient methods for exchanging information. Attempts to eavesdrop on quantum communication are revealed by the laws of quantum mechanics: measuring a quantum system disturbs it, which immediately alerts the sender and receiver to any intrusion.

Unlike conventional approaches, it leverages phenomena like superposition and entanglement, allowing the **creation and distribution of encryption keys that are immune to interception or tampering**. Among the most promising applications are **quantum key distribution (QKD)**, which enables fundamentally secure exchange of encryption keys, and **quantum random number generation (QRNG)**, which provides truly unpredictable randomness for cryptography and other uses.

These technologies are at the forefront of efforts to strengthen digital security and lay the foundation for future communication networks. They underpin applications ranging from **secure government and financial communications** to **protecting critical infrastructure**, **ensuring trust in digital services**, and **supporting future innovations in cloud, IoT, and high-performance computing**.

In short, quantum communication promises to transform sectors relying on secure data exchange, such as finance, government, healthcare, and critical infrastructure. By leveraging quantum technologies, society is poised for unprecedented advances in data privacy, resilience against powerful computational attacks, and new possibilities for distributed sensing and timing.

Next you will find a deep dive on quantum communication technologies and a focus on the two most mature technologies: QKD and QRNG.

03 10 key technologies

Quantum communication - Tech radar

ADOPT

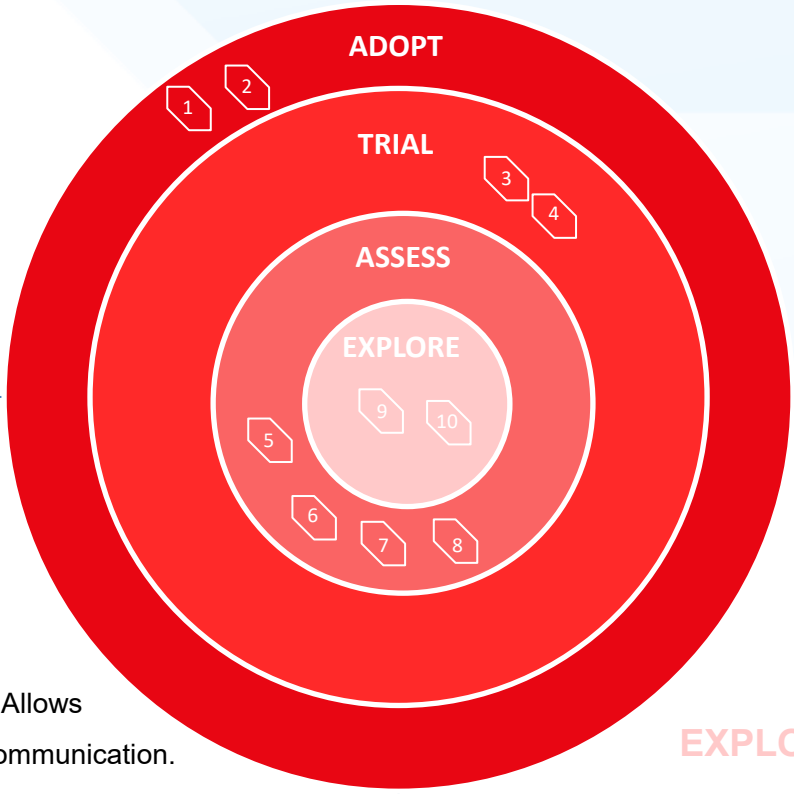
1 **Quantum key distribution** (QKD): Uses quantum states to securely generate and share cryptographic keys, revealing any eavesdropping.

2 **Quantum random number generators** (QRNG): Generates truly random numbers for strong encryption.

TRIAL

3 **Quantum networks**: Link quantum devices using entanglement.

4 **Integrated photonics**: Enable scalable efficient quantum communication.



ASSESS

5 **Quantum teleportation**: Allows long-distance quantum communication.

6 **Quantum repeaters**: Extend quantum communication range by storing and retransmitting quantum information.

7 **Quantum memories and interfaces**: Store and transfer quantum states, enabling synchronisation across a quantum network.

8 **Quantum entanglement distribution**: Process of generating and sending entangled particles to distant locations, ensuring their states remain correlated.

EXPLORE

9 **Quantum clock synchronisation**: Synchronises distant clocks with extremely high precision.

10 **Quantum internet**: a network of interconnected quantum computers that transmits, processes and receives information encoded in quantum states.

