Quantum Networking and Service

Version 1.0

December 2021

Table of Contents

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com.

Follow the GSMA on Twitter: **@GSMA.**

About the GSMA Internet Group

The GSMA Internet Group (IG) is the key working group which researches, analyses and measures the potential opportunities and impacts of new web and internet technologies on mobile operator networks and platforms. We maintain the most up-to-date knowledge base of new internet and web innovations through intelligence gathering of available global research and active participation in key Standards organisations.

www.gsma.com/workinggroups

1 Introduction

1.1 Overview and Scope

Scope of the document is to address two main avenues:

1. The **seamless networking integration** of quantum nodes/system with high Technology Readiness Level (TRL), e.g., QKD, QRNG, Trusted Nodes, etc in current networks (e.g, fixed and 4G/5G infrastructures);
2. the **modelling of quantum services**.

Concerning the topic 1), the document is considering:

a) management, control and orchestration (e.g., functional architectures, abstractions, interfaces layering, topology);
b) b) physical integration (e.g., integrated photonic components for QKD, quantum channels integration with WDM channels).

High level integration requirements are derived, including: interoperability, robustness, efficiency, scalability, policy control, application-oriented, etc. A roadmap for integration is also proposed.

Regarding the topic 2) the document is considering:

a) applicability of the “as-a-service” model for different end-to-end quantum services (e.g., for application-to-application, device-to-device, node-to-node applicability) in actual scenarios with the combination/integration of different technologies (e.g., QKD for SDN, for NFV, for MEC, for 5G Slicing, etc…);
b) analysis of main aspects about SLA, sustainability and biz impacts.

Moreover, the document is providing also a critical overview of the ongoing experimental Proof-of-Concepts (PoC) and use-cases and the migration strategy to integrate quantum nodes/system with high TRL in current networks (e.g, fixed and 4G/5G infrastructures).

Lessons learnt and proposals for new PoC and use-cases (including topics such as also Passwordless, DLT, Post Quantum Cryptography) are als provided.

Eventually recommendations and guidelines are provided to avoid standardization gaps and/or potential overlapping (e.g., ITU, IETF, ETSI, CEN-CENELEC…) in the domain of Quantum Networking and Services, also to set actions/synergies in standardization bodies

Detailed technical analysis and specifications are out of scope, but references to the state-of-the-art and best practices are listed for the Readers willing to get more details.

1.2 Abbreviations

Term	Description
P	Polynomial Time
NP	Non -Deterministic Polynomial Time

Term	Description
BQP	Bounded-error Quantum Poly-Time
DH	Diffie-Hellman
FCAPS	Fault, Configuration, Accounting, Performance, Security
IKE	Internet Key Exchange
IPsec	Internet Protocol security
MACsec	Medium Access Control security
OSI	Open System Interconnection
OTN	Optical Transport Network
PPP	Point to Point Protocol
PSPACE	Polynomial Space
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution
SDN	Software Defined Network
SSL	Secure Session Layer
TLS	Transport Layer Security
VPN	Virtual Private Network

1.3 References

Ref	Doc Number	Title
[1]	[Boaron2018]	Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussières, Ming-Jun Li, Daniel Nolan, Anthony Martin, and Hugo Zbinden, Secure Quantum Key Distribution over 421 km of Optical Fiber, Phys. Rev. Lett. 121, 190502 – Published 5 November 2018

Ref	Doc Number	Title
[2]	[Bacco2019]	Bacco, D., Da Lio, B., Cozzolino, D. et al. Boosting the secret key rate in a shared quantum and classical fibre communication system. Commun Phys 2, 140 (2019). https://doi.org/10.1038/s42005-019-0238-1
[3]	[Cao2019]	Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma and J. Zhang, "Cost-efficient quantum key distribution (QKD) over WDM networks," in IEEE/OSA Journal of Optical Communications and Networking, vol. 11, no. 6, pp. 285-298, June 2019, doi: 10.1364/JOCN.11.000285.
[4]	[Wang2020]	R. Wang et al., "End-to-End Quantum Secured Inter-Domain 5G Service Orchestration Over Dynamically Switched Flex-Grid Optical Networks Enabled by a q-ROADM," in Journal of Lightwave Technology, vol. 38, no. 1, pp. 139-149, 1 Jan.1, 2020, doi: 10.1109/JLT.2019.2949864.
[5]	[Chapuran2009]	Chapuran T. E. et al., Optical networking for quantum key distribution and quantum communications, New Journal of Physics, 2009 New J. Phys. 11 105001.
[6]	[Bahrami,2020]	Arash Bahrami , Andrew Lord, Timothy Spiller, Quantum key distribution integration with optical dense wavelength division multiplexing: a review, IET Quantum Commun., 2020, Vol. 1 Iss. 1, pp. 9-15
[7]	[Kumar2015]	Kumar, R.; Qin, H.; Alléaume, R. Coexistence of continuous variable QKD with intense DWDM classical channels. New J. Phys. 2015, 17, 43027.
[8]	[Alléaume2020]	Alléaume, R. Aymeric, C. Ware, and Y. Jaouën, "Technology Trends for Mixed QKD/WDM Transmission up to 80 km," in Optical Fiber Communication Conference (OFC) 2020, OSA Technical Digest (Optical Society of America, 2020), paper M4A.1.
[9]	[Kumar, Qin2015]	Kumar, R., Qin, H., Alléaume, R.: ‘Coexistence of continuous variable QKD with intense DWDM classical channels’, New J. Phys., 2015, 17, (4), p. 043027, doi: 10.1088/1367-2630/17/4/043027
[10]	[GSMA2021]	https://www.gsma.com/newsroom/resources/ig-11-quantum-computing-networking-and-security/
[11]	[Hahn2019]	Hahn, F., Pappa, A. & Eisert, J (2019). Quantum network routing and local complementation. npj Quantum Inf 5, 76.
[12]	[Iranzo2012]	Iranzo, J., & Manrubia S. C., (2012) Evolutionary dynamics of genome segmentation in multipartite viruses. Proceedings of the Royal Society B – Biological Sciences 279: 3812–3819.
[13]	[Mohamed,2015]	Mohamed, F. A., & Ali, N. A. M. (2015). Space debris low earth orbit (LEO). International Journal of Science and Research (IJSR), 4.
[14]	[Raja2021]	S. P. Raja, "Green Computing and Carbon Footprint Management in the IT Sectors," in IEEE Transactions on Computational Social Systems, vol. 8, no. 5, pp. 1172-1177, Oct. 2021, doi: 10.1109/TCSS.2021.3076461.
[15]	[Krishnaswamy 2020]	Quantum Blockchain Networks, D.Krishnaswamy, 2020. https://dl.acm.org/doi/abs/10.1145/3397166.3412802
[16]	[ITU]	https://www.itu.int/pub/R-REC
[17]	[ETSI]	https://www.etsi.org/committee/qkd

Ref	Doc Number	Title
[18]	[QCaaS]	Quantum Computing as a Service Market $26 Billion by End of Decade (thequantumdaily.com)
[19]	[Kozlowski,2020]	Kozlowski, Wojciech, Axel Dahlberg, and Stephanie Wehner. "Designing a quantum network protocol." Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies. 2020.
[20]	[evQ2021]	https://evolutionq.com/quantum-safe-publications/qrng-report-2021-evolutionQ.pdf
[21]	[Dahlberg2019]	Axel Dahlberg, Matthew Skrzypczyk, Tim Coopmans, Leon Wubben, Filip Rozpędek, Matteo Pompili, Arian Stolk, Przemysław Pawełczak, Robert Knegjens, Julio de Oliveira Filho, Ronald Hanson, and Stephanie Wehner. 2019. A link layer protocol for quantum networks. In Proceedings of the ACM Special Interest Group on Data Communication (Beijing, China) (SIGCOMM '19). ACM, New York, NY, USA, 159–173.
[22]	[Huang2021]	Huang, L., Zhou, H., Feng, K. et al. Quantum random number cloud platform. npj Quantum Inf 7, 107 (2021). https://doi.org/10.1038/s41534-021-00442-x https://www.nature.com/articles/s41534-021-00442-x
[23]	[QRNG,AWS]	https://aws.amazon.com/fr/blogs/quantum-computing/generating-quantum-randomness-with-amazon-braket/
[24]	[ITU-T X.1714]	ITU-T Recommandation X.1714 (2020), *Key combination and confidential key supply for quantum key distribution networks*.
[25]	[ETSI TS 103 744]	Technical Specification TS 103 744 (2020), *CYBER;Quantum-safe Hybrid Key Exchanges (2020)*
[26]	[NIST SP 800-56Ar3]	NIST Special Publication 800-56A Revision 3(2018), *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography.*
[27]	[NIST SP800-133r2]	NIST Special Publication 800-133 Revision 2 (2020), *Recommendation for Cryptographic Key Generation*.
[28]	[NIST SP800-56Cr2]	NIST Special Publication 800-56C Revision 2 (2020), *Recommendation for Key-Derivation Methods in Key-Establishment Schemes*.
[29]	[BSI TR-02102-1]	BSI Technical Guideline TR-02102-1 (2021), *Cryptographic Mechanisms: Recommendations and Key Lengths*.
[30]	[IETF RFC 8784]	IETF Standard RFC8784 (2020), *Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security*.
[31]	[IETF RFC 7296]	IETF Standard RFC7296 (2014), *Internet Key Exchange Protocol Version 2 (IKEv2)*.
[32]	[IETF draft-ietf-ipsecme-ikev2-multiple-ke-03]	IETF draft standard draft-ietf-ipsecme-ikev2-multiple-ke-03 (2021), *Multiple Key Exchanges in IKEv2 draft-ietf-ipsecme-ikev2-multiple-ke-03*.
[33]	[IETF draft-campagna-tls-bike-sike-hybrid-06]	IETF draft experimental draft-campagna-tls-bike-sike-hybrid-06, *Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS)*.
[34]	[IETF RFC 5246]	IETF Standard RFC5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

Ref	Doc Number	Title
[35]	[cho2021]	Joo Yeon Cho, ‘Using QKD in MACsec for secure Ethernet networks’, to appear in IET Quantum Communication, 2021
[36]	[Ghernaouti-Hélie2005]	Solange Ghernaouti-Hélie, Mohamed Ali Sfaxi, ‘Upgrading PPP security by Quantum Key Distribution’, International Conference on Network Control and Engineering for QoS, Security and Mobility Netcon 2005, Lannion, France
[37]	[Ghernaouti-Hélie2005]	Solange Ghernaouti-Hélie et al, “Using Quantum Key Distribution within IPSEC to secure MAN communications”. MAN 2005 conference
[38]	[Mink2009]	Alan Mink et al., ‘Quantum Key Distribution and Commodity Security Protocols: Introduction and Integration’, International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, July 2009
[39]	[Acín2007]	Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., & Scarani, V. , ‘Device-independent security of quantum cryptography against collective attacks’. *Physical Review Letters*, *98*(23), 230501 (2007).
[40]	[Sangouard2011]	Sangouard, Nicolas, et al. "Quantum repeaters based on atomic ensembles and linear optics." *Reviews of Modern Physics* 83.1 (2011): 33.
[41]	[Arute2019]	Arute, Frank, et al. "Quantum supremacy using a programmable superconducting processor." *Nature* 574.7779 (2019): 505-510.
[42]	[Kozlowski2021]	Kozlowski, W., Dahlberg, A., & Wehner, S., ‘Designing a quantum network protocol’. In *Proceedings of the 16th International Conference on emerging Networking Experiments and Technologies* (pp. 1-16) (2020, November).
[43]	[Wehner2018]	Wehner, S., Elkouss, D. and Hanson R. Quantum Internet: A vision for the road ahead. Science 362.6412 (2018).
[44]	[Zhong2020]	Zhong, Han-Sen, et al. "Quantum computational advantage using photons." *Science* 370.6523 (2020): 1460-1463.
[46]	[Aram2008]	Harrow, Aram W; Hassidim, Avinatan; Lloyd, Seth (2008). "Quantum algorithm for solving linear systems of equations". *Physical Review Letters*. **103** (15): 150502.
[47]	[Natham2012]	Wiebe, Nathan, Daniel Braun, and Seth Lloyd. "Quantum algorithm for data fitting." *Physical review letters* 109.5 (2012): 050505.
[48]	[Guoming2017]	Wang, Guoming. "Quantum algorithm for linear regression." *Physical review A* 96.1 (2017): 012335.
[49]	[Bojia2017]	Duan, Bojia, et al. "Quantum algorithm for support matrix machines." *Physical Review A* 96.3 (2017): 032301.
[50]	[Grover1996]	Grover, Lov K. (1996-07-01). "A fast quantum mechanical algorithm for database search". *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*. STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery: 212–219.
[51]	[Childs2003]	A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. A. Spielman, Exponential algorithmic speedup by quantum walk, Proc. 35th ACM Symposium on Theory of Computing, pp. 59–68, 2003, quant-ph/0209131

