From Existing Quantum Key Distribution Systems towards Future Quantum Networks

Ludovic Noirie

From Existing Quantum Key Distribution Systems towards Future Quantum Networks

Ludovic Noirie
Bell Labs
Nokia
Massy, France
ludovic.noirie@nokia-bell-labs.com

***Abstract*—With the current development of quantum computing, some existing cryptographic protocols may be broken in the future, such as RSA with Shor's algorithm. To secure the future secret communications, but also the current ones from retrospective decryption, Pre-Shared Keys (PSK) can be used today, and two types of complementary solutions are currently being studied: Post Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). The objective of this paper is to describe the latest, which relies on the laws of quantum physics to secure the sharing of secret keys. Among the current QKD systems, some are already commercially available. Their distance range is limited, generally around 100 km. To overcome this distance limitation, a first solution is currently being deployed in field trials using trusted nodes, forming the so-called Quantum Communication Infrastructure (QCI). The drawback is that users must trust QCI nodes, in which quantum communication are stopped, going back to classical data processing that can be eavesdropped. To overcome this problem, researchers are investigating solutions to build future quantum networks and Quantum Internet (QI), in which the processing in the networks remains quantum, using quantum buffers and entanglement swapping in *quantum repeaters* to increase the distance range of QKD. We briefly discuss the advantages and disadvantages of QKD versus PQC, with the two actually being complementary.**

***Index Terms*—quantum key distribution, quantum communications, quantum communication infrastructure, quantum networks, quantum internet, post-quantum cryptography**

I. Introduction

People searched for means of communicating secrete information since classical antiquity, a well known example being Caesar's cipher. The first unbreakable code is the *Vernam cipher*, developed in 1917 by Gilbert Vernam and Joseph Mauborgne, and also known as the *one-time pad* [1, p. 50]. The binary version of this code uses a shared secret key between the sender and the receiver to encrypt message with a bit-by-bit XOR, without reusing any part of the key. Claude Shannon proved its inviolability using his information theory [2]. The problem is that one-time pad requires a one-use-only shared secret key of the length of the message to be encrypted.

In modern telecommunication networks such as Internet, other cryptographic techniques are currently used, using secrete keys that are shorter than the message to be encrypted. They rely on the assumption that they are hard to decrypt. A well known example is RSA, which relies on the difficulty to factorize integers into prime factors, the best known classical algorithms for this task being non-polynomial.

But Shor invented in 1991 a quantum algorithm [3] that can factorize integers very efficiently. This algorithm relies on quantum phenomena such as quantum superposition and quantum entanglement, which allows for a kind of *quantum parallelization* of computation. We do not yet have quantum computers that are able to correctly process Shor's algorithm for large numbers. But the current development of quantum computers is a threat for RSA-based security systems.

For this reason, a lot of effort has been put in research for new cryptography methods that are resistant to quantum computers, to have *quantum-safe* communications. A first class of solutions under studies is Post-Quantum-Cryptography (PQC). They still rely on using secrete keys that are shorter than the message to be encrypted, and they rely on the assumption that it is difficult to break them, but they are supposed to be not breakable by quantum computers [4]. In North America, the National Institute of Standards and Technology (NIST) initiated a competition to develop such PQC solutions [5]. In the test phase of this computation, some of the proposed solutions were broken. The selected ones have not yet been broken, but who knows if they will not in the future?

A second class of solutions under studies is Quantum Key Distribution (QKD). QKD creates a shared secret key between two remote entities. Its security relies on the laws of quantum physics [1]. Bennett and Brassard invented BB84, the first QKD protocol in 1984 [6]. Since them, other QKD protocols have been designed [7]–[11], the ETSI QKD Industry Standardization Group [12] is standardizing QKD, and companies such as ID Quantique [13] are selling QKD-capable products. In Europe, several Quantum Communication Infrastructure (QCI) field trials [14] have been set up to extend the distance range of QKD, using trusted nodes. Looking forward, QKD is an important application of future quantum networks [15]–[17].