Non-exhaustive list of quantum communication technologies

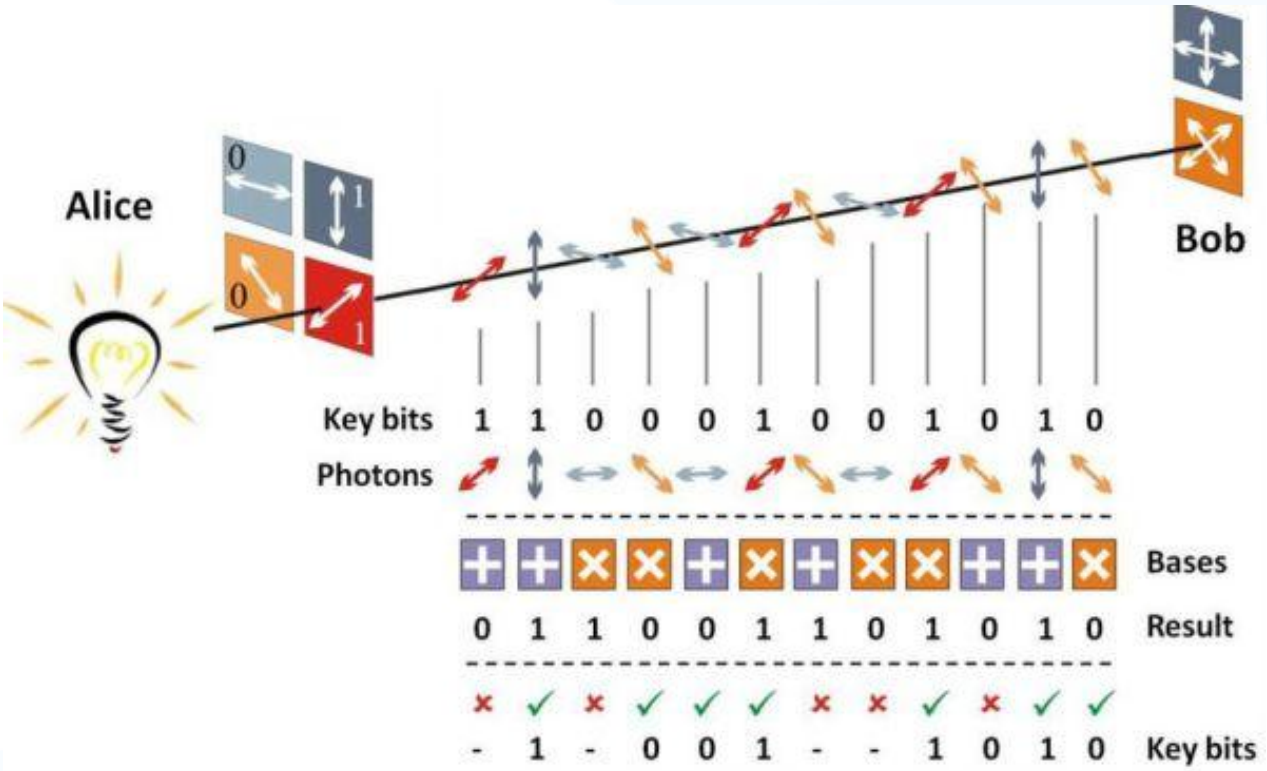
04 Key technologies

Focus on quantum key distribution

What is QKD?

Quantum key distribution (QKD) is the **most mature quantum security technology, and** is already facing real-world deployments in finance, government networks and telecoms**.** It is a cutting-edge technology that uses the principles of quantum mechanics to **securely exchange encryption keys between two parties**.

By transmitting photons (light particles) in specific quantum states, QKD ensures that any attempt to eavesdrop on the key exchange is immediately detectable, guaranteeing a level of security unattainable by classical cryptographic methods.



Quantum key distribution schema
Quantum Flagship

04 Key technologies

Focus on quantum key distribution

What are the concrete applications?

QKD offers a powerful solution for **securing sensitive data across a wide range of sectors**. Its most immediate impact is expected in **finance**, where it can protect high-value transfers, shield transactions from future quantum-enabled attacks, and ensure compliance with increasingly strict regulatory frameworks.

Similarly, in **defence and government**, QKD provides a way to safeguard state communications, diplomatic exchanges, and classified information against interception, making it a strategic tool for national security and sovereignty. The **telecommunications sector** is emerging as a key driver of adoption, not only by integrating QKD to secure bandwidth, datacentres, and infrastructure, but also by positioning itself to commercialise these capabilities. A growing opportunity lies in offering **"quantum-as-a-service"**, where telecom providers could deliver quantum-secure communication solutions to clients across industries, creating a new revenue stream and strengthening customer trust.

Looking further ahead, QKD holds promise for **healthcare**, where it could be used to secure the exchange and storage of sensitive patient data, particularly as health systems expand digital records and cross-border data sharing. In **space applications**, QKD-enabled satellites and drones are being developed to enable truly global secure communications, ensuring resilience even where terrestrial networks are unavailable or vulnerable.

What's happening in Luxembourg?

In Luxembourg, Starion is leading the INT-UQKD project (International Ultra-Secure Quantum Key Distribution), an international collaboration that aims at developing quantum-safe communications using QKD. Members of the consortium include national players Starion Luxembourg, POST, the University of Luxembourg's SnT and HITEC Luxembourg, and international players evolutionQ and SpeQtral.