Ref	Doc Number	Title
[52]	[Farhi2001]	Farhi, Edward, et al. "A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem." *Science* 292.5516 (2001): 472-475.
[53]	[Dixit2021]	Dixit, Vivek, et al. "Training restricted Boltzmann machines with a D-Wave quantum annealer." *Front. Phys. 9: 589626. doi: 10.3389/fphy* (2021).
[54]	[Farhi2018]	Farhi, Edward, Jeffrey Goldstone, and Sam Gutmann. "A quantum approximate optimization algorithm." *arXiv preprint arXiv:1411.4028* (2014).
[55]	[Moll2018]	Moll, Nikolaj, et al. "Quantum optimization using variational algorithms on near-term quantum devices." *Quantum Science and Technology* 3.3 (2018): 030503.
[56]	[Preskill2018]	Preskill, John. "Quantum computing in the NISQ era and beyond." *Quantum* 2 (2018): 79.
[57]	[Y.QKDN-iwfr]	Draft Recommendation ITU-T Y.QKDN-iwfr “Quantum key distribution networks - interworking framework”

2 Integration of quantum nodes and systems in current networks

This section will address the main issues concerning the integration of quantum nodes and systems in current networks. The integration is considered from both the physical layer and the higher levels perspectives (e.g., management and control).

The topics concerning the integration of quantum nodes and systems in current infrastructures are still limitedly covered by the standardization efforts. Integration and interoperability aspects are fundamental to plan the exploitation of such disruptive technologies and services.

The section is mainly addressing QKD systems, given the relatively high Technology Readiness Level (TRL). Nevertheless, in view of upgradability of quantum nodes and systems towards long terms scenarios (e.g., Quantum Internet) also some key open questions about the integration of quantum networks in current infrastructures is briefly considered.

This table provides a brief reminder of the concepts of technological maturity:

Standardization Readiness Level (SRL)	**Stage of Technology Development**	**Technology Readiness Level (TRL)**	**Standardization activities to consider beginning**
SRL 1	Basic research	1: Basic principles observed 2: Concept / application formulated	Identify critical measurements needed
SRL 2	Feasibility Research Multiple independent research groups	3: Proof of concept	Terminology standards Test and measurement standards
SRL 3	Prototype Development Commercial R&D being performed	4: Component / subsystem validation in lab setting 5: Component / subsystem validation in relevant environment	Characterization and performance standards Metrics and benchmarks
SRL 4	Product Development Multiple companies	6: System/sub-system prototype demonstration in a relevant environment 7: System demonstration in relevant environment	Interface standards

SRL 5	Commercial products offered by multiple companies	8: System completed and qualified through test and demonstration 9: System proven through successful operation under expected operating conditions	Testbeds Certification standards Procurement standards

Table 1 - technological maturity (source: Draft D1.4 Technical Report on Standardization outlook and technology maturity part 1: Network aspects of QIT, ITU-T FG QIT4N)

2.1 Integration: physical layer issues

The coexistence of quantum and classical communication channels on a common optical network infrastructure is a necessary condition for allowing QKD systems to move from niche markets to large volumes.

Deploying new fiber cable is indeed very expensive and quantum encryption would hard be sufficient as use case to get a return of the investment in an acceptable time. Building such a common infrastructure is made difficult by the big performance gap between classical and quantum communication links, in both achievable capacity and distance. Thanks to optical amplification and coherent optical transmission, ~10 Tbit/s classical information can be transmitted over thousands of kilometers, with no intermediate signal processing.

The record distance reported for a QKD link at the time this paper is written is 421 km [Boaron2018], but with a very low key rate (6.5 bit/s over 405 km). The current record secret key rate is 105.7 Mbit/s [Bacco2019] but over a short distance (7.9 km) and using a special fiber infrastructure (a multi-core fibers with 37 cores, with each core capable of 2.86 Mbit/s). No technology is around the corner to fill this performance gap.

It is not necessary, for secret key exchange purposes, that a QKD system achieves a bit rate comparable with that of a classical channel. It is however mandatory that the distance QKD can cover is comparable to the length of the fiber spans of the classical communication network, so that in any hybrid classical/quantum communication infrastructure the quantum channels can be terminated and processed at intermediate trusted nodes. Indicative span length values are 10-20 km for metro-access, 20-40 km for metro-aggregation and 40-100 km for metro core. Making cost effective this new network architecture, where traditional optical transport nodes (e.g., wavelength switches and packet switches) are co-located and interoperate with QKD trusted nodes, is the big challenge that QKD designers will have to face in the next years.

An example of cost model and cost-constrained network planning is reported in [Cao2019] . The working assumption made in [Cao2019], and hereinafter, is that classical and quantum communication channels will share the same fiber by means of wavelength division multiplexing (WDM) techniques.

Excluding the use of separate fibers because of the aforementioned cost issues, WDM ensures the highest possible segregation between classical and quantum channels. It also guarantees the compatibility with multiple types of signal formats and QKD systems flavors.

Finally, it allows to dedicate wavelengths for the transmission, over classical channels, of information needed for synchronization and processing of the quantum data exchanged by Alice and Bob. In a WDM architecture, QKD trusted nodes may be co-located with Reconfigurable Optical Add-Demultiplexers (ROADM). Possibly, the same ROADM could be reused for switching the wavelengths of the QKD system [Wang2020]. Since no optical amplification is possible for a quantum channel, due to the no cloning theorem, and the Amplified Spontaneous Emission (ASE) noise will irremediably compromise its quality, any optical amplifier along the channel path should be by-passed, e.g. by means of high-isolation optical filters to separate and recombine classical and quantum channels.

Not only the ASE noise but also the crosstalk originated by the classical channel onto the quantum channels should kept as low as possible. This is especially an issue in DV-QKD systems that rely on single or quasi-single photon sources. The crosstalk could be due to the insufficient isolation of the optical filters used to separate the quantum channels from the classical ones or to non-linear propagation effects, such as Spontaneous Raman Scattering (SRS) in optical fiber.

The current optical filters technology should be able to guarantee enough isolation when selecting a quantum channel at Bob Receiver: 110 dB isolation is reported in [Chapuran2009], resulting from the cascade of several optical filters placed along the path from Alice to Bob.

SRS occurs when a photon of a classical channel is scattered in fiber and generates a photon at a frequency overlapping the frequency of a quantum channel. The SRS noise power is proportional to the power of the classical interfering channel (usually referred as pump) and is higher at wavelengths higher than that of the pump.

This suggests using for quantum channels wavelengths lower than the wavelengths of the classical channels. In [4][Chapuran2009] it is suggested that the total power of the classical channels is kept much lower than ~22 mW (~13.4 dBm) not to affect co-propagating QKD channels. Other non-linear propagation effects in optical fiber, as Four-Wave Mixing (FWM) and Cross-Phase Modulation (XPM), are a potential source of penalty but SRS seems to be dominant in hybrid QKD/classical systems [Bahrami,2020]. A significant exception is represented by situations where QKD and classical channels share the same portion of spectrum, typically the C band, which is the wavelength region around 1550 nm.

These systems require a proper wavelength allocation plan to prevent FWM products from falling onto the bandwidth of a QKD channel. Possible solutions to mitigate the crosstalk between classical and quantum channels are the definition of a wavelength plan that minimizes the non-linear transfer of power from classical into quantum channels and the use of high-isolation optical filters to split the bands used for the two systems.

For example, using the O band, i.e. the wavelength region around 1310 nm, for quantum channels and the C band for classical channels would introduce a large guardband in between the spectra of the two systems. This facilitates the design of the optical filters and mitigates the SRS. On the other hand, QKD systems operating in C band could exploit the low fiber loss (SMF) in that band. Moreover, the optical components for CV-QKD systems could be developed more easily in C band, leveraging on the commonalities with the components already developed for coherent optical transmission systems.

At the moment, both the options (QKD in O band and classical channels C band, or both systems in C band) are considered, with no clear winner, even if CV-QKD in C band is gaining momentum [Kumar2015]. For this kind of systems, experiments [Alléaume2020] demonstrated good robustness to the crosstalk generated by the classical channels. The system in [Kumar, Qin2015] achieved a key rate of 0.49 kbits/s over a 75 km transmission span. Aspects like the definition of a wavelength allocation are important to ensure multi-vendor interoperability, based on standardized system specifications.

Multi-vendor interoperability is guaranteed in classical communication systems by several standardization organizations, at any layer of the transport protocols stack.

The standardization of QKD systems is also progressing at a good pace [GSMA2021. However, the physical layer of hybrid classical/QKD systems remains largely unaddressed in these works.

An example of physical layer specification that would be opportune to standardize is the level or ASE noise from optical amplifiers, or of in band crosstalk from classical channels, that can be tolerated by quantum channel receiver. Typically, it should be less than the detector dark noise to lead to acceptable penalties. Another example is the maximum transmission power that should be allowed to a classical channel not to interfere with a QKD channel.

What system parameters should be monitored and how this information should be processed to infer the impact on the system performance is also an important matter of standardization. The current lack of commercial or open source modelling tools for the simulation of classical/QKD systems does not help in this aspect and it is an obstacle that should be removed. These tools would indeed allow to validate any specification using an agreed simulation framework and without making use of expensive experimental setups.

2.2 Integration of quantum nodes and systems in current optical networks: higher levels integration

Despite some technological quantum solutions are at SRL 5, seamless integration of these quantum devices or equipments is not immediate.

For example, QRNG are already standardized but the question of certification may appear in some use cases. For QKD, the standardization effort and progress are good both in ITU-T and ETSI. But here the question of certification is still the subject of work in specialized organizations (e.g. BSI in Germany and ANSI in France) and other SDO (ISO/IEC for example).

Requirements for technical integration in existing networks are very dependent on the taking into account of the standards by the suppliers and the choices of architecture and integration specific to each telecom operator. In Asian countries, which ere ahead of Europe or USA in QKD networks, the integration choices were very specific.

It is however possible to have basic understanding of high level integration requirements:

	Equipment	Networks
Interoperability	Possibility to mix different vendors	Management protocols, SDN-compatibility, open solutions if possible
Scalability	Point-to-point and multi-point keys transport	Service reconfigurability and upgradability

		Flexibility for network architectures
Efficiency	Performance of key supply and relay node routing solutions	KPIs in real-time and capacity to keep SLAs
Robustness	Device and hop-by-hop link fault detection and recovery methods	Protection solutions
Policy control	Interfaces parameters (classical and quantum channels) Internal parameters	QoS planning requirements QoS monitoring requirements QoS optimization requirements QoS provisioning requirements QoS protection recovery requirements
Application-oriented	APIs compatibility Metadatas compatibility	SDN-ready, Integrability with other existing ICT protocols and applications
Security	Standards Compliance Certification	Integrability

For the last category in previous table (security), complementarity of QKD and PQC will be a natural evolution.

According ITU-T contributors, “QKD and PQC are two pillars complementary to each other for quantum safe cryptography”. The best level of security will be the inclusion of PQC security requirements in the hybrid type of global solution.

There is a Technical Report Draft in Study 13 on “overview of hybrid security approaches applicable to QKD networks” (TR.hybsec-qkdn). This draft lists all other SDOs which may be useful to complement QKD (for example, with authentication feature) or to build future hybrid security solutions (e.g. PQC and QKD, may be also with other features). Of course, it is already possible (and already tested) to mix classical cryptographic methods and QKD solutions, for example with specific “combiner-like” features.