In this paper, we give a survey of existing QKD systems, which are limited to short distances (typically $\sim$100 km by fiber and $\sim$1000 km by satellites), and we show how such systems can be extended on longer distances, first using trusted nodes in QCI, then in trustless QI. We also position QKD and its extensions with QCI and QI vs. PQC, considering the advantages and disadvantages of each class of solutions.

The remainder of this paper is structured as follows. Section II describes some QKD protocols. Then, Section III explains

how the distance range of the current QKD systems can be extended using trusted nodes in a QCI, and Section IV explains how the future QI remove the need of trusted node, providing a fully trustless quantum networking solution to extend the QKD distance range. Finally, Section V discusses the positioning of QKD vs. PQC and Section VI concludes.

II. Quantum Key Distribution Systems

In this section, we introduce QKD systems with their generic functions. QKD may use Discrete Variables (DV-QKD) that generally are qubits, i.e., quantum objects modeled in an Hilbert space of dimension 2, like for BB84, BBM92 and E91 protocols, or Continuous Variables (CV-QKD) using quantum objects modeled in an Hilbert space of infinite dimension, like for GG02.

A. QKD generic functions

The objective of QKD is to create a shared secret key between two entities, Alice and Bob, that could be used later for message encryption. QKD systems use a quantum channel to exchange quantum information (qubits, or more generally quantum states), and a classical channel to exchange classical information (bits) that may or may not be classically encrypted, but must be authenticated. There may be a potential third entity, Eve, that wishes to intercept this key by eavesdropping on the quantum and/or classical channels between Alice and Bob. QKD can be decomposed in the following functions [12], [18], [19]:

1) *Raw key generation*: Alice and Bob use the quantum channel to generate a sequence of random bits (*raw keys*), an identifiable fraction of which are theoretically equal (see the error estimation phase below);
2) *Sifting*: Alice and Bob exchange information on the classical channel to identify the bits that are theoretically equal, without revealing any information about their values. These bits are referred to as the *sifted keys*;
3) *Error estimation*: Alice and Bob consume part of their sifted keys to estimate the error ratio between the sifted keys. Errors can result from quantum channel imperfections and/or Eve's eavesdropping, and Alice and Bob abort the QKD process if the error ratio is too high, indicating the potential presence of an eavesdropper;
4) *Error correction*: Alice and Bob apply an error correction code to their remaining sifted keys, ensuring they now share an identical, albeit smaller, sequence of bits;
5) *Privacy amplification*: Even with a low error ratio, Eve may have intercepted a fraction of the sifted keys, but Alice and Bob can sacrifice some more bits to decrease the amount of information available to Eve;
6) *Authentication*: Alice and Bob verify the authenticity of the messages they exchanged on the classical channel, which were signed using a pre-shared secret key smaller than the one created by the QKD protocol;
7) *Protocol ends*: The remainder of the sifted keys form a new secret key shared by Alice and Bob.

About the authentication function: Usually, the classical channel is classically authenticated [1], [12], [13], using for example Wegman–Carter authentication [16, table 1], [18], which consists in signing the message using a pre-shared secret key using cryptographic hash functions. Wand *et al.* [20] proposed to use post-quantum cryptography (PQC) to authenticate the classical channel. Noirie and Varloot [19] proposed a solution for BB84 and BBM92 QKD protocols that uses quantum error estimation to authenticate both quantum and classical channels with the consumption of a smaller preshared key, which is provably secure thanks to fundamental results in both information theory and quantum physics.

B. Prepare and measure DV-QKD: BB84

A prepare-and-mesure QKD protocol is a DV-QKD protocol in which a sender, Alice, prepares a qubit in a random state, and sends it to a receiver, Bob, who measures it according to randomly chosen axes of measurement.

