European Cyber Security Perspectives 2020

kpn

National Cyber Security Centre
Ministry of Justice and Security

Deloitte.

pwc

IDQ

accenture

ANALYZEDATA

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

TNO

Universiteit Leiden
Governance and Global Affairs

Radboud University

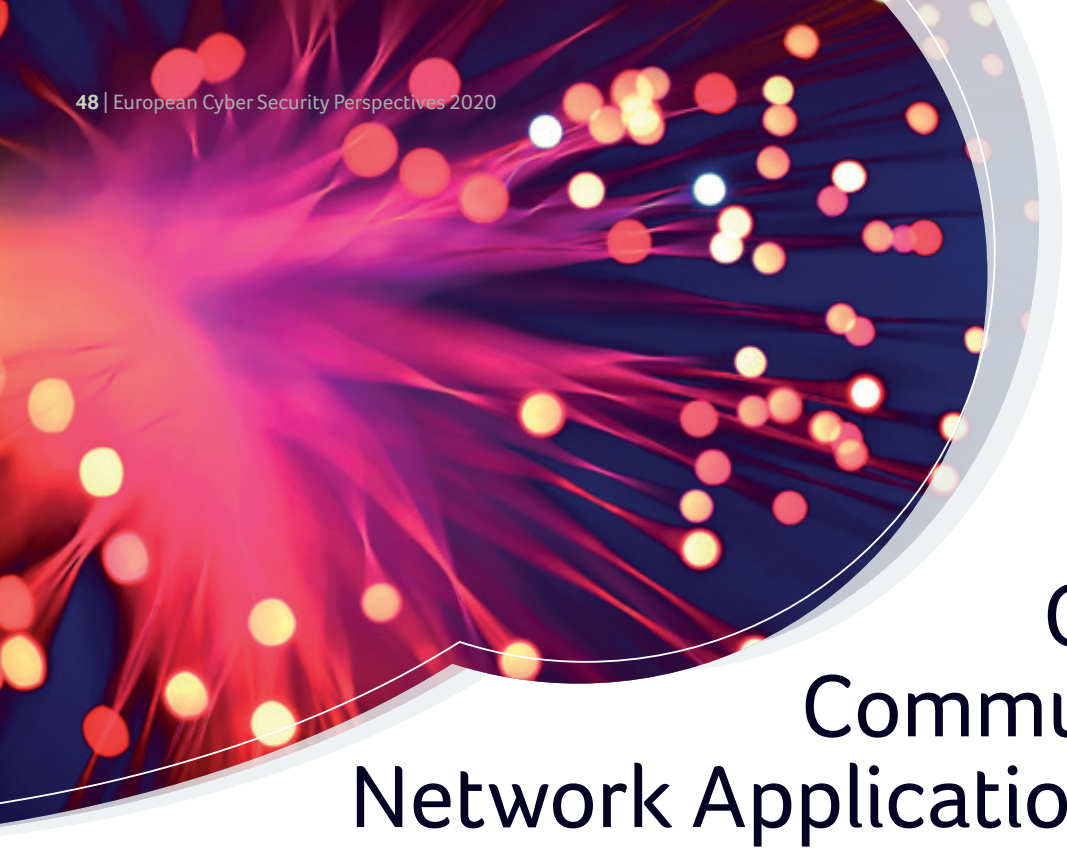
TREND MICRO
Securing Your Connected World

paloalto NETWORKS

Xebia Security

NLNETLABS

VU VRIJE UNIVERSITEIT AMSTERDAM



Quantum Communication Network Applications Today and Tomorrow

Jean-Sébastien Pegon & Bruno Huttner, IDQuantique

Quantum Key Distribution: a recognized answer to Quantum Computer security threats

It is now well known that quantum computers will break most internet security solutions relying on public key cryptography, such as RSA, ECC or Diffie-Hellman. Various announcements from governmental organisations (NSA, NASA, EU, ...), standards bodies such as NIST[1], ETSI or ITU, and private companies working on quantum computers (IBM, Google,...) have made the threat absolutely clear: encryption breaches would generate a systemic failure. Classical or post quantum cryptography solutions are based on assumptions about the ease of solving complex problems (NP Hard), knowing the computational power available at a given point of time. In contrast Quantum Key Distribution[2] (QKD) is recognized as an Information Theoretically Secure (ITS) answer to the threat to security posed by quantum computers.

> Quantum cryptography is a technology that uses quantum physics to secure the distribution of symmetric encryption keys. A more accurate name for it is Quantum Key Distribution (QKD). It works by sending photons, which are "quantum particles" of light, across an optical link. The Heisenberg Uncertainty Principle stipulates that in quantum physics observation causes perturbation. This is used to verify the security of the distributed keys and prevents the risk of eavesdropping.

> Contrary to classical physics, quantum physics is fundamentally random. It is the only theory within the fabric of modern physics that integrates randomness. Quantum Random Number Generators (QRNG) use these quantum-random properties to generate truly random numbers. Moreover, the high availability of randomness from a QRNG ensures instant inexhaustible entropy to avoid delays in transaction processing. The key generation of QKD systems is also enriched thanks to QRNGs.