2.3 Management, control and orchestration

When network operators deploy the QKD network to secure data in their communication network, they need to consider how the QKD network will be incorporated into their classical communication network for QKD-derived keys’ delivery to secure application entities in classical communication network. Secure application entities can reside in various network domains within classical communication network. While QKD network domain and secure application entities' network domain can be managed and configured independently via its own SDN controller, a network operator can introduce multi-domain SDN orchestrator for a single and integrated management for both network domains. Therefore, an SDN controller is deployed for a given network domain while the whole network system is orchestrated by an SDN orchestrator.

For the use case of QKD-derived keys' delivery to secure application entities in optical transport network (OTN), with the rich fiber environment in telecom companies and because of steep performance degradation of QKD over optical fiber length compared with the performance of OTN, network operators can choose the deployment of a QKD network with dark fiber to be separated from classical OTN to operate and manage each network without the performance degradation of each network.

With this separated deployment in the network configuration and each network's operation under the network operator's integrated network management, QKD network domain and OTN network domain need to be interconnected between two nodes which, respectively, belong to each network domain for QKD-derived keys' delivery to secure application entities in OTN.

Usually this kind of interconnection plays the role of providing QKD-derived key delivery API between the key supplier, that is, QKD node and the key receiver, that is, secure application entity. Under this configuration, QKD does not guarantee that QKD-derived key will be used securely in secure application entity because its use in secure application entity is beyond the responsibility of QKD. However, in this case, as QKD node and secure application entity in OTN node belong to the same network operator's telecom network, the network operator can control both networks and guarantee the secure use of QKD-derived keys with telecom operators' security.

For the security from key generation to the use of the key in telecom network, the address matching between QKD node and OTN node in two network domains needs to be resolved before key delivery under the network operator's management.

Therefore, the network operator needs to coordinate both QKD and OTN network domains and a multi-domain SDN (Software Defined Network) orchestrator is required for this reason. In this use case, SDN orchestrator can play the coordinating role with the information received from the SDN controller of QKD network and the information from the SDN controller of OTN, respectively. With this configuration, the network operator can ensure the secure end-to-end QKD service provisioning between QKD network and OTN.

For the SDN orchestrator to play the coordinating role between QKD and OTN network domains, the interface between an SDN orchestrator and an SDN controller of QKD network needs to be defined. This interface describes the flow of information between the SDN controller performing as a server and the SDN orchestrator operating as a client.

Through this interface, SDN orchestrator can orchestrate QKD network in terms of discovery of QKD network topology, monitoring of QKD network status and resource inventory, end-to-end QKD service provisioning with path calculation in QKD network, management policy, performance management as well as the address matching as described above.

With this configuration extended, an SDN orchestrator can orchestrate multi-QKD network domains from multi-vendors via each SDN controller of each QKD network as well as both QKD and classical optical transport network domains as shown in Figure 1.

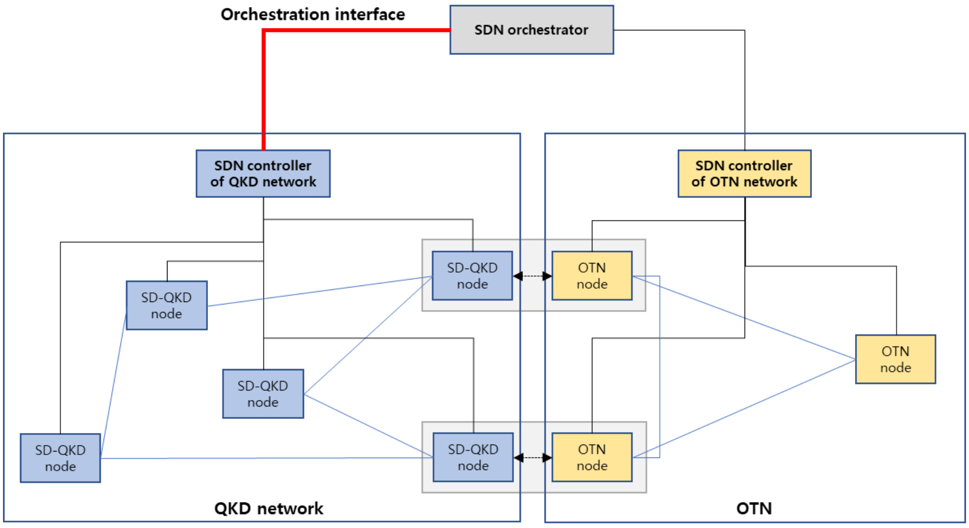


Figure 1 - Use case of SDN orchestrator for QKD network and OTN [Source: 19 - DGS QKD 018] [1]

For the security consideration, contrary to the exposed orchestration interface of the SDN controller in a QKD network, as the SDN controller in a QKD network does not directly handle QKD-derived keys generated and transported inside the QKD network, and the SDN orchestrator does not receive any QKD-derived keys through the orchestration interface from the SDN controller in a QKD network, QKD-derived keys cannot be exposed through the orchestration interface between the SDN controller in a QKD network and the SDN orchestrator. Therefore, the QKD-derived key itself can be secured from the orchestration interface.

The introduction of quantum nodes/systems will bring unavoidably to heterogeneous networks that consist of the mixture of quantum and classical communication technologies, both from terrestrial and spatial field. Additionally, the need to integrate the elements coming from different vendor will add to difficulty of operating final product.

Building separate network for QKD assures high performance and isolation but is highly impractical due to high non-incremental up-front cost, and is plainly difficult to deploy on commercial level.

On the other hand, high complexity of managing life cycle of classical and quantum channels coexisting in the same network and even sharing the same physical media, requires to adopt solutions that allow to bring the operational costs down, for example automated algorithms utilizing AI - artificial intelligence - and ML - Machine Learning - to optimize the most power and bandwidth consuming elements in processes like path computing.

SDN, already established in optical network architectures, is pacing the path for integrating quantum and classical worlds by enabling vendor agnostic, dynamically configurable control and management, both o network and service level.

There is wide existing range of security standardisation and recommendation documents related to both SDN and NFV from different bodies (ETSI, ITU-T, CIS,) to build upon. The recognition of natural SDN's concept utilization in the integration into existing network infrastructure is proved by the existence of already published standards describing model of communication between network

[1] The orchestration interface (red solid line) between the SDN orchestrator and the SDN controller of the QKD network is shown. The key delivery API (dashed line) from ETSI GS QKD-014 or remote function call from ETSI GS QKD-004 can be used for secure application entities (SAEs) in OTN nodes in the OTN network to retrieve keys from key management entities (KMEs) in SD-QKD nodes in QKD network. SAEs in OTN nodes are located within the same security boundary as their connected KMEs in SD-QKD nodes.

controller using abstract interfaces (QKD-15; Y.QKDN_SDNC..,). Above mentioned Y.QKDN_SDNC proposed functional architecture for QKDNode that include SDN Controller part.

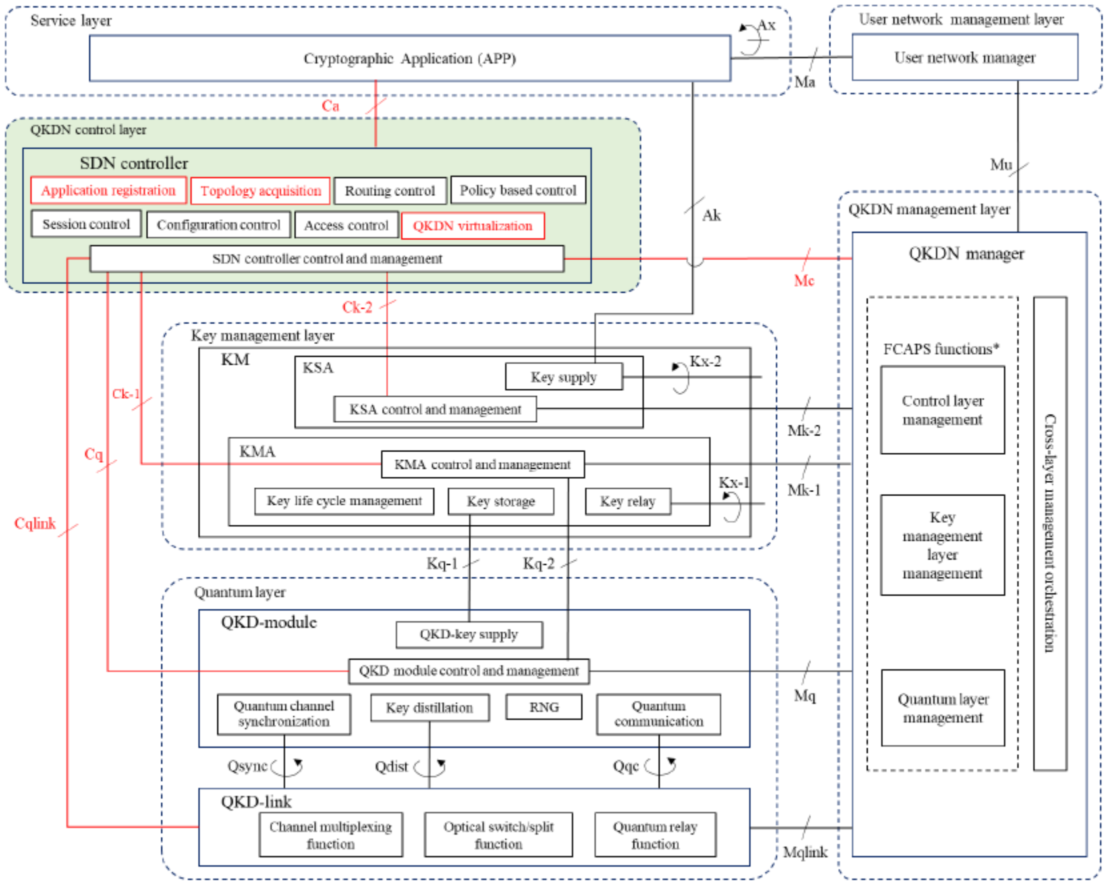


Figure 2 – Example of QKD network management and control layers

As proposed by both ETSI and ITU-T, the functions of SDN controller include application registration, topology acquisition, routing control, policy-based control, session control, configuration control, access control and QKDN virtualization. As both hierarchy and isolation is supported in SDN, according to requirements separate SDN controllers can be defined for multivendor and multi-client/domain network with potential “zero touch” integration.

From security concerns point of view, as SDN Controller only provides control and management functions, the key itself is never shared with controller (it does not add new risk to the process).

2.4 Quantum Forwarding Plane (QFP)

For obvious sustainability and usability reasons, there is a clear need for an integration as tight as possible of quantum network management procedures with those applied in current (classical) networks, adhering to the best practices in network operation usually referred as carrier grade.

This should include minimizing the impact on existing network best practices, seeking a smooth integration with operational tools and procedures.

As introduced in the following section on quantum service models, the application of the Quantum Forwarding Plane (QFP) concept guarantees a clear separation of concerns, abstracting the quantum processes from their different applications (key distribution, randomness, entangled states…) and facilitating the applicability of SDN technologies as the essential mechanism to support network management.

This, far more complex, but very flexible approach is currently being investigated in several research projects and advanced testbeds.

The SDN architecture considers a grouping of management functions to provide functionalities for managing, as appropriate, the functionalities of the planes. These functions comprise functionalities for supporting fault, configuration, accounting, performance and security (FCAPS) management. Examples of such functionalities are inventory management, software upgrades, fault isolation, performance optimization, energy efficient operations, and initial configuration of network components on all planes.

As said above, it is essential to match this functionality with the equivalent ones in classical networks and, whenever possible, reuse as many carrier grade components as possible. The current trends in network management, focused on automation by means of the integration of loosely-coupled managed domains, are in the position to address these requirements, facilitating a variety of integration patterns, from strictly hierarchical approaches based on location or business relationships to the more complex, peer-to-peer interactions that constitute one of the foundations of the current Internet.

3 Overall Integration Requirements

SDN orchestration in QKD network can be defined as the continuing process of automatically coordinating the available resources according to optimization criteria to establish and release the end-to-end QKD service provisioning through different network domains controlled by each SDN controller, respectively.