A qubit is a quantum systems that can be represented by a vector in a Hilbert space of dimension 2, up to a normalization factor (usually taken to 1) and a phase factor. It can be measured according to any orthonormal basis in the Hilbert space (an axis in the Bloch sphere representation): if the basis is $(|0\rangle, |1\rangle)$ and $|\psi\rangle = a|0\rangle + b|1\rangle$ (superposition principle) with $|a|^2 + |b|^2 = 1$, then the probability to measure 0 is $|a|^2$ and the probability to measure 1 is $|b|^2$ (Born rule). A qubit can be encoded for example by the polarization of a photon (0 and 1 corresponding to vertical and horizontal polarization), but there are other ways to encode a qubit in a photon (e.g., time-bin encoding), the modeling of the qubit remaining invariant: a vector in a Hilbert space of dimension 2.

BB84 is the original prepare-and-mesure QKD protocol, invented by Bennett and Brassard in 1984 [6]. BB84 steps are the following, the quantum preparation, transmission and measurement being represented in Figure 1:

1) Alice prepares a qubit $|\psi\rangle$ in a state she randomly chooses in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$[1] and sends it to Bob, $|\psi\rangle$ corresponding to bits (m_A, b_A) with the mapping $(|0\rangle, |1\rangle, |+\rangle, |-\rangle) \mapsto ((0,0), (0,1), (1,0), (1,1))$.
2) Bob measures the qubit he receives according to an axis in the Bloch sphere randomly chosen in $\{Z, X\}$, giving bits (m_B, b_B) with the mapping $((Z, |0\rangle), (Z, |1\rangle), (X, |+\rangle), (X, |-\rangle)) \mapsto (|0,0\rangle, |0,1\rangle, |1,0\rangle, |1,1\rangle)$.
3) Born rule gives:
   - $m_A = m_B \Rightarrow 100\% : b_A = b_B$;
   - $m_A \neq m_B \Rightarrow 50\% : b_A = b_B$, $50\% : b_A \neq b_B$.
4) After Bob's measurements, Alice and Bob communicate through an authenticated classical channel:

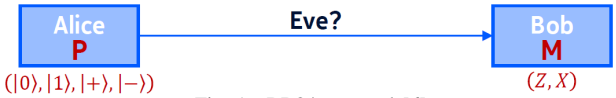

Fig. 1. BB84 protocol [6].

[1]Where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ are superposed states, corresponding to diagonal and anti-diagonal polarizations with polarization encoding.

- Alice and Bob exchange the values of m_A, m_B and discard the cases where $m_A \neq m_B$;
- Then, they exchange a sample of the remaining (b_A, b_B) bits to statistically detect eavesdropping;
- If Eve is not detected, they use the other remaining (b_A, b_B) bits to build their shared secrete key.

The security of BB84 is ensured by the complementarity principle of quantum measurements: an eavesdropper Eve cannot measure a property of a quantum system without destroying the information about a complementarity property, the complementary properties being here the value of the qubit on Z or X axes. If she intercepts and measures the qubit during its transmission, when $m_A = m_B$, and if she chooses the axis $m_E \neq m_B$ (the values of m_A and m_B are unknown by Eve), then the probability that $b_A \neq b_B$ is 50% instead of 0%. Thus, the intervention of Eve in the quantum channel is probabilistically detectable. Note that Eve cannot make a copy of the qubit, because of the no-cloning theorem [21].

BB84 can be implemented in the Quirk simulator[2], see https://ludovic-noirie.fr/QC/QKD/BB84.htm.

C. Entanglement-based DV-QKD: BBM92 and E91

An entanglement-based QKD is a DV-QKD protocol in which a pair of qubits in a Bell state is produced either by Alice, Bob or a third party, Alice and Bob receiving each one qubit of the pair and measuring it.