QKD has been deployed by many organisations, primarily to protect data integrity or long lifetime data by using quantum keys to harden current encryption solutions. More recently telecom service providers have started to assess how this technology could be integrated in large scale backbone networks, not only to encrypt data but also to improve the security of the distributed control and management network. This article proposes an overview of the possible telecom use cases and the foreseen next steps to ease the integration of quantum cryptography in data and mobile networks.

QKD securing datacenter interconnection (DCI) or site to site connectivity

DCI requires secured high bandwidth connectivity and low latency. Hence using symmetric Layer 1 encryption

(1) https://csrc.nist.gov/events/2015/workshop-on-cybersecurity-in-a-post-quantum-world

(2) https://www.idquantique.com/quantum-safe-security/overview/qkd-technology/

such as AES-256 combined with QKD makes perfect sense, since a link of 100 Gbps can be encrypted using quantum keys in just a few microseconds with minimum bandwidth overhead[3]. It is the perfect first line of defence for all data streams at a reasonable cost per bit. Most network vendors propose this Layer 1 encryption solutions in their portfolio.

Since ETSI proposed a standard interface[4] (REST API) to exchange keys between QKD nodes and key consumer layers such as encryption equipment, the first common use case is to enhance DCI security thanks to quantum keys. The quantum key XOR with the standard session key generates a super session key, which is used by the network encryption equipment. Thus, the network security certification remains valid and it is even improved thanks to the ITS nature of QKD.

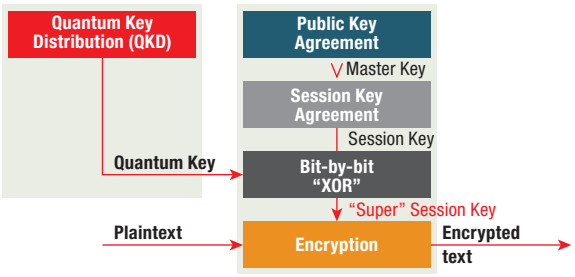


Figure 1: Dual Key Agreement

One QKD equipment can be connected to many (up to 80) consumer agents, therefore the cost of a QKD link can be "shared" by several data applications while avoiding to rely on RSA/ECC or DH for the key exchange. This solution, recognized by the industry, is available on the market and is rolled out in production environments.

The need for Quantum Communication Networks beyond site to site connectivity

The secured datacenter interconnection use case is current certainly an important commercial application of QKD. The next step is to secure large telecom networks with hundreds of nodes. QKD needs to be integrated in existing designs as an overlay solution with minimum impact on deployed networks, including their provisioning and monitoring. It is now possible to connect QKD nodes to each other while mapping existing topologies. The concept of Quantum Communication Network becomes a reality and enables the distribution of keys beyond standard distances (~100 km) and beyond basic point-to-point architectures. Thanks to an efficient Key Management System (KMS), keys can be routed and used by distant nodes connected to each other through QKD nodes or trusted repeaters. It opens the door to broader applications, for instance in Software Defined Networks (SDN) and mobile transport optical networks.

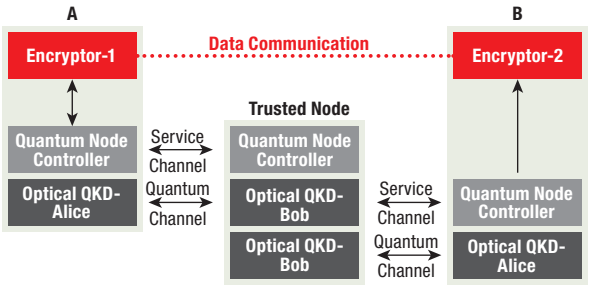


Figure 2: Trusted Node overview

QKD integrated in an SDN architecture

The digital transformation of the economy and enterprises has changed our day to day life. It is also impacting legacy IP services, such as MPLS-based solutions. This transformation for network service providers is enabled by SDN and Network Function Virtualization (NFV). SDN is an overlay technology optimizing the use of private MPLS-based and internet-based connectivity. Therefore, it improves the network resource usage based on application performance requirements. SDN allows network operators to use web-based interfaces frequently relying on Application Programming Interfaces (APIs) to order, configure and operate real-time network carrier nodes and services. SDN is also used by enterprise customers to smoothly configure internet services or cloud connectivity. It provides agility and speed of execution, thanks to automatic setup. It leads to significant productivity improvements and over the top business models.