As SDN orchestration can be used to start the series of automated processes required to satisfy a customer's QKD service request generated via a customer website in telecom network, an SDN orchestrator can be a master entity which enables each SDN controller to establish and release multiple paths in its own network domain to conform a customer's end-to-end QKD service provisioning request through different network domains.

To enable the end-to-end QKD service provisioning through different network domains in telecom network, the SDN orchestrator of a network operator has the following requirements:

- Translation from the end-to-end QKD service provisioning requests from a customer to the configuration of the different network domains through each SDN controller and to the allocation of secure application entities for this service provisioning
- Establishment and release requests of the end-to-end QKD service provisioning with the inter-domain connections between secure application entities through orchestration interfaces
- Identification of multi-domain path calculation across the different network domains including inter-domain connections and endpoints for each end-to-end QKD service provisioning request
- Change of the established path calculation in QKD network with constraints from network operator
- Discovery of QKD nodes and QKD links under each SDN controller in the QKD network and an abstracted view of the QKD network topology
- Inventory monitoring of QKD-derived key resource available from key management system in each QKD node and in each QKD link
- Monitoring of FCAPS management of QKD network and notification of changes of FCAPS management in QKD network
- a clear separation of concerns, abstracting the quantum processes from their different applications (key distribution, randomness, entangled states…)

Through the orchestration interface between the SDN orchestrator and the SDN controller of QKD network, network operators can address the outlined requirements from the SDN orchestrator. The SDN controller is a server and the SDN orchestrator is a client in terms of communication between them. On the other hand, as more QKD vendors are entering the network infrastructure market, network operators should consider the possibility of passing QKD-derived keys between different QKD vendors for end-to-end QKD service provisioning. In this case the interface through which a QKD node from one QKD vendor transports QKD-derived keys to pass them to the end node from the other QKD vendor will be necessary and this interface will be important for network operators if they adopt multi-vendor policy for QKD and integratedly use them as a single QKD network. In this approach, the interface of key management system in QKD node is considered to be developed horizontally, that is, between key management systems in both QKD nodes from different QKD vendors.

Recently ETSI ISG QKD started to develop the standard for this interface [ETSI]. The vertical interface of key management system in QKD node is already used for key request and key supply from secure application entity. A next section will provide more details about ETSI relevant activities. On the other hand, ITU-T SG13 are also developing Draft Recommendation which specifies a framework for interworking QKD networks [Y.QKDN-iwfr]. This addresses both the interworking of QKD networks among multiple QKD network providers and the interworking of QKD networks with different technologies.

4 Overview of standardization efforts

4.1 ITU and ETSI relevant specifications

Series of recently published ITU-T Recommendations on QKD [ITU]

- Y3800 "Overview on networks supporting quantum key distribution" (10/2019)
- Y3801 "Functional requirements for quantum key distribution networks" (04/2020)
- Y3802 "Quantum key distribution networks – Functional architecture" Corr. 1 (04/2021)
- Y3803 "Quantum key distribution networks – Key management" (12/2020)
- Y3804 "Quantum key distribution networks – Control and management" (09/2020)

As an example the Recommendation ITU-T Y.3800 gives an overview on networks supporting QKD and addresses network aspects to implement QKD technologies.

In particular, this Recommendation addresses the following:

- an overview of QKD technologies;
- network capabilities to support QKD;
- conceptual structure and basic functions of QKD networks (QKDNs).

Figure 3 illustrates an example of applying QKD to secure a point-to-point (P-to-P) application link. QKD modules generate keys and supply them to the applications. The application link where encrypted data is transmitted can be any communication link in a conventional or a future network.

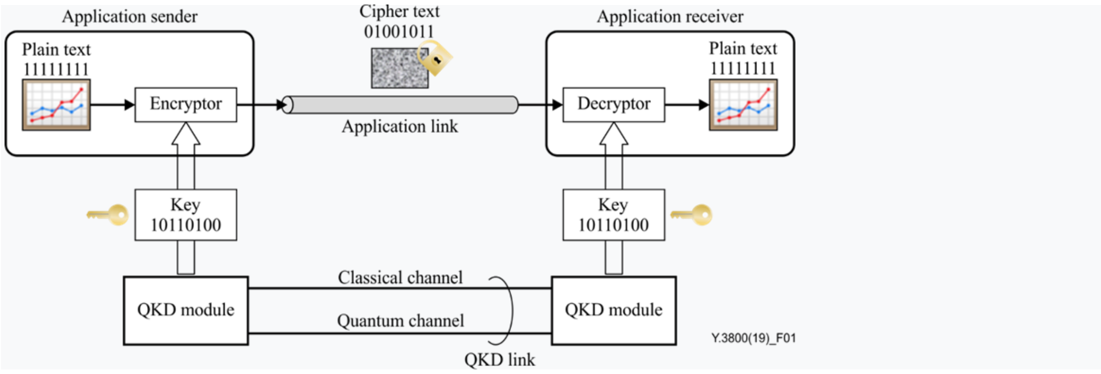


Figure 3 – Configuration example of QKD use for securing a P-to-P application link [source: ITU Y.3800]

ETSI’s Industry Specification Group (ISG) on QKD is currently developing specifications for the quantum networks and communications [ETSI]. This is the list:

- ETSI GS QKD 015 V1.1.1 (2021-03)
- ETSI GS QKD 004 V2.1.1 (2020-08)

- ETSI GS QKD 012 V1.1.1 (2019-02)
- ETSI GS QKD 014 V1.1.1 (2019-02)
- ETSI GR QKD 007 V1.1.1 (2018-12)
- ETSI GR QKD 003 V2.1.1 (2018-03)
- ETSI GS QKD 011 V1.1.1 (2016-05)
- ETSI GS QKD 005 V1.1.1 (2010-12)
- ETSI GS QKD 008 V1.1.1 (2010-12)
- ETSI GS QKD 004 V1.1.1 (2010-12)
- ETSI GS QKD 002 V1.1.1 (2010-06)

For example the ETSI GS QKD 014 V1.1.1 (2019-02) “Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API” specifies a communication protocol and data format for QKD network to supply cryptographic keys to an application.

It is in the form of an API (Application Programming Interface) that allows application developers to make simple method calls to a QKD network and to be delivered key material. It is intended to allow interoperability of equipment from different vendors.

The API defines a single interface for the delivery of key material to applications in both scenarios. It is beyond the scope of the present document to describe how a QKD network generates key material shared between distant nodes. A REST (Representational State Transfer) API is specified as a simple, scalable, widely deployed approach that is familiar to a large developer community. The REST API specifies the format of the URIs, the communication protocols (HTTPS), and the JSON (JavaScript Object Notation) data format encoding of posted parameters and responses, including key material.

4.2 Standardization activities on hybrid approaches

This section provides a landscape of the standardization activities on hybrid approaches for migration towards quantum-safe algorithms or protocols within international, regional and national organizations.

Hybrid approaches are for key exchange consist in generating a key exchange functionality by combining at least two different key exchange methods.

Quantum computing has become a serious threat for the security of existing and future communication networks. It could solve certain computational problems, such as integer factorization (which underlies RSA encryption) and discrete logarithm (which underlies DH key sharing) substantially faster than classical computers. The migration of legacy networks to quantum-safe (i.e., secure against quantum computing) networks is a complex task that needs to be well prepared. In this context, several SDOs have developed or are developing several standards on the topic of quantum-safe security.

However, most of these standardization activities are envisioned and performed by experts in post-quantum cryptography. The compatibility of those published or under study standards with QKD has not been verified presently despite the fact that QKD protocols are also key exchange protocols. Hence, hybrid approaches for key exchange consist in generating a key exchange functionality by combining at least two different key exchange methods can be considered. Nevertheless, these hybrid approaches for key exchange might not be directly applicable to QKD based on existing standards.

To overcome this gap, various efforts have been made to exploit QKD in the existing communication networks to improve their security. Many researches have been in progress for the integration of QKD with the protocols in different layers of OSI model.

While the use of QKD in fiber optical networks gets significant advances, research and development on the application of QKD in the different layers is still premature although QKD is not different from other available key distribution primitives. Compared to physical layer implementation like OTN (Optical Transport Network), generally, the changes of the existing protocols for key exchange are expected.

The examples of such research efforts are the integration of QKD point-to-point protocol (PPP) [Ghernaouti-Hélie2005] and MACsec [cho2021] at the link layer (i.e., OSI layer 2) and the integration of QKD with IPsec [Ghernaouti-Hélie2005] at the network layer (i.e., OSI layer 3). Furthermore, the integration of QKD at the transport layer (i.e., OSI layer 4) with SSL/TLS [Mink2009] has been attempted.

On the Data Link Layer, QKD can be used as a key exchange protocol for PPP which is data link protocol to connect two nodes [Ghernaouti-Hélie2005].

Medium access control security (MACsec) which is an IEEE 802.1AE standard for secure communication on Ethernet links. MACsec ensures the confidentiality, integrity and origin authenticity of Ethernet frames in local area network. The secrecy of MACsec stems from a root key that is either configured as a pre-shared key or derived from a mutual authentication protocol.

QKD can be used to provide keys for MACsec [cho2021].

For the network and transport layer, both Internet Protocol Security (IPsec) and Transport Layer Security (TLS) develop a shared secret and then use that to compute keys for encryption and integrity protection.

Internet Protocol Security (IPsec) is a suite of protocols that provides security to Internet Protocol (IP) communications at the network layer by authenticating and encrypting the IP data packets. IPsec is often used to provide a Virtual Private Network (VPN), either between two locations or between a remote device and an enterprise network. IPsec can also provide end-to-end security. Internet Key Exchange (IKE) is the protocol used to set up a security association in the IPsec protocol suite. IKE uses a Diffie-Hellman (DH) public key exchange to set up a shared session secret, from which cryptographic keys are derived. Public key techniques or, alternatively, a pre-shared key, are used to mutually authenticate the communicating parties.

Transport Layer Security (TLS) is the transport layer protocol which provides end-to-end security for network communication services. TLS is based on earlier Secure Sessions Layer (SSL) protocol and is explicitly invoked by an application. Although it is widely used in various applications, its most common use is to encrypt the traffic between a web server and a browser.

QKD keys can be used to establish the shared secret for a TLS session or an IKE security association. In this case, QKD keys would replace the DH (Diffie-Hellman) shared secret thus eliminating the need to calculate a DH shared secret [Mink2009].

All these works are moving towards the utilization of QKD technology for enhancing the security of modern computing applications on the internet.

There are several examples on hybrid approaches for key exchange mechanisms as reported in the following sub-sections:

4.2.1 ETSI TS 103 744, Quantum-safe hybrid key exchanges

ETSI TC CYBER QSC published a technical specification on quantum-safe hybrid key exchanges in December 2020. This technical specification addresses the concept of hybrid approaches for key exchanges by specifying two methods for deriving cryptographic keys from multiple shared secrets. These shared secrets might be established using quantum-safe or not quantum-safe cryptographic methods or any other ways to establish a pre-shared secret.

TS 103 744 [ETSI TS 103 744] specifies that one of the key agreement scheme shall be elliptic curve Diffie-Helman as defined in clause 5.7.1.2 of [NIST SP 800-56Ar3]. This standard specifies several cryptographic primitive algorithms that shall be used for e.g. hash functions, pseudorandom functions or key derivation functions.

Two types of hybrid key agreement schemes are specified by TC CYBER QSC. The first scheme is called ‘concatenate hybrid key agreement scheme’, the other one ‘cascade hybrid key agreement scheme’.

The first scheme consists in running all the key agreement schemes in parallel. The messages exchanged between the initiator and the responder are the result of the concatenation of the messages generated by each key agreement scheme at each step of the hybrid key agreement scheme. Furthermore, the shared secret that will be used as an input of the key derivation function is the result of the concatenation of the secrets established with each key agreement scheme and one optional pre-shared key.

The second scheme consists in running the key agreement schemes sequentially. In this case, each message exchanged between the initiator and the responder will be related to one step of one of the key agreement schemes. The final key material is computed by applying as many iterations of the key derivation function as the number of key agreement schemes composing the hybrid key agreement scheme. The results of each iteration of the key derivation function are a secret and some key material. The input secret of the i^{th} iteration is obtained with the secret exchanged by the i^{th} key agreement scheme and the secret that has been computed at the $(i-1)^{th}$ iteration. At the first iteration, the input secret may be obtained with the secret exchanged by the first key agreement scheme and a pre-shared secret.