BBM 92 is such a protocol, invented by Bennett, Brassard and Mermin in 1992 [7]. BBM92 steps are the following, the Bell state creation, the transmission of the qubits and their measurement being represented in Figure 2:

1) Alice and Bob share a pair of qubits in Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)$.
2) Alice measures her qubit according to an axis randomly chosen in $\{Z, X\}$ like Bob in step 2 of BB84, giving bits (m_A, b_A).
3) Bob measures his qubit according to an axis randomly chosen in $\{Z, X\}$, like in step 2 of BB84, giving bits (m_B, b_B).
4) The Born rule outcome and the communications between Alice and Bob are exactly the same as BB84, see Subsection II-B.

Fig. 2. BBM92 protocol [7].

The creation of the shared key in BBM92 relies on the properties of the Bell state. The BBM92 security is ensured like for BB84.

BBM92 can be implemented in the Quirk simulator, see https://ludovic-noirie.fr/QC/QKD/BBM92.htm.

[2]Quirk, a drag-and-drop quantum circuit simulator by Craig Gidney, see https://algassert.com/quirk. See also a presentation and a usage of this tool by the Ludovic Noirie: https://ludovic-noirie.fr/html/sciences/quirk/, the Section 7.2 being on QKD.

E91 is another entanglement-based protocol, invented by Ekert in 1991 [8]. It works a bit like BBM92 but uses different measurement axes, with three possible choices $\{Z, Z+X, X\}$ for Alice and three possible choices $\{Z+X, Z, Z-X\}$ for Bob (see Figure 3). For the E91 protocol, the creation of the shared key as well as its security rely on the quantum properties of the Bell state. Like for BBM92, the shared key is created with the measured bits when Alice and Bob choose the same axes. But to detect eavesdropping, they use the measured bits when the chosen axes have an angle of $\pm 45°$ in the Bloch sphere representation, to check the Bell's inequality violation [22], [23]: the inequality violation decreases or even disappears according to the level of eavesdropping.

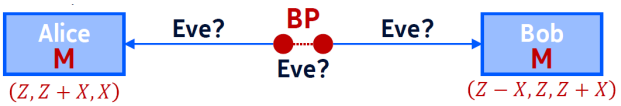

Fig. 3. E91 protocol [8].

E91 can be implemented in the Quirk simulator, see https://ludovic-noirie.fr/QC/QKD/E91kg.htm for the key generation and https://ludovic-noirie.fr/QC/QKD/E91bic.htm for the Bell's inequality checking.

D. CV-QKD

There is another kind of QKD that uses quantum states in a Hilbert space of infinite dimension (CV-QKD). We do not detail it in this paper. An example is the GG02 protocol invented by Grosshans and Grangier in 2022 [9].

E. Current QKD systems

QKD is a mature technology. Some products are commercially available, for example the Cerberis XG QKD System from ID Quantique [13], which works over typically ~ 60 km of fiber transmission for a final key creation rate of ~ 2 kbit/s. The maximum reach of such product using fiber transmission is of the order of ~ 100 km, because of the exponential loss of fibers: for 50 km, about 1 photon over 10 is received, while for 100 km, only about 1 photon over 100 is received.

Longer distances up to $\sim$1000 km can be achieved with free space optics, using satellites, like in the experiment of Liao *et al.* [24].

Telecom equipment suppliers are involved in field trials to test the compatibility of their transmission security products with QKD systems. For example, Nokia tested the compatibility of its 1830 Security Management Server (1830 SMS [25]) with the QKD solution from Proximus and the QKD systems from ID Quantique [26], see Figure 4.

The QKD systems created symmetric keys between two datacenters located in Brussels (Alice) and Mechelen (Bob) in Belgium, which were coordinated by the 1830 SMS to secure their optical communications. The trial with Proximus highlights how quantum cryptography can be implemented in a live commercial network. Adding an additional layer of security, Nokia's 1830 SMS, a quantum-safe key generator and orchestrator, provided classic quantum-safe encryption using pre-shared symmetric key distribution in instances where the stability of data using QKD were compromised or altered.

