Horizon
The EU Research & Innovation Magazine

European Commission

# Codemakers race to secure the internet as quantum threat looms

With quantum computing on the horizon, cryptographers are working to secure digital communications against a new generation of potential threats.

31 July 2025 - By ANTHONY KING

How do you outsmart a computer that could soon eclipse anything we have ever built? That is the challenge facing researchers who are working to build up our defences against the coming age of quantum computing.

Quantum computers promise a giant leap in computational power, but they will also bring risks. Their code-breaking capabilities could enable governments or criminals to intercept online communications and steal sensitive data. The threat is not a distant one.

According to Professor Marcos Curty, a leading expert in quantum communication and cryptography, there is a reasonable probability that the first such computers could be switched on within the next 10 to 15 years. We need to start preparing now.

“We want to be sure that messages can continue to be sent securely without someone being able to access that information, either now or in the near future,” he said.

## Training for tomorrow

Curty is a communications engineering professor at the University of Vigo in Spain and the scientific director of the Vigo Quantum Communication Center (VQCC) based there.

Part-funded by the EU, the VQCC officially started in January 2022. It is a key node in the European Quantum Communications Infrastructure – the EU’s flagship effort to build a secure quantum communication infrastructure across Europe.

The aim is to make Vigo an international hub for quantum-safe communications. In line with this ambition, Curty is coordinating an EU-funded training network called Quantum-Safe Internet (QSI) to develop quantum-

resistant cryptography and quantum key distribution technologies.

Bringing together researchers from five EU countries, as well as from Canada, Japan, Switzerland, the UK and the US, the network intends to train young cryptographers for the challenges of a quantum computing world.

## The clock is ticking

Quantum computers may still be a few years off, but the risks are already present.

“One of our biggest concerns with cryptography is the ‘store now, decrypt later’ concept,” said Silvia Ritsch, a PhD candidate at Eindhoven University of Technology in the Netherlands. “Someone could store your encrypted communications today and wait until they have the tools to access them in the future.”

The idea is simple, yet serious. Third parties can intercept and store encrypted data now, and wait until more powerful decryption tools, such as quantum computers, are available in the future. Once they have those tools, they can go back and decrypt the stored data, which may still be sensitive or valuable.

That is where cryptographers come in. They study, design and test new methods for protecting data. Their role will take on added importance in the context of quantum computing.

According to Curty, upgrading the digital infrastructure that protects communications could take five to seven years, making early preparation and improvements in cryptography essential.

## Evolving tools for evolving technology

Codes are not new. Julius Caesar used a simple alphabet-based cipher to conceal military information. Over time, these simple systems have evolved into the complex cryptographic methods we rely on today, protecting everything from online payments to personal health records.

“Protecting company secrets from foreign digital spying will become even more relevant in future,” said Curty. “And concerns about personal privacy have become more prominent, especially following recent whistleblower revelations about mass surveillance.”

Today’s encryption systems rely on mathematical puzzles that are easy to solve with a private key, but extremely difficult without one. These puzzles form the backbone of secure online communication. But as quantum computing capabilities develop, they may become easier to crack.

There are two possible solutions: quantum cryptography, based on quantum mechanics, and post-quantum cryptography, relying on advanced mathematical algorithms.

## The quantum puzzle

Another member of the QSI team is Alex Grilo, an experienced cryptography researcher with the French National Centre for Scientific Research based at the Sorbonne University in Paris, France. He specialises in constructing quantum public-key encryption and secret-sharing protocols, and warns of the potential dangers.

“If a malicious party breaks our current cryptography using a quantum computer, all our private information is suddenly vulnerable,” he said.

That’s the bad news. The good side to quantum is that it can also offer solutions to this problem.

Quantum cryptography uses the principles of quantum mechanics to enable secure communication. One advantage of quantum systems is that information cannot be measured or copied without changing it, meaning eavesdropping attempts are detectable.

“Any attempt by an eavesdropper to access information encoded in a quantum state will inevitably disturb the state,” said Curty.

The method uses a string of light pulses which act like an advanced Morse code that cannot be intercepted without being disrupted.

“If you try to copy a quantum particle, you will disturb the particle,” explained Alessandro Marcomini, a PhD student at the University of Vigo. His research focuses on using quantum systems to securely share cryptographic keys, rather than the message itself.

Post-quantum cryptography, on the other hand, does not rely on quantum physics, but instead develops new mathematical algorithms designed to be difficult for quantum computers to solve. This is the area where Ritsch has focused her doctoral research.

“Quantum computers work very differently from classical computers, so it requires that we really think differently about the problems,” she said. This involves designing non-linear problems and paradigm shifts that puzzle quantum computers.

# Building a global defence

Clearly, this is an issue of global concern, and international exchange and collaboration are central to the work of the QSI team, not just within Europe, but also beyond.

Ritsch recently visited the University of Amsterdam to deepen her cryptography expertise. In 2024, Marcomini spent three months at the University of Toyama in Japan, where he worked alongside Japanese experts in quantum communication. A further exchange is planned in 2025.

Both Marcomini and Grilo will team up with Japanese partners to present their work at Expo 2025 in Osaka, Japan. Through talks in Japanese and English, interactive demonstrations and games for children, they aim to raise awareness about quantum threats and showcase the creative minds working to counter them.

Quantum computers may still be a decade away from widespread use, but the race to secure the internet has already begun.

*Research in this article was funded by the Marie Sk?odowska-Curie Actions (MSCA). The views of the interviewees don’t necessarily reflect those of the European Commission. If you liked this article, please consider sharing it on social media.*

### Showcasing EU research at the World Expo

**Osaka, Japan**
13 April – 13 October

This summer, millions of people from around the world will head to Osaka, Japan, for **Expo 2025**. At this global gathering, countries and regions will share how they’re tackling some of today’s biggest challenges, from sustainability and digital connectivity to inclusivity and security.

The central theme of this year’s event is **Designing Future Society for Our Lives**. Visitors will get a chance to see how **EU-funded research** is helping shape that future. QSI will be featured during the **Peace, Human Security and Dignity** thematic week, which runs from 1 August to 12 August. The EU’s **Nurturing Tomorrow** pavilion reflects

Europe’s commitment to building a greener, more connected and inclusive world.

The EU pavilion is hosting exhibitions, talks and interactive experiences that spotlight **cutting-edge EU research and innovation projects** – all aimed at solving real-world problems and building international cooperation. Whether you’re curious about the future of clean energy, digital tech, or inclusive design, there’s something for everyone.

**Virtual visit**
Can’t go to Osaka? Explore the Expo online at:
https://www.expo2025.or.jp/en/future-index/virtual/virtual-site/

# More info

- QSI
- QSI project website
- EU Digital Strategy
- EU Cybersecurity strategy
- The European Quantum Communication Infrastructure (EuroQCI)
- EU at Expo 2025