TS 103 744 indicates that QKD is one of the possible ways to establish pre-shared secrets.

4.2.2 NIST standards (USA)

NIST didn’t write any standards dedicated to hybrid key exchanges. However, NIST provides recommendations on various options to securely generate symmetric keys from several symmetric keys or values ([NIST SP800-133r2]), and on one way to combine several secrets, established by various key exchange schemes, to generate, from multiple secrets, one secret that is used as input for a key derivation method. ([NIST SP800-56Cr2])

4.2.3 IETF RFC 8784

[IETF RFC 8784] is an IETF standard for mixing pre-shared keys in the Internet exchange protocol version 2 (IKEv2) for post-quantum security. This IETF standard has been published in June 2020.

This document describes an extension of IKEv2 to allow it to exploit alternative key exchange mechanisms by using pre-shared keys.

[IETF RFC 8784] has been written under the assumption that each IKE peer has a list of pre-shared keys along with their associated identifiers that can have been shared using any kind of post-quantum key exchange methods. Then, [IETF RFC 8784] introduces notifications that allow the initiator and the responder to use or not pre-shared keys in their IKEv2 transaction. The decision to not use pre-shared keys can be taken by one of the two parties in several steps of the protocol. In this case, the initiator and the responder use the conventional IKEv2 protocol. When a pre-shared key is used, they are combined with the three sub keys generated the conventional IKEv2 protocol specified in [IETF RFC 7296]. The combination of the sub keys with the pre-shared keys is performed with pseudorandom function.

Note – [IETF RFC 8784] doesn’t specify the key exchange methods that can be used to exchange the pre-shared secrets.

4.2.4 IETF draft-ietf-ipsecme-ikev2-multiple-ke-03 (work in progress)

[IETF draft-ietf-ipsecme-ikev2-multiple-ke-03] is an IETF draft for multiple key exchanges in IKEv2. The third draft of this IETF work item will expire in January 2022. This document describes an extension of IKEv2 to allow multiple key exchange while computing a shared secret during a Security Association setup.

[IETF draft-ietf-ipsecme-ikev2-multiple-ke-03] aims at updating [IETF RFC 7296] by giving the possibility to use alternative key exchange methods in addition to the Diffie-Hellman key exchange methods specified in [IETF RFC 7296]. The different key exchange methods are performed successively. The secrets established from each key exchange are combined to generate a shared secret that will be used in the same manner than the way the shared secret established with a Diffie-Hellman key exchange is used in [IETF RFC 7296]. The secret established with the nth key exchange is combined with the intermediate keys resulting from the (n-1) first key exchanges using pseudorandom functions.

Note – [IETF draft-ietf-ipsecme-ikev2-multiple-ke-03] doesn’t specify the additional key exchange methods. However, algorithms resistant to quantum computer attacks are mentioned as a possibility.

4.2.5 IETF draft-campagna-tls-bike-sike-hybrid-06 (work in progress)

[IETF draft-campagna-tls-bike-sike-hybrid-06] is an IETF draft for hybrid post-quantum key encapsulation methods (PQ KEM) for Transport Layer Security 1.2 (TLS). The sixth draft of this IETF informative work item will expire in September 2021. This document is intended to define hybrid key exchanges in sufficient details to allow independent experimentations to interoperate.

[IETF Draft-campagna-tls-bike-sike-hybrid-06] describes additions to TLS to support PQ hybrid key exchanges, applicable to TLS version 1.2 [IETF RFC 5246]. The defined hybrid key exchange combines the shared secrets established by two key exchange methods. One key exchange method is based on Ephemeral Elliptic-Curve Diffie-Hellman (ECDHE). The other one can be based either on SIKE, Kyber or SIKE. Those three algorithms are part of the 3rd round of NIST standardization process of key exchange algorithms that are resistant to quantum computer attacks. The hybrid premaster secret that will serve as TLS 1.2 [IETF RFC 5246] pre-master secret results from the concatenation of both shared secrets.

5 Long term perspective: towards Quantum Networks

In the long term (2030+), it is likely that quantum technologies will be exploited to develop Quantum Networks capable of providing quantum communications and networking (e.g., based on entanglement) and quantum computing services (e.g., Cloud Quantum Computing, Blind Computing, etc).

The Quantum Internet [Kozlowski2020] will leverage on traditional current network for the purpose of executing methods and protocols which are provably more efficient than the classical counterparts. In particular it is expected to enable secure quantum communication to future quantum computing devices.

A Quantums network includes quantum nodes, and links and are expected to be integrated with the current networks:

- Links: transfer of quantum information between quantum nodes. It is conveniently feasible using photons as carriers, often dubbed flying photons. For example, classical and quantum links can be used: photons are transmitted and controlled using standard components, in particular exploiting optical fibers and satellite communication. Multiplexing in frequency time, space and/or polarization can allow for increasing of the communication rate in fiber-communication.
- Quantum Nodes: storage and processing units of quantum information. They can include routing, processing, storage systems, quantum repeaters and quantum end-nodes/devices. In these nodes matter qubits are used to route, process and store the quantum information. Today, matter qubits are exploited for these uses, indeed photons are hard to store.

The main technical challenges in realising a long term quantum network, apart transmission losses and the coupling with the telecom band, include decoherence, and the conditions created by the no-cloning theorem. Specifically:

- decoherence is the loss of quantum information due to interactions with the environment;

the no-cloning theorem states that arbitrary quantum data cannot be copied. This is making impossible to use standard techniques of amplification or retransmission to compensate for transmission or decoherence losses.

Given that in a quantum network it is impossible to use standard techniques of amplification or retransmission to compensate for transmission or decoherence losses.

Nowadays networks are hybrid networks allowing just point-to-point quantum communication – QKD exchange – that is limited to the optical fiber length or satellite-to-ground distance. The end-to-end communication passes through trusted (then classical) nodes. The maximum distance reachable by now on optical fiber communication is around 400kms. A First upgrade toward an end-to end quantum communication can be obtained by the implementation of measurement-device-independent protocols [Kozlowski2020] that enable the use of untrusted devices.

Perfect solutions would be quantum repeaters, components enabling long-distance entanglement by connecting short-distance entangled pairs [Dahlberg2019]. Quantum information then is transferred exploiting entangled-based protocols.

Two entangled pairs each have one qubit in the memory of a middle repeater. An entanglement swap-operation is performed on these qubits which destroys the entanglement of the two pairs, but as a result the remote qubits become entangled. This is overcoming the roadblocks about losses and the no-cloning theorem. Nowadays no quantum repeaters exists out of the lab: the coherence time of an entangled pair is extremely short compared with the minimum time required for a communication protocol. In the future, the natural destroy of the entangled link can be a plus in term of security, but by now remains the main obstacle.

Currently no protocol stack for quantum networks has been defined and standardised, and no quantum networks capable of end-to-end qubit transmission or entanglement production have been realized.

Distillation of entanglement is the main quantum error correction procedure known for entanglement-based communication. It is less demanding on fidelity and resources with respect to quantum error correction for quantum computation, but distributed protocols incur in round trip delays due to classical communication, required in parallel in many quantum communication protocols.

Control plane protocols are also an emerging field in quantum network research, especially in the area of routing. Nevertheless we are unaware of any system-level papers, but [Kozlowski2020] which is proposing a quantum network stack including protocols for concrete hardware implementations. In particular, a high-level architecture of a quantum node is presented, where the network stack is expected to be part of a local operating system (OS). The stack is responsible for managing operations relating to the generation of entangled pairs which it executes with the help of local OS services.

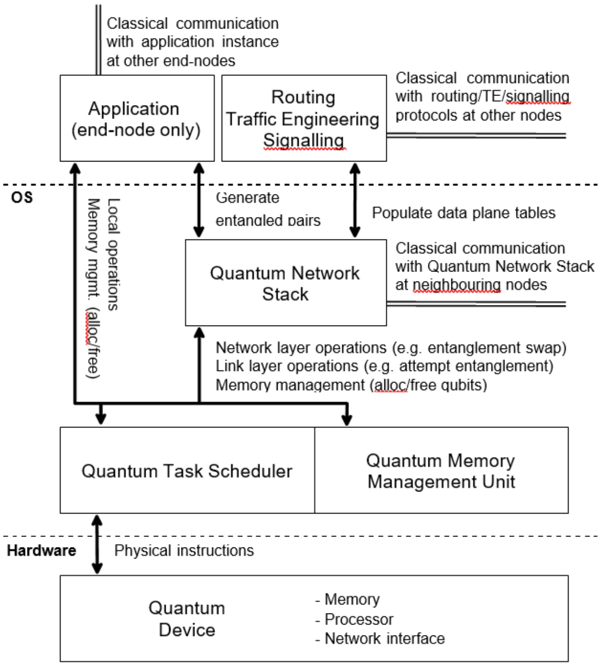

Classical communication with application instance at other end-nodes
Application (end-node only)
Routing Traffic Engineering Signalling
Classical communication with routing/TE/signalling protocols at other nodes
OS
Local operations Memory mgmt. (alloc/free)
Generate entangled pairs
Populate data plane tables
Quantum Network Stack
Classical communication with Quantum Network Stack at neighbouring nodes
Network layer operations (e.g. entanglement swap)
Link layer operations (e.g. attempt entanglement)
Memory management (alloc/free qubits)
Quantum Task Scheduler
Quantum Memory Management Unit
Hardware
Physical instructions
Quantum Device
- Memory
- Processor
- Network interface

Figure 4 - Example of Operating System for a Quantum Node

6 A generalized model enabling “quantum as a service”

Many of the approaches so far to model quantum networks and services are done in terms of layers with different functionalities (quantum layer, key management layer, etc), with not very precise definitions, focused on following the same general approach that has been successful in classical networks.

These layered approaches are based on the assumption that quantum information can be modelled in the same way as classical information, defining some sort of packetization patterns for qubits. But the nature of the technologies suitable for generating and then measuring quantum signals are based on the physical properties of communication channels, now and in the mid-term future. This has implications in the transfer of qubits from the transport perspective, and how it is modelled.

Quantum communications technologies must be integrated into a general networking framework that supports a general system view, is aware of the network and is suitable to be controlled within it, ideally in an automatized way, such that optimal performance can be achieved within the technological and physical limits.

Rather than mimicking the model of the classical network, this network framework must be based on components that implement a well-defined functionality, with this functionality defining the flow of information among the components to implement a given architecture. This flow, in turn, define the interfaces. Well-defined interfaces and clear component functionality allow for a modular view, which allows for a *disaggregated* building of the network, in the sense that different manufacturers can provide components that can work together.

The proposed model for a quantum services network reference framework considers the main logical components that exist in conceivable quantum networks and services, describing their relationship, and pointing to the places where interfaces are necessary and describe the information that has to be exchanged through them.

This approach is specifically intended to support the industrialization of quantum networks. It allows to locate the points where standards are necessary in the form of agreed interfaces, disaggregate the functionality in components that can become a separate product and make easier to integrate these additional components in the existing telecommunications network and security ecosystem.

A quantum network is essentially a communication network, with quantum devices installed in some network points. A *quantum node* encapsulates all software and hardware components necessary to manage the functionality of a quantum protocol to deliver them to final applications. This might be, for example, secret keys in the case of QKD, or entangled states in a more general case.

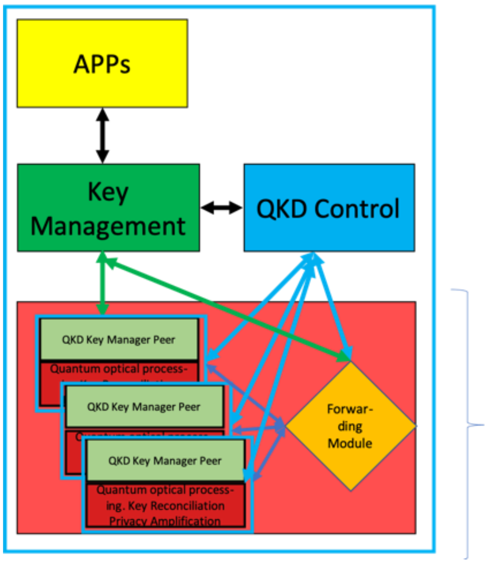
A *quantum host* is the collection of quantum modules in the same node and all the components implementing the manipulation of quantum signals over a quantum channel that links the nodes. This is akin to the typical data forwarding plane in classical networking and here the quantum part of the network can be abstracted in a similar way as the *quantum forwarding plane* (QFP), which for example, in the specific case of QKD would encapsulate a full QKD protocol.