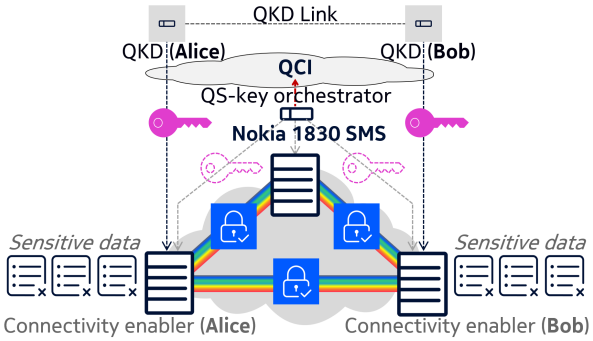

Fig. 4. Nokia Quantum-Safe Networking using Nokia 1830 SMS [25].

III. Quantum Communication Infrastructures

QKD is limited in distance, typ. ∼100 km over fiber. To get distribution of secrete keys over longer distance, researchers are deploying in field trials Quantum Communications Infrastructure (QCI) solutions that rely on trusted nodes (TN).

A. Trusted nodes

Figure 5 illustrates what is a QCI with end nodes (EN), trusted repeaters (degree 2 TN in circles) and trusted routers (degree 3^+ TN in squares).

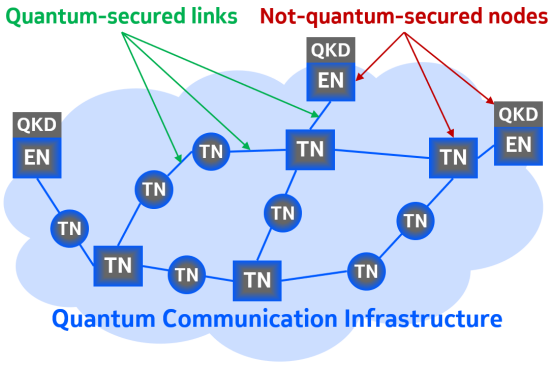

Fig. 5. QCI with quantum links and trusted nodes (TN).

Each link is quantum secure by a QKD systems. They are used to create secrete keys shared between adjacent nodes in a quantum-safe way.

In each trusted node, the quantum communication is ended and some classical processing is done. To create a secret key between Alice and Bob using an intermediate trusted node Charlie, Alice uses a QKD-created secret key k_{AC} with Charlie, Bob uses a QKD-created secret key k_{BC} with Charlie, Charlie processes them with a classical XOR operation $m_C = k_{AC} \oplus k_{BC}$ and sends m_C to Bob through a classical communication channel. Because the two keys are random secrets and only the XORed value is sent within the classical network, nobody outside Alice, Bob and Charlie can infer the values of k_{AC} or k_{BC}. Bob processes with a classical XOR $k_{AB} = k_{BC} \oplus m_C = k_{AC}$. Alice and Bob can then use the key $k_{AB} = k_{AC}$ as a secured shared key between them, provided they trust Charlie, because he shares the same information as them. The process can be repeated hop-by-hop to create a secrete shared key between any pair of nodes in the network.

B. QCI field trials

The European Commission launched in 2019 the EuroQCI initiative [14]. One of the objectives is to federate the QCI field trials in Europe, some of them having already produced some results, and link them either by fiber or by satellites.

C. QCI Limitations

Because each trusted node processes the QKD-created keys with classical processing, there is no physical limit for the distance for key creation between end nodes of the network.

The counterpart is that each node becomes a weak point for security. The end users must rely on the QCI provider for the security of the creation of the secrete key they share. It is not fully quantum secured, only the transmission between nodes is quantum secured. If the QCI provider is not reliable, an eavesdropper may be active inside a node of the network. But this can be mitigated in some use cases (e.g., military ones).

