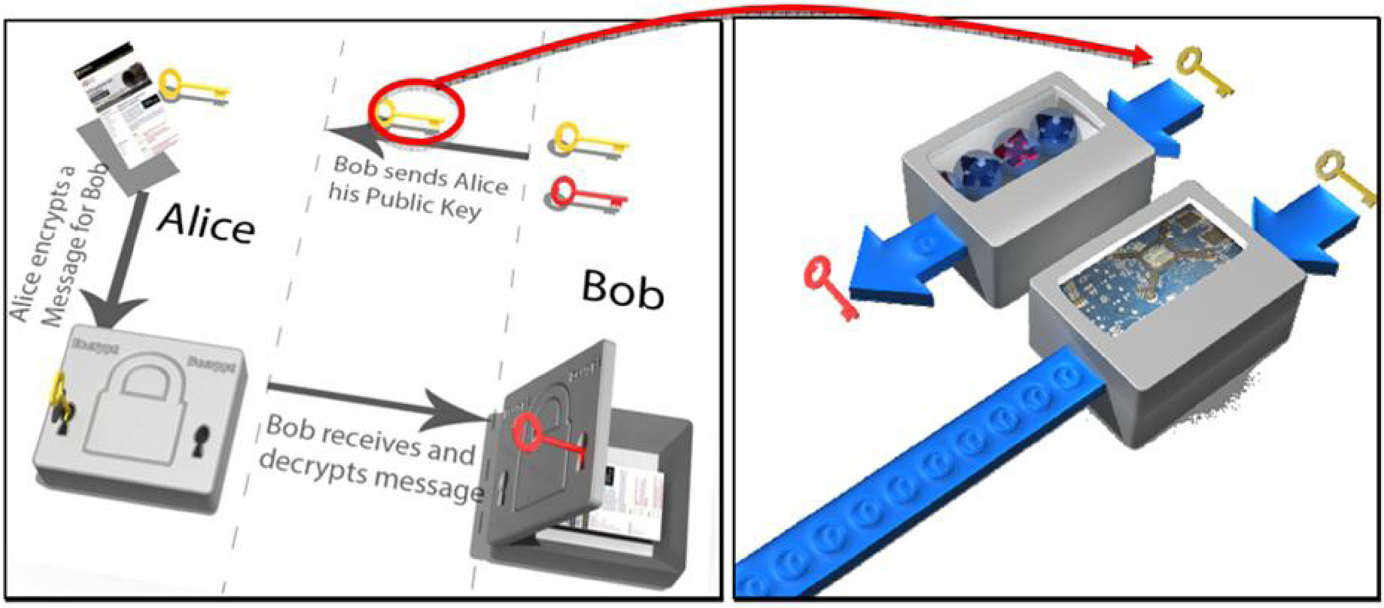
Quantum Computing and the risk to security and privacy

The advent of large-scale quantum computing offers great promise to science and society, but brings with it a significant threat to our global information infrastructure. Public-key cryptography - widely used on the internet today - relies upon mathematical problems that are believed to be difficult to solve given the computational power available now and in the medium term.

However, popular cryptographic schemes based on these hard problems – including RSA and Elliptic Curve Cryptography – will be easily broken by a quantum computer. This will rapidly accelerate the obsolescence of our currently deployed security systems and will have dramatic impacts on any industry where information needs to be kept secure.

Quantum-safe cryptography refers to efforts to identify algorithms that are resistant to attacks by both classical and quantum computers, to keep information assets secure even after a large-scale quantum computer has been built.


Alice encrypts a Message for Bob
Alice
Bob sends Alice his Public Key
Bob
Bob receives and decrypts message

A - Eavesdropper obtains public key from public channel

B - Quantum computer can break security by reverse computing private key faster than a conventional computer

What is at risk?

Without quantum-safe cryptography and security, all information that is transmitted on public channels now – or in the future – is vulnerable to eavesdropping. Even encrypted data that is safe against current adversaries can be stored for later decryption once a practical quantum computer becomes available. At the same time it will be no longer possible to guarantee the integrity and authenticity of transmitted information, as tampered data will go undetected. From business, ethical, and legal perspectives, this would violate the regulatory requirements for data privacy and security that are in existence today.

Cryptanalysis and the standardization of cryptographic algorithms require significant time and effort for their security to be trusted by governments and industry. ETSI is taking a proactive approach to define the standards that will secure our information in the face of technological advance.

Quantum-safe cryptography and security is essential for:

- Protecting government and military communications
- Securing financial and banking transactions
- Assuring the confidentiality of medical data and healthcare records
- Safeguarding the storage of personal data in the cloud
- Restricting access to confidential corporate networks

ETSI TC Cyber Quantum Safe Cryptography (QSC) Working Group

The ETSI Cyber Quantum Safe Cryptography (QSC) Working Group aims to assess and make recommendations for quantum-safe cryptographic primitives protocols and implementation considerations, taking into consideration both the current state of academic cryptography research and quantum algorithm research, as well as industrial requirements for real-world deployment. Our focus is on the practical implementation of quantum safe primitives, including performance considerations, implementation capabilities, protocols, benchmarking and practical architectural considerations for specific applications. Our objectives DON'T include the development of cryptographic primitives.

This group considers the security properties of the proposed algorithms and protocols along with practical considerations, such as extensible security architectures and technology switching costs, which will allow these recommendations to support a variety of industrial use cases. We make pragmatic comparisons and concrete characterisations and recommendations to assist the global technology community to select and deploy the best available quantum-safe alternatives.

Our published specifications can be found here: https://www.etsi.org/standards-search#TB=856,836

For further details on QSC please visit: http://www.etsi.org/qsc

Q4 2018

ETSI provides members with an open and inclusive environment to support the timely development, ratification and testing of globally applicable standards for ICT-enabled systems, applications and services across all sectors of industry and society. We are at the forefront of emerging technologies. We address the technical issues which will drive the economy of the future and improve life for the next generation. We are a not-for-profit body with more than 850 member organizations worldwide, drawn from 68 countries and five continents. Members comprise a diversified pool of large and small private companies, research entities, academia, government and public organizations. ETSI is one of only three bodies officially recognized by the EU as a European Standards Organization (ESO).

www.etsi.org

ETSI, 650 Route des Lucioles, 06921 Sophia Antipolis Cedex, France. Tel: +33 4 92 94 42 00 - info@etsi.org