The QFP thus constitutes the foundation for the abstraction process of grouping the required network functionality in different components defined by their characteristics relevant for a particular purpose, while hiding or summarizing characteristics irrelevant to this purpose. The QFP encapsulates all the capabilities that would be added to a standard telecommunications network to make the network quantum.

To some extent, it is an attempt to clearly define, using a terminology from networks, the so-called quantum layer in early quantum network models. A clear boundary between the quantum forwarding plane and the rest would allow to discern which parts are new and which ones can be essentially taken from networking or service-oriented technologies.

In the rest of this section, we will consider the concrete case of a QKD network, as the most mature example we have. In QKD networks, the final product are the symmetric secret keys, hence the QKD protocols (from the production of the quantum states to classical post processing) belong to the QFP. The QFP concept can be equally applied to networks dedicated to entanglement distribution or the trivial network (one single node) of a QNRG. The QFP supports the consumption of its products following the *as-a-service* paradigm, what implies a natural convergence with current trends in cloud, and distributed in general, computing.

In a QKD network, the processing of quantum states results in symmetric keys that are tagged and stored in the local memory of the module, awaiting to be delivered. This defines the *QKD module*, which is able to create a key between the two ends of the quantum channel. One or several of these modules interact with a *Key Forwarding module*, able to relay the keys from one node to the next in a chain of nodes. The next component is the *QKD Control module*, whose functionality is to control the QKD modules and their connections. In addition, since the maximum distance in a single link is heavily penalized because of the limitations in the physical medium, the network has to be capable of doing multi-hop links, where the key is relayed from one node to the next in a chain of nodes. To do this, part of the key is consumed and this key is not available for the final application. This task is just key transport done on behalf of the network and is carried out, when needed by a *Trusted Repeater module,* which can be also used to build interoperability in the network among QKD module manufacturers at the link level.



Quantum “segment”
of the node, part of the
Quantum Forwarding
Plane (QFP)

Figure 5: Schematics of a QKD node in a Quantum network. The components in the QFD do not have an equivalent in a classical network. The rest of the components can be built based on current networking technologies

Note that we do not consider that the application issues its requirements directly to the control (e.g. demanding a given flow of key between two specific nodes in the network with certain characteristics), but they go through the *Key Manager*, which is the last component. If the Key Manager cannot satisfy the requirements, it will ask for the connections to be created by the network control. This design means that there is a unique entry point of the application in the QKD node, which facilitates both the implementation of the applications and the collection of all the requests so that the key management can decide on the priorities and preemptively ask for the creation of keys among nodes.

While QKD Control can be specific for each device (Forwarding) manufacturers, their control communications with the Key Managers and among nodes should be standardized. In the case of a centralized control, specifically in the Software Defined Networking (SDN) case, this would impy the standardization of the South Bound Interface from the SDN controller to a node controller (SDN Agent). This component-based approach also satisfies the design rule of implementing clearly distinct and non-overlapping functionalities. The functionalities that are above the quantum forwarding plane, are essentially classical functionalities that can be considered extensions of components that are already in the market. For example, and continuing with the QKD example, there are manufacturers of key management systems that would just need to add some specialized modules to their products to deal with the continuous supply of symmetric keys produced in a QKD network. In the same way, existing SDN controllers can be extended with modules to deal with the control needs of a QKD network.

6.1 Quantum Security “as a Service”

Security awareness last years created market for safe communication transport, that QKD is one of the answers, maybe the most promising one, but the technology itself to this day is too expensive (and still very much in development phase) for individual implementation. In addition to business customers coming from health, banking industries and even from the governance, the operators themselves are potential consumers of QKD offer.

The confidentiality promised by QKD make it potential answer to securing 5G connectivity between base stations, MEC and 5G core. This gives the field to network operators to integrate QaaS (QKD or Quantum-as-a-Service in their portfolio.

In QaaS concept every user can apply for the QKD service (SKR) from the same provider network. However, assuring efficient, flexible and high manageable service requires introduction of SDN to the technical implementation to overcome challenges coming from multiuser environment (SDN for QaaS). In such case SDN for QaaS framework should follow standards proposals, with infrastructure, control and services abstract layers defined.

Centralized SDN controller can manage both classical and quantum infrastructure with knowledge of network architecture, infrastructure layer parameters, optimizing classical/quantum network taking under consideration requirements to establish quantum channels.

The southbound (to infrastructure) and northbound (to services/applications) interfaces provide communication with control plane (QKD 004 and QKD 015 ETSI standards)

The security mechanisms are applied to management plane itself to handle communication between NFV platforms, between SDN controller and infrastructure layer, etc. (SSL/SSH connections with QKD keys)

6.2 Quantum Random Number Generators as a Service

QRNG-as-a-service is a potentially attractive service for a suite of quantum cloud service offerings because it can be made available immediately and has a potential market with users who are looking for quantum-safe cybersecurity services [evQ2021].

Quantum Random Number Generators (QRNGs) are already offered by numer of companies in application not only for cryptograpy but for simulators, often linked to sampling tasks.

Various practical QRNG schemes have been developed, with practical implementations like single photon splitting by a beam splitter, homodyne detection of the vacuum field noise, phase diffusion in lasers, amplified spontaneous emission (ASE) noise, and the intensity fluctuation of spontaneous emission from light emitting diodes (LEDs) or atoms. See first IG group White Paper for more detailed development [GSMA2021].

There are already propositions of Quantum Random Number Generators as a Service:

- QRNG beacon service from NIST (USA);
- Telefonica partnership with Quside (spin-off from ICFO, Spain) and Qcrypt (USA) companies [reference];
- Alibaba and University of Tokyo [nature].

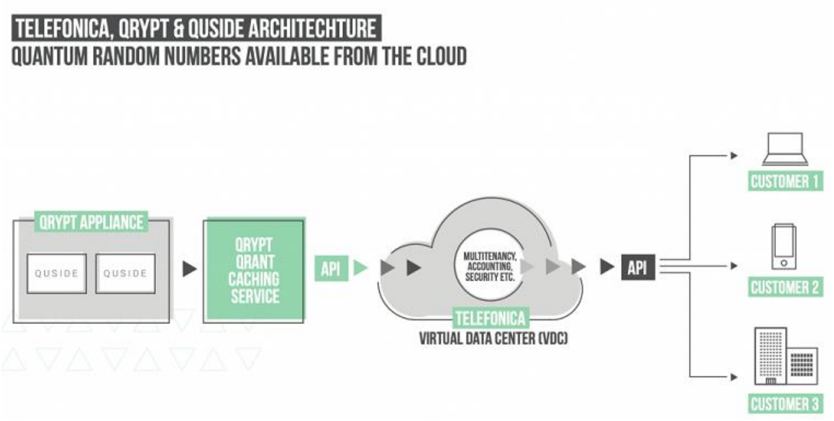

TELEFONICA, QRYPT & QUSIDE ARCHITECHTURE
QUANTUM RANDOM NUMBERS AVAILABLE FROM THE CLOUD
QRYPT APPLIANCE
QUSIDE
QUSIDE
QRYPT QRANT CACHING SERVICE
API
MULTITENANCY, ACCOUNTING, SECURITY ETC.
TELEFONICA
VIRTUAL DATA CENTER (VDC)
API
CUSTOMER 1
CUSTOMER 2
CUSTOMER 3

Figure 6 – Example of QRNG as a Service [ref]

This paper [nature] describes the integration of four different types of quantum random number generators on the Alibaba Cloud servers to enhance cybersecurity. Post-processing modules are integrated into the quantum platform to extract true random numbers. Improved authentication protocols are provided where original pseudo-random numbers are replaced with quantum ones. Users from the Alibaba Cloud, such as Ant Financial and Smart Access Gateway, request random numbers from the quantum platform for various cryptographic tasks. For cloud services demanding the highest security, such as Alipay at Ant Financial, they have combined the random numbers from four quantum devices by XOR the outputs to enhance practical security.

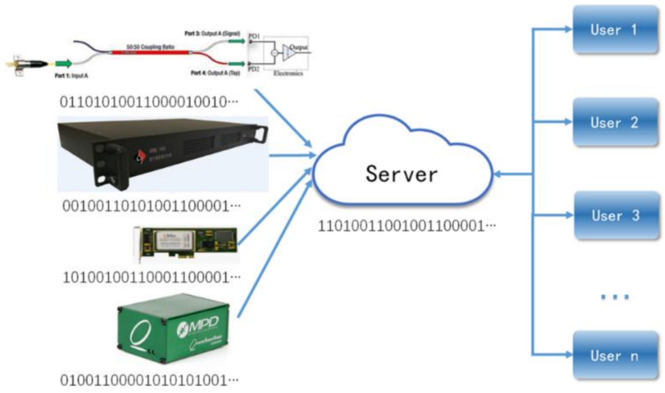


Figure 7 – Schematic Diagram of the QRNG Cloud Platform [Huang2021]

Another application example is virtual private networks (VPNs). The QRNG platform is a practical step of implementations toward the full-process quantum-safe solutions in cloud services. The communication between SAGs and Alibaba Gateways can apply quantum-safe VPNs, whose architecture diagram is shown in the following figure.

The QRNG service is worldwide, provided to ten different places at Shanghai, Japan, Hongkong, Singapore, Malaysia, Indonesia, Australia, United Kingdom, Germany, US East, US West, as shown in the following figure.

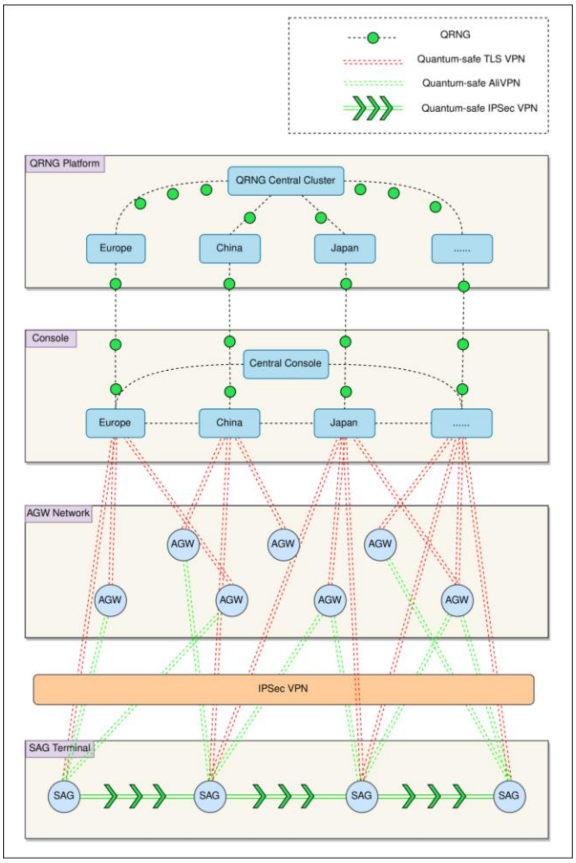


Figure 8: QRNG in quantum-safe VPNs [Huang2021]

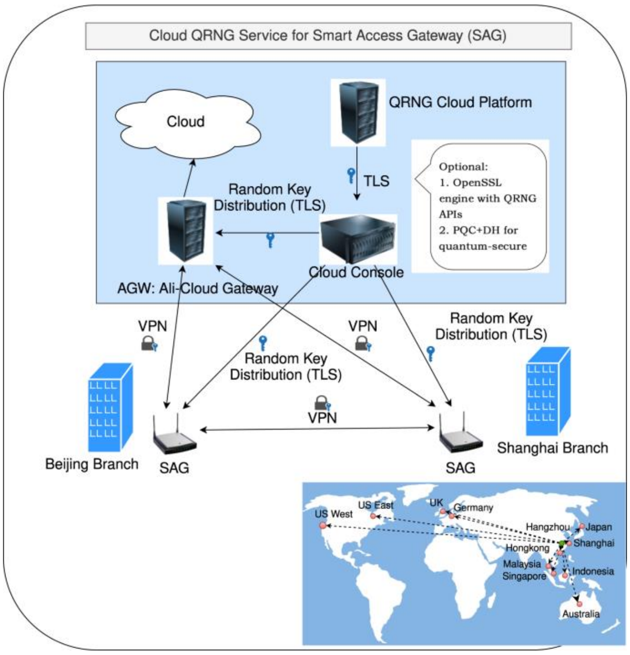


Figure 9: Smart Access Gateway QRNG Cloud Implementation [Huang2021]

Other approach based on untrusted devices have been developed that can resist stronger attacks in theory like device-independent (DI) schemes that require the violation of a Bell inequality or semi-DI (or self-testing) approaches that require some weaker assumptions to bound the side information. Such assumptions can be related to the dimension of the underlying Hilbert space, the measurement device or the source, for example the mean photon number or the maximum overlap of the emitted states.