However, this creates new security challenges since data is carried over the internet in order to reach hybrid clouds, mixing public and private hosted services. SDN is orchestrated centrally exchanging critical configuration messages to remote nodes. QKD technology on one hand can improve the security of SDN control and management planes but also needs to be integrated and remotely managed by SDN controllers to benefit from the same agility and configuration processes as new network architectures. Major carriers are already looking at using QKD integrated in SDN networks to improve the security level and prevent new attack vectors.
SDN control plane uses standard network security protocols such as SSH, TLS or IPSec, which can be combined with QKD. The DH session key can be XOR with a Quantum key provided by the QKD node[5].
Existing security certifications of the SDN network remain valid, but the security of the key exchange

[3] https://www.idquantique.com/testing-begins-on-uks-ultra-secure-quantum-network-link-using-the-equipment-of-id-quantique/

[4] https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_QKD014v010101p.pdf

[5] Alejandro Aguado, Victor Lopez, Jesus Martinez-Mateo, Thomas Szyrkowiec, Achim Autenrieth, Momtchil Peev, Diego Lopez, and Vicente Martin "Hybrid Conventional and Quantum Security for Software Defined and Virtualized Networks" https://ieeexplore.ieee.org/document/8064559

becomes quantum-safe thanks to QKD and QRNG. To speed up the adoption of QKD in SDN networks, new interfaces need to be defined and standardized. The good news is that there is already some activity within ETSI and ITU defining SDN interfaces to QKD equipment. This ongoing standardization is an important step towards large scale implementations and vendor interoperability. It is also planned to demonstrate its implementation in 2020 through a European Testbed project called "OpenQKD" involving 38 European partners including major Telecom Service Providers[6].

QKD securing 4G/5G Backhaul

As 5G mobile networks are being rolled out to boost B2B digital transformation in various critical sectors such as e-Health, autonomous vehicles, or smart Cities/Factories/Buildings, the risk of cyberattacks has never been greater or the attack surface wider. Therefore, the level of security expected increases compared to previous mobile network generations which were not designed to transport critical data and are certainly not quantum-safe. Like SDN, 5G standard uses TLS or IPSec protocols presenting identified security weaknesses in the key exchange protocol based on RSA, ECC or Diffie-Hellman.

pioneering QKD deployment in 5G production networks. QRNG is also used to improve the entropy of the RAND function used for the Mobile Authentication protocol[8].

5G technology, thanks to network slicing, opens new opportunities while offering differentiated services and pricing per user or IoT devices. End-to-end multi-layer security is one of the performance criteria between various profile of devices. Some of the applications of the B2B sectors relies on robotics or video analytics, which are both demanding in terms of performance (high data rate and low latency) and security. Since quantum cryptography offers universal security without degrading the performance, it is a perfect fit for critical industry use cases.

We observe that some B2B customers are ready to pay more to benefit from premium performance and long-term security ensuring forward secrecy and data integrity of critical applications. The investment in QKD technology and networks is justified to address these demanding use cases. Furthermore, Quantum Key

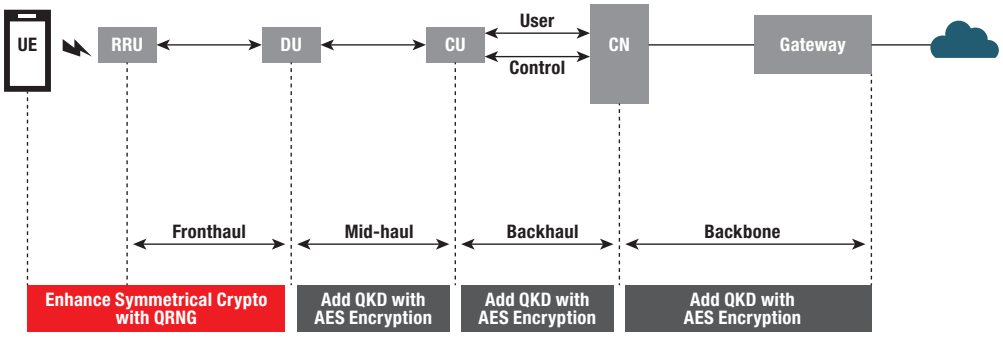


Figure 3: 5G architecture overview with Quantum Technologies

The mobile community have started to look at the impact of quantum computing attacks on 5G networks. The standardization workgroups and assessment have started. But knowing on one hand the delay between the approval of standards and its actual implementation, and on the other hand the lifetime of a mobile generation (approximately 20 years considering 2G is still available in many countries), mobile providers should certainly start their own assessment and piloting solutions in 2020.

The demand for enhanced mobile security for critical applications should allow mobile service providers to justify their investment. Some applied research papers[7] explain how QKD was successfully implemented in 5G mobile testbeds or networks. South Korea is already

Distribution can be offered only on selected network legs, for example between an edge computing node and the customer location using 5G IoT. As quantum computers mature, the volume of customers interested by quantum-safe security solutions will continue to increase justifying long-term investment to expand the solution to the entire network. Finally, quantum-safe security applied today to 4G or 5G is a service differentiator compared to other providers or wireless technologies.

(6) https://openqkd.eu/

(7) R. Nejabati, R. Wang, A. Bravalheri, A. Muqaddas, N. Uniyal, T. Diallo, R. S. Tessinari, R. S. Guimaraes, S. Moazzeni, E. Hugues-Salas, G. T. Kanellos and D. Simeonidou " First Demonstration of Quantum-Secured, Inter-Domain 5G Service Orchestration and On-Demand NFV Chaining over Flexi-WDM Optical Networks https://ieeexplore.ieee.org/document/8696286

(8) https://www.idquantique.com/quantum-safe-security/applications/telecommunications