04 Key technologies

Focus on quantum random number generators

Quantum random number generators (QRNGs) use the inherent **unpredictability of quantum mechanics** to **produce truly random numbers**, which are crucial for secure cryptographic applications and complex simulations. Unlike classical random number generators, QRNGs leverage quantum phenomena ensuring numbers generated are entirely **unpredictable and unbiased**.

What is QRNG?

A quantum random number generator is a device or system that utilizes the properties of quantum physics to generate random numbers.
These random numbers have high entropy and are fundamentally unpredictable, even with complete knowledge of the system's initial state.

What are the concrete applications?

QRGNs have transformative potential across a spectrum of industries, with their most compelling use found in sectors that demand the highest standards of **cybersecurity and data integrity**. In **financial services**, QRNGs are being deployed to secure transactions and protect sensitive client information, addressing both regulatory compliance and the looming threat of quantum-enabled attacks. **Banks and financial institutions require robust encryption systems**, and quantum-generated randomness ensures that encryption keys cannot be predicted or replicated, making attacks virtually impossible.

Telecommunications also stand to benefit greatly from QRNGs, particularly as carriers look to future-proof networks against sophisticated cyberattacks and adapt to post-quantum security requirements. Integrating quantum random number generation at the core of telecom infrastructure enables end-to-end data protection. This same principle extends to **data centers**, where QRNGs shield data-in-transit and preserve the confidentiality of stored backups, without compromising availability or redundancy.

05 Conclusion

A quick glance at projections, opportunities and risks

Quantum communication is moving rapidly from research to deployment, with QKD and QRNG already in early commercial use and more advanced technologies such as quantum networks, repeaters, and memories progressing through trials and assessments. In the coming years, **these technologies are expected to mature into building blocks of a quantum-secure digital infrastructure**, with strong links to the development of **a future quantum internet**.

The **opportunities are substantial**: from safeguarding critical government and financial communications to enabling new business models for telecoms, cloud providers, and data centers. **Industries with the highest stakes in data integrity, such as finance, healthcare, and defence, will be among the first movers**, while broader adoption in IoT, mobility, and consumer services will follow.

At the same time, risks and uncertainties remain. **Market adoption depends on high deployment costs, standardisation, and international interoperability**. Geopolitical competition around quantum infrastructures raises **questions about sovereignty and trust**. Moreover, **the pace of quantum computing progress will strongly influence the urgency and timing of demand for quantum communication solutions**.

Taken together, these dynamics point to a market that is strategic, opportunity-rich, but still maturing. **Explore our Market applications report on our knowledge hub** to discover concrete market applications and illustrations where early commercial traction is already emerging, and where future growth may be most impactful.

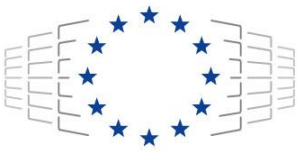
06 Sources

Quantum technologies

- CSIS, “Quantum Technology: Applications and Implications”, May 2023
- Quantum Flagship, “Quantum Technologies in a nutshell”
- IBM, “What is quantum computing?”
- Innovation News Network, “Why quantum computing is advancing rapidly – but adoption remains slow”, June 2025
- Techtarget, “9 quantum computing challenges IT leaders should know”, April 2025
- IBM, “What is quantum cryptography?”
- Fortune Business Insights, “Quantum Cruptography Market”, June 2025
- McKinsey Digital, “Quantum sensing: Poised to realize immense potential in many sectors”

Quantum communication

- McKinsey Digital, “Quantum Communication: Trends and outlook”, February 2025
- McKinsey Digital, “Quantum communication growth drivers: Cybersecurity and quantum computing”, February 2025
- MIT Technology Review, “What is quantum communication?”, February 2019
- Restena.lu, “Luxembourg Experimental Network for Quantum Communication Infrastructure (LuxQCI)”
- Nasa, “Quantum Communication 101”
- The Business Research Company, “Quantum Communication Global Market Report 2025”
- BBG.com, “Are you ready for Quantum Communications?”, March 2023
- Market Research Future, “Quantum Communication Companies”
- Markets and Markets, “Quantum Communication Market”, November 2024
- Grand View Research, “Quantum Communication Market Summary”
- Quside, “Quantum Random Number Generator (QRNG) Everything You Need to Know”



EuroCC 2 has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101191697. The JU receives support from the European Union's Digital Europe Programme and Germany, Bulgaria, Austria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Ireland, Italy, Lithuania, Latvia, Poland, Portugal, Romania, Slovenia, Spain, Sweden, France, Netherlands, Belgium, Luxembourg, Slovakia, Norway, Iceland.

LUXINNOVATION TECHNOLOGIES AT A GLANCE REPORT

Discover more insightful content at www.luxinnovation.lu/knowledge-hub

Luxinnovation knowledge digest contributors

Research & writing: Tiffany Devresse
Analysis support: Samira Bouzid
Editing & review: Sara Bouchon, Lena Mårtensson

LUXINNOVATION
#MakingInnovationHappen