It is possible to use quantum processors to create new services not limited to specific calculus processing, but also to get benefit from non deterministic nature of quantum process. Today, generating high-quality random numbers based on quantum technologies represents an excellent application of noisy and intermediate scale quantum (NISQ) QPUs. For example [QRNG,AWS] describes described an implementation of a quantum random number generator in Amazon Braket with the use of quantum processors (QIP). These NISQ QPUs are quantum computers that can be programmed to run arbitrary circuits up to a certain depth and qubit limit due to the inherent noise in the device.

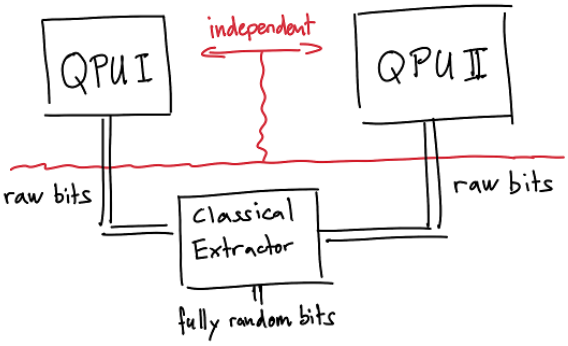


Figure 10: Using two NISQ QPUs and classical post-processing to generate randomness [QRNG,AWS]

6.2.1 Security in transit and in storage

The most common scenario to assure no unauthorized access to keys during manufacturing and distribution chain is to instal certificates on device and having public key infrastructure.

Such certificate is used to sign communication and authenticate device itself while confidentiality and integrity of communication is guaranted by E2E TLS protocol based communication. The symmetric keys are simpler in that aspect as they do not require managing public kay infrastructure. By using QKD to obtain keys we eliminate weak point which is pre distribution. Using quantum channels allows practical implementation of OTP (one-time-pad) technique as keys, real random, can be generated simultaneously on both ends of communication channel.

6.3 Quantum Computing-as-a-Service

Quantum computers can solve certain specific problems, such as factoring integers, and discrete logarithm problem, dramatically faster than we know how to solve them with today’s computers.

Quantum Computing-as-a-Service (QCaaS) can be seen as an evolution of Cloud Computing services: instead of purchasing physical quantum computers, which may be hard to maintain and operate, QCaaS customers may access quantum computers in the cloud.

The global QCaaS market is expected to reach $4 billion by 2025 and $26 billion by 2030 according to research done by The Quantum Insider team, a subsidiary of The Quantum Daily [QCaaS]. The figures represent an ~80% CAGR 2021-2030.

The set of computational problems efficiently solved by a quantum computer is BQP (Bounded-error Quantum Poly-Time) and includes problems for which a classical efficient algorithm is unknown. BQP ia a class of problems that can be solved by a quantum computer using a polynomial amount of time in the input size, with an error probability of at most 1/3 (figure 11).

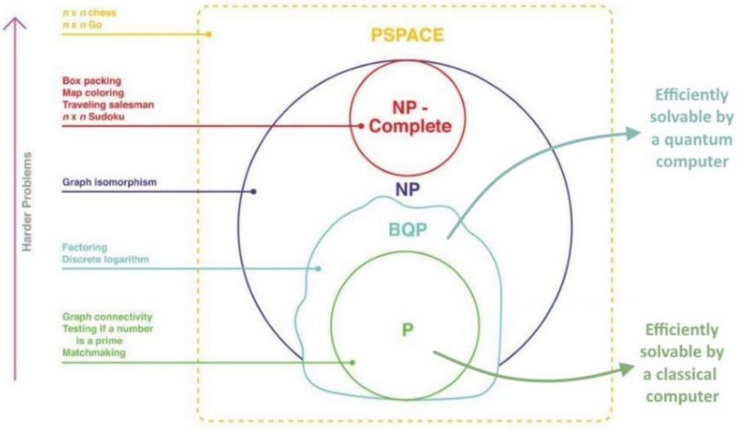
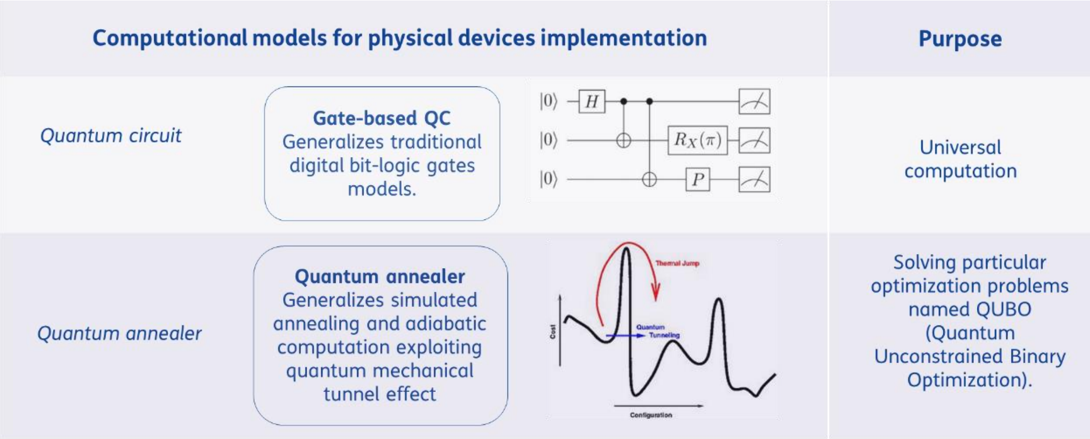


Figure 11 – Computational complexity – adapted from images by MIT OpenCourseWare, Scientific American

Quantum computing technology is at its early stages. The lack of a proper error correction theory is the main obstacle to the possible realization of a full-purpose quantum computer: the noise in quantum gates in nowadays quantum devices relies on theoretical immaturity more than on engineering. Still, the quantum devices available today, mainly through the cloud, can be employed as support of classical processor in solving instances of hard computational problem. Those devices have been dubbed by the theoretical physicist John Preskill Noisy-Intermediate-Scale-Quantum (NISQ) [Preskill2018].

NISQ-devices are bases on two computational models: quantum gate based model and quantum annealer.

Figure 12 – Quantum computational models for physical device implementation.



Computational models for physical devices implementation			Purpose
Quantum circuit	**Gate-based QC** Generalizes traditional digital bit-logic gates models.		Universal computation
Quantum annealer	**Quantum annealer** Generalizes simulated annealing and adiabatic computation exploiting quantum mechanical tunnel effect		Solving particular optimization problems named QUBO (Quantum Unconstrained Binary Optimization).

Potential applications of Quantum Computing-as-a-Service (QCaaS) exploting NISQ devices includes solving some subroutines of classical hard problems, mainly in the machine learning field, possibly providing a quadratic or even exponential speedup.

Potential candidates are problems that exploit one of the following sub problems:

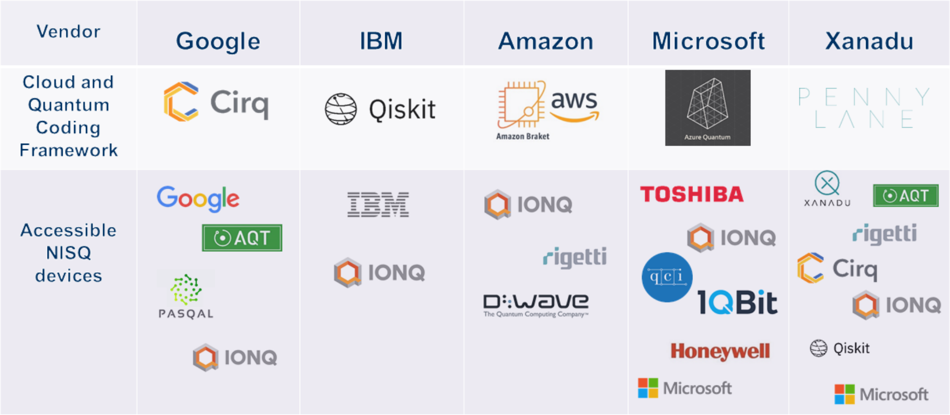
- Matrix inversion – HHL algorithm [Aram2008] (data fitting [Natham2012], quantum least square linear regression [Guoming2017], least square version of support version machine [Bojia2017])
- Unstructured search – Groover algorithm [Grover1996] and quantum walk [Childs2003];
- Finding local minima – Quantum annealing [Farhi2001];
- Sampling – exploiting quantum annealing (training Boltzmann machines [Dixit2021])

Nowadays, the most popular problems implemented on NISQ devices are optimization problems that can be mapped into:

- Quantum Approximate Optimization Algorithm (QAOA) [Farhi2018];
- Variational Quantum Algorithm (VQA) [Moll2018].

Cloud quantum computing provides direct access to available NISQ-devices and Quantum Annealers, but also to classical emulators, simulators.

Figure 13 shows some example of development platforms and documentation for quantum computing languages and tools.



Vendor	Google	IBM	Amazon	Microsoft	Xanadu
Cloud and Quantum Coding Framework	Cirq	Qiskit	aws Amazon Braket	Azure Quantum	PENNY LANE
Accessible NISQ devices	Google AQT PASQAL IONQ	IBM IONQ	IONQ rigetti D:Wave The Quantum Computing Company	TOSHIBA IONQ qci 1QBit Honeywell Microsoft	XANADU AQT rigetti Cirq IONQ Qiskit Microsoft

Figure 13 – Examples of development platforms and documentation for quantum computing languages and tools.

6.4 SLA, Sustainability and Business Impacts

Quantum as a Service will have implications to Network Management and SLAs in business-to-business constructs. Inherent quantum security and privacy must be retained. A beginning point may be the assessment of quantum resistant cryptographic primitives, multiparty computation and zero knowledge proofs. The balance between performance agreement and latency is inherent in this discussion. Transactions and communications over a quantum network will occur in microseconds, however, remain to pose concerns for long distance communication due to loss and repeater privacy. Long distance communications will occur over single path fibre cables and satellite communications. This allows for communication blocking/interference by bad actors and generates a need for space policing and concerns for space debris. With the average life expectancy of a Lower Earth Orbit satellite at 5 years and a Geosynchronous Equatorial Orbit satellite at 12 - 20 years, which may be the preferred satellite variant for quantum networks due to the stationary nature and need for constant communication, there remains a concern for sustainability [Mohamed2015)]. This further encourages innovation in battery and solar technologies to increase the life expectancy of a single quantum pathway through reduced rate of decay and waste. One could assume therefore that a “green” approach to Quantum Networking is a requirement and certainly core to sustainability.

To improve transaction times, communication splitting must occur by sending out a single, circular distributed message through message segmentation and routing that is split at decision points as a part of a tree [Hahn 2019]. However, due to the multistate nature of quantum, multi-partite complementation will be needed to increase both data resiliency over the network and differential stability [Iranzo2012].

Appropriately, Service Level Agreements will likely require intermediation due to multi-partite complementation and/or internodal failover due to memoryless processing. Thus, increasing the value of data clearing houses and aggregators [Hahn, 2019].

