Global Developments

Recently there has been remarkable progress in the deployment of quantum technologies in communication infrastructures, with several quantum key distribution (QKD) networks under construction around the world. In the UK, metropolitan quantum networks have been built by the Quantum Communications Hub in Cambridge and Bristol, connected by a long-distance link via London. Quantum digital signatures were demonstrated in the NICT metro network in Tokyo. Meanwhile in China a 2000km backbone connects Beijing and Shanghai, while the Micius satellite will extend QKD to global distances. The current high-level of activity in quantum communications means that there is a pressing need to develop industrial standards for the technology.

Unique Advantages of Quantum Cryptography

Interest in quantum cryptography stems from its unique security properties derived directly from the Laws on Nature, rather than assumptions about the difficulty of certain mathematical operations. It will allow networks that are more resilient to technological advances in the future. There is a concern that network communications that are encrypted using conventional public key cryptography may be stored today and decrypted in the future when more powerful processors or new methods of crypt-analysis are available. In contrast, quantum cryptographic protocols should be resilient to all advances in computing and mathematics.

The first applications of quantum cryptography are likely to be those requiring long term secrecy, such as encryption of sensitive government or corporate data or the health records of individuals. Recently demonstrated examples include secure communication of human genome sequences and inter-site data replication in the financial sector.

The Threat of Quantum Computers

Quantum cryptography will also be secure from a quantum computer. Quantum computers can process the inputs of a calculation in parallel and can therefore solve certain numerical problems much more efficiently than a “classical” processor. We know that a quantum computer can factorise large integers very efficiently. As the factorisation problem is the basis of conventional public key cryptography, this would significantly weaken many of the techniques that we rely on today. As such there is a pressing need to develop cryptography that will remain secure when large scale quantum computers become available. The solution to these new threats is likely to involve a combination of both quantum cryptography and new “quantum-resistant” algorithms, with improved resilience to number crunching by a quantum computer.

The Need for Industrial Standards

Standards are essential for ensuring the interoperability of equipment and protocols in complex systems, as well as stimulating a supply chain for components, assemblies and applications through the definition of common interfaces. Without standards there would be no global networks for fibre optic and mobile communications, or low cost consumer electronics based on reliable and widely available components from multiple suppliers. New standards are required to integrate quantum communications into networks and to stimulate its commercialisation.

ETSI has been leading the development of industrial standards for quantum communications through their Industry Specification Group (ISG) for QKD. Its mission is to develop ETSI Group Specifications and Reports describing quantum cryptography for ICT networks. To date it has published several Group Specification documents on QKD Use Cases, Application Interfaces, Security Proofs, Module Specification and Characterisation of Components, and most recently an ETSI White Paper on the Implementation Security of QKD.

Current work items of the ISG focus upon defining a standard interface to deliver key material to applications, deployment scenarios for QKD, the metrology of QKD systems and implementation security issues. The ISG is also working on establishing a security evaluation procedure for QKD equipment which will form the basis of a security certification process.

The work of the ETSI ISG in QKD is important to enable the future interoperability of the quantum communication networks being deployed around the world. Just as important, it will ensure that quantum cryptography is implemented in a safe manner that mitigates the risk of side channels and active attacks. By defining common interfaces, it will stimulate markets for components, systems and applications.

The membership of the ISG comprises large companies, telecom operators, SMEs, NMIs, government labs and Universities and has representatives from North America, Asia and Europe.

For further details on Qkd please visit: http://www.etsi.org/qkd

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