Question 15/17 – Quantum-based security

(Continuation of Question 15/17)

1 Motivation

The advent of large-scale quantum computers offers both potential significant benefits and disruptions on conventional telecommunication systems based on ICT.

On one hand, quantum technologies can enhance the telecommunications/ICT infrastructure, applications and services. Like any other communication systems and networks, such kind of solutions need to be secured, e.g. quantum enhanced networks.

On the other hand, the impact of some properties that quantum computers can exhibit due to their nature can lead to significant threats.

Indeed, the current cryptography security relies on computationally difficult problems: a discrete logarithmic problem and an integer-factorization problem. They are considered to be difficult to solve in a reasonable time, given the current architectures of current computers available today and in the medium term. Yet, public key cryptography using asymmetric keys is a cornerstone of authentication over public networks. As, by their nature, quantum computers can solve integer-factoring and discrete-logarithm problems in a reasonably fast time compared to current computers. They are, by ripple effect, able to break the foundations on which public key cryptography is currently built on, threatening an existential corner stone of todays' cyber life and digitalization. Such attack, that breaks current cryptography using an emerging quantum computer, is known as quantum attack.

The quantum attack threats can be addressed by different quantum-safe solutions.

One quantum-safe solution is to leverage the quantum physics and information, known as Quantum Key Distribution (QKD).

QKD enables two parties to produce a shared random secret key known only to them which can be used to encrypt and decrypt messages using conventional cryptographic algorithms. The security of QKD is derived from quantum physics, and does not rely on computational power assumptions, for which reason it makes QKD resist to quantum attacks (but exposed to implementation attacks). QKD had two limits that create network topological and integration issues: a) it is point-to-point (p-t-p) and can only be applied to two parties, A and B; and b) it has distance limitations on its communication channel, i.e. quantum channel. To overcome these two limitations, the concept of QKD networks has been introduced in the industry consisting of (1) an ensemble of nodes that are linked together through QKD systems working in p-t-p, and (2) a management system that is shared between and embedded in each of the QKD nodes. The purpose of this management system is to distribute secret keys between two or more nodes within the same QKD network that might not be directly linked. Currently, commercial QKD systems are stable and mature enough to start planning for large scale QKD networks. There are several initiatives by companies/institutions to develop QKD networks, while standards are under development for QKD systems and QKD networks. Additionally, random numbers are a fundamental key element in engineering with important applications in cryptography. The inherent randomness, thought to be at the core of quantum mechanics, makes quantum systems a good source of entropy. Quantum Random Number Generation (QRNG) is one of the most mature quantum technologies with many alternative generation methods, ranging from small form factor chips to extraction from quantum computers. In the context of telecommunication/ICTs, QRNG is a part of QKD systems and QKD networks.

Another quantum safe solution is post-quantum cryptography (PQC) which leverages mathematics and algorithms.

PQC refers to cryptographic algorithms designed to withstand known quantum attacks. PQC aims to develop secure cryptographic systems against both quantum and classical computers and can interoperate with existing communications protocols and networks.

Finally, both QKD and PQC, which have pros and cons, can be used together forming a hybrid quantum-safe solution by which additional control planes may need to enable interoperability between them.

QKD, PQC and their hybrid usage form different use cases of quantum-safe solutions.

With the above context there is a strong need for SG17 to study:

– Security aspects of QKD, QKDN and QRNG solutions;
– QKD, QKDN and QRNG as security capability solutions for the telecommunications/ICT infrastructure, applications and services;
– Use of PQC solutions to secure the telecommunications/ICT infrastructure, applications and services in particular as hybrid use case with QKD;
– Security of quantum-based technologies used by the telecommunications/ICT infrastructure, applications and services, e.g. quantum enhanced networks.

Recommendations and technical papers/reports under responsibility of this Question as of 12 September 2024: X.1702, X.1710, X.1712, X.1714, X.1715 and X.1770, and Technical Reports TR.sec-qkd, TP.sgstruct, TR.hyb-qkd, TR.sec-ai.

Texts under development as of 12 September 2024: X.1716 (X.sec_QKDN_AA), X.1716 (X.sec_QKDN_CM), X.sec_QKD_profr, X.sec-QKDNi, and Technical Reports TR.ac-pqc, TR.hyb_qsafe, TR.kdc_qkdn, TR.QKDN-SP.

2 Question

Study items to be considered include, but are not limited to:

– What are the new and emerging topics for quantum-based security?
– What are the categories of new and emerging topics for quantum-based security?
– What are the impacts and challenges of conventional communications from advent of largescale quantum computers?
– What are the key elements for building quantum-based security?
– What is transition strategy for building quantum-based security?
– How should threats and vulnerabilities in quantum-based security be handled?
– What are the security requirements for mitigating threats in quantum-based security?
– What are the security technologies to support quantum-based security?
– How should secure interconnectivity between entities in quantum-based security be kept and maintained?
– What are globally agreeable security solutions for quantum-based security, which are based on telecommunication/ICT communications?
– What are best practices or guidelines of security for quantum-based security?
– Considering the cryptographic answers and solutions known as PQC to address the threats posed by quantum computers to encryption:
    • how telecommunications/ICTs use PQC, in conjunction with other relevant Questions?
    • when adding QKD, how telecommunications/ICTs which need to use both QKD and PQC can interoperate with both in hybrid scenario?
– As quantum-based technologies enhancing telecommunications/ICTs are developing and growing, how to ensure that they are secure?

3 Tasks

Tasks include, but are not limited to:

– Identify new and emerging topics for quantum-based security.

– Identify new categories of emerging topics for quantum-based security.

– Produce a set of technical Recommendations and Reports providing comprehensive security solutions to establish quantum-based security.

– Study to define security aspects of quantum-based security, which is based on telecommunication/ICT infrastructure.

– Study and identify security issues and threats in quantum-based security.

– Study and develop secure interconnectivity mechanisms for quantum-based security.

– Study and develop information management system for entities providing quantum-based security.

– Considering the cryptographic answers and solutions known as PQC, to address the threats posed by quantum computers to encryption:
  - study how telecommunications/ICTs use PQC, in conjunction with other relevant Questions.
  - study the use of PQC to secure the telecommunications/ICT infrastructure, applications and services in particular as hybrid use case with QKD.

– Study the security of quantum-based technologies used by the telecommunications/ICT infrastructure, applications and services, e.g. quantum enhanced networks.

An up-to-date status of work under this Question is contained in the SG17 work programme at https://www.itu.int/ITU-T/workprog/wp_search.aspx?sp=18&q=15/17.

4 Relationships

Recommendations:

– X-series and others related to security

Questions:

– All ITU-T SG17 Questions

Study groups:

– All ITU-T SGs

Standardization bodies:

– ETSI TC Cyber

– ISG-QKD

– ISO/IEC JTC 1/SC 27

– OASIS

– IETF

Other bodies:

– GSMA

– ATIS

– CCSA

– TIA

– TTA

– TTC

WSIS Action Lines:

– C5

Sustainable Development Goals:

– 8, 9, 11