Due to the initial high-cost nature of Quantum Networks and Services, a shared ownership or leasing model will be required to allow for the greatest operational depreciation and return on investment for QNS Owner/Operators. Further, smart contract implementation through Distributed Ledger Technologies will prove to be useful in managing use and billing across the global framework needed for full implementation. Such technologies will allow for near real-time transaction completions and minimize the perpetuity of daily, hourly, or minute based reconciliations.

Globally, there will be early adopters and a late majority as with any new technology. In this instance, concerns will lag around cost, failover risk, organizational risk posture, trust, security, and workforce education. Further, concerns will arise in the late majority and laggards around the inability or limited potential for communication content logs resulting from memoryless processing. Therefore, solutions will need to be developed to resolve the concerns of this group. Such solutions might include primary and secondary messaging protocols as a message validation process to minimize risk/concerns rather than a communication content log. Else, establishment of transaction logs written to a DLT [Krishnaswamy 2020]

7 Examples of demonstrators: MadQCI

MadQCI (Madrid Quantum Communications Infrastructure) is a quantum networking testbed deployed within the Madrid metropolitan area, with two components: a ring of about 28 km installed on the Telefoonica Spain production network, and the other part of the Madrid Research Network (REDIMadrid). Network and node designs follow the abstraction based on QFT and the SDN paradigm

The first segment is especially well suited testing high Technological Readiness Level (TRL) services and devices, given the systems installed must follow the standard procedures for telco equipment and comply with operator constraints. The other segment of MadQCI s part of the Madrid Research Network. The PoPs in this network are more open to experimentation and are adequate for lower TRLs, and optical paths can be dynamically modified. The network is connected with the Spanish National Research and Education Network (NREN) RedIRIS point of presence, and from there it is connected to the European academic network GÉANT.

MadQCI is also unique in that is comprised of two independent network service providers, Telefónica and REDIMadrid. This is the first example of a multitenant quantum network. This shared tenancy enables to connect nodes which are further apart in the metropolitan area and test the design of *quantum border nodes*. The full network is currently designed with thirteen links and eleven PoPs, all of them at research and production facilities, and many share the optical fibre simultaneously for classical and quantum communications. MadQCI is currently running two demonstrators of special relevance for this document.

The first demonstrator considers the application of QKD for B2B and 5G networks in edge scenarios, addressing the need for an enhanced layer for securing the transport segment, traditionally seen as a "black box" from the end-user perspective.

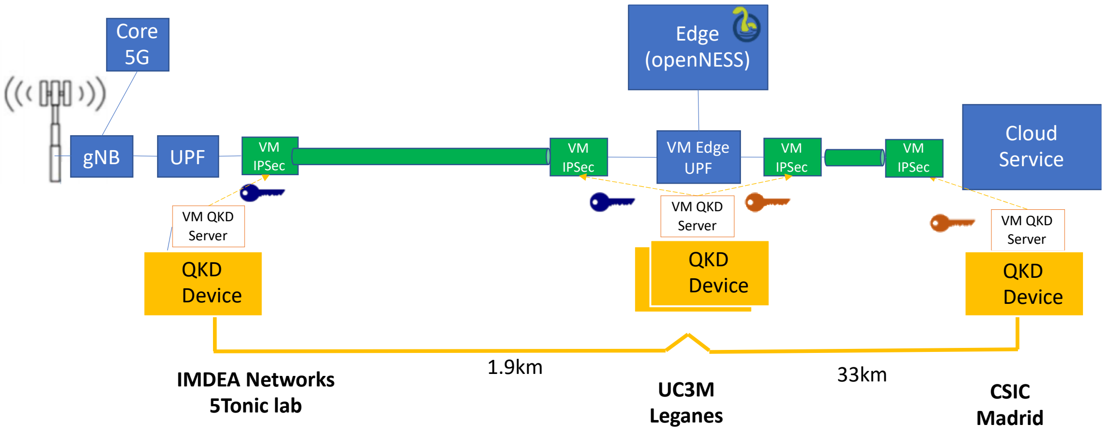


Figure 14: Applying QKD to 5G edge scenarios at MadQCI

This demonstrator is intended to evaluate the role of QKD for enhancing mobile network and edge security, since traditional transport services (e.g., virtual private networks-VPNs, label switched paths-LSPs or tunnels) can additionally integrate QKD for securing end-to-end communications. This will eventually allow services on top of the transport network, such as VPNs for business to business (B2B) or connectivity from radio base stations to core or data centre premises (e.g., for 5G), to incorporate quantum-safe security for end-user communications.

The second demonstrator considers the integration of QKD in private and permissioned *Distributed Ledger* (DL, or *blockchain* to employ the commonly used term) networks, evaluating how to significantly the security and performance of private transactions.

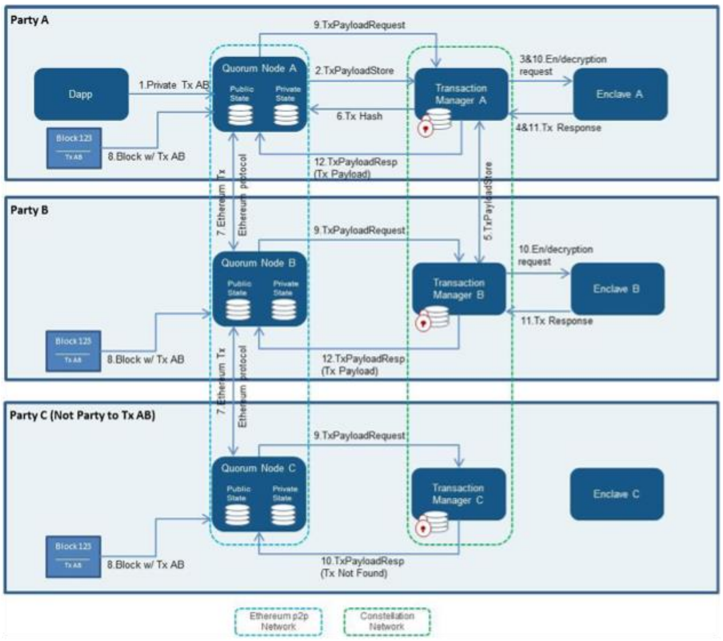


Figure 15: Applying QKD to DL private transactions at MadQCI

Current DL platforms support the use of private transactions between different nodes in the network. To support this, they rely on external systems to encrypt the private transactions payload using a set of asymmetric keys previously shared off chain between the involved entities, adding a level of complexity in terms of operation and management of the DL nodes. The use of QKD can remove the need of these systems to perform private transactions enabling a secure exchange of symmetric keys between the different entities that want to perform private transactions. The demonstrator explores as well the required interfaces for controlling QKD key management and the use of QNRG-as-a-service at the different DL nodes.

QKD can also be used to permission sub-networks within a larger DLT network. Instead of using the standard permissioning system of the underlying platform, a set of QKD keys could be shared between all the nodes of the network that want to share a dedicated communication channel for the exchange of transaction within the network.

8 Conclusions

Quantum technologies are progressing fast. Even if significant developments are still needed, in light of the potential opportunities generated by the expected industrial impacts of quantum technologies, several investments are made worldwide across the public and private organizations.

Feasibility demonstrations and performance testing are very important and required: this thread could be facilitated by the development of platforms where innovators (e.g., research institutions, software developers, hardware industry, internet service industry, security professionals) meet together to share open innovation capable of boosting the creation and development of new ecosystems on quantum.

Coordinated standardization efforts are required: for example, the topics concerning the integration of quantum nodes and systems in current infrastructures are still limitedly covered by the standardization activities. Integration and interoperability aspects are fundamental to plan the exploitation of such disruptive technologies and services.

For example the physical layer of hybrid classical/QKD systems remains unaddressed. What system parameters should be monitored and how this information should be processed to infer the impact on the system performance is also an important matter of standardization.

Moreover, the current lack of commercial or open source modelling tools for the simulation of classical/QKD systems does not help in this aspect and it is an obstacle that should be removed. These tools would indeed allow to validate any specification using an agreed simulation framework and without making use of expensive experimental setups.

Another main challenge might be the development of human resources with appropriate skill: the know-how should involve understanding telecommunications, computer science as well as engineering of quantum systems.

8.1 Examples of standardization gaps

8.1.1 QKD

As previously reported in ITU and ETSI there are ongoing activites for the standardization of QKD.

Figure 16 shows a general configuration example of QKD use for securing a P-to-P application link where the areas for standardization can be identified: from physical interfaces, to interfaces between the QKD node and the Encryptors to interfaces for management and control.

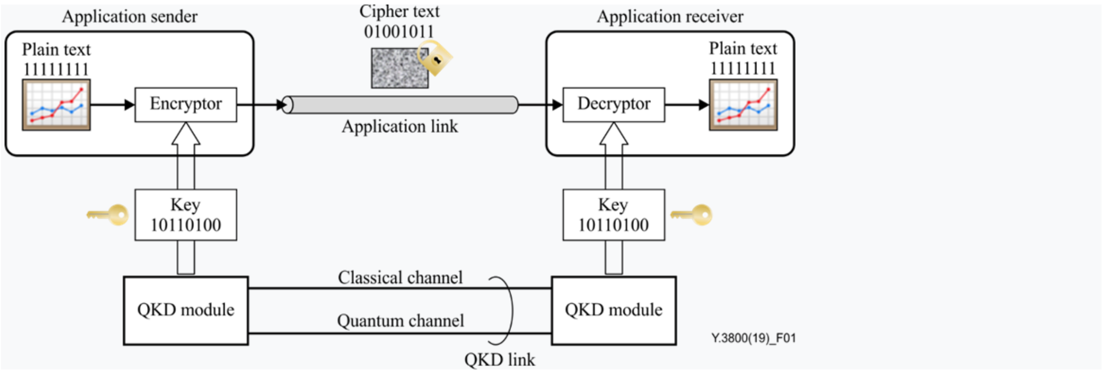


Figure 16 – Configuration example of QKD use for securing a P-to-P application link [source: ITU Y.3800]

In general, there are still several gaps which have to be considered:

- the level or ASE noise from optical amplifiers, or of in band crosstalk from classical channels, that can be tolerated by quantum channel receiver
- the maximum transmission power that should be allowed to a classical channel not to interfere with a QKD channel.
- attenuation/reflection characteristics of all components and sub-systems in a quantum node/system
- interfaces of all of all components and sub-systems in a quantum node/system
- interfaces for interoperability and interworking of quantum nodes/systems within current networks
- interfaces for management, control and orchestration
- assurance (policies and processes to ensure that services offered over networks meet a pre-defined service quality level for an optimal subscriber experience.)
- others ?

8.1.2 Quantum Computing

Two main paradigms have been identified in nowadays quantum computing technologies landscape: noise exploitation and noise control.

- the first, consider entropy as a resource: a perfect QRNG would avoid environmental interaction for not to introduce undesired patterns in the noise source, employed in simulations accuracy – classical and quantum – gaussian prior generation – for machine learning tasks. In the end of the day, randomness has also been the key property of quantum systems for proving the computational supremacy of NISQ devices
- the second, considers the noise a quantum state is subject to as an obstacle: lack of an efficient error correcting code for example is one of the mais issue toward the realization of a full purpose quantum computer, whose main requirement is the ability of perfectly control quantum state and processes. The fact seems to suggest that quantum-noise-tuning will be the key achievement toward the second quantum revolution.

A common understanding on the need of standardization in this domain is not yet emerging. In fact, due to readiness-level of quantum technologies, many consider the early standardisation a possible impediment: it would design a privileged path for the proof of concept, at the cost of other possible unexplored directions. Others retain standardisation a possible speed-up toward first effective feasibility demonstrations.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
v1.0	17 December	New PRD Publication Acknowledgements: Agnieszka Zalesinska-Stepniak (Orange) Serena Di Giorgio (TIM), Antonio Manzalini (TIM), Daejoon Cha (SKT), Diego Lopez (Telefonica), Dong-Hi Sim (SKT), Fabio Cavaliere (Ericsson) Jacques Mouton (Syniverse), Monique Morrow (Syniverse), Olivier Le Moult (Orange),	IG	Antonio Manzalini (TIM)

Other Information

Type	Description
Document Owner	Yolanda Sanz / GSMA
Editor / Company	Antonio Manzalini / Telecom Italia

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom
www.gsma.com