IV. The Future Quantum Internet

The solution to avoid to trust nodes in QCI is to have a full quantum network or Quantum Internet (QI), using quantum repeaters. In this section we describe how such quantum networks will work. The technological bottlenecks will be discussed in the next section.

A. The Quantum Internet

The QI Research Group at IRTF defined the "architectural principles for a QI" [17]. Figure 6 illustrates how the architecture of the future QI could be. The quantum network data plane is made of quantum links (in blue) and quantum nodes that can be quantum repeaters (QR in blue circles), quantum routers (QR in blue squares) or quantum End Nodes (EN), on which some quantum applications (app in gray rectangle) are running. The entities can communicate using a classical network (gray cloud, it could be the classical Internet). The control plane of the quantum network uses this classical network.

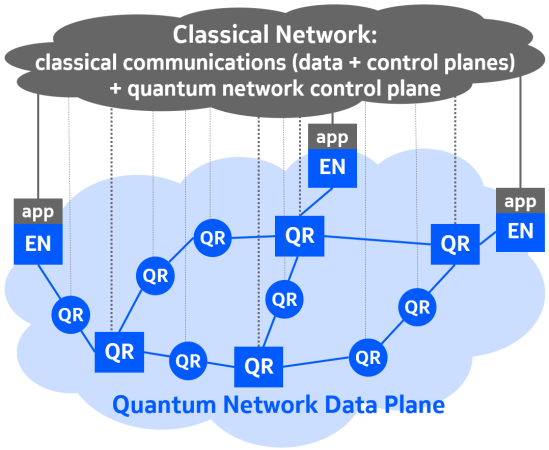

Fig. 6. QI with quantum end-nodes (EN) and quantum repeaters (QR).

Using quantum teleportation and entanglement swapping, the role of the QI is to deliver Bell states between any pair of nodes in the network, that will be consumed by the quantum applications, either directly (e.g., BBM92 or BB91

QKD protocols), or to proceed to quantum teleportation of qubit states (e.g., BB84 QKD protocol, distributed quantum computing, etc.). Because pairs of qubits in a given Bell state are indistinguishable, end users can test some of the pairs they receive to detect any misbehavior of the network. Thus, end users do not need to trust the QI provider!

B. Role of the quantum repeaters

The only difference between quantum repeaters and quantum routers is the connectivity of the nodes. Both have *quantum repeating* capabilities. *Quantum routing*, which we do not discuss in this paper, is required only for nodes with connectivity 3 or beyond.

First, for each quantum link in the network, one of the adjacent node creates Bell states, keeping one of the qubits of each Bell state in its quantum buffer, and sending the other qubit to the other adjacent node. Then, quantum nodes process to entanglement swapping to propagate Bell state to not adjacent nodes, as represented in the Figure 7(b).

Quantum repeating is realized thanks to entanglement swapping. As shown in Figure 7(b), entanglement swapping corresponds to the quantum teleportation [27] of a qubit belonging to a Bell state, the purple one in the intermediate node C, using the green Bell state shared between C and B. The outcome is a new Bell state shared between A and B. Therefore, for any pair of nodes in the network, one can create shared Bell states by processing to entanglement swapping along a path between the pair of nodes. Note that the quantum teleportation is not instantaneous. Indeed, this process involves a Bell state measurement (2 bits) in C and the transmission by C to B of the two measured bits through the classical network.

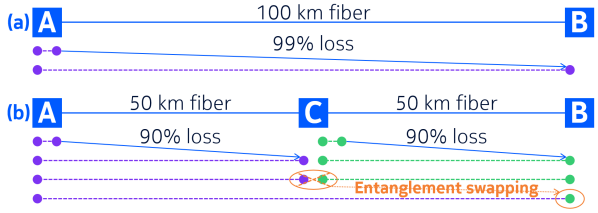

Fig. 7. Bell state creation between Alice (A) and Bob (B):
(a) 100 km fiber with direct qubit transmission;
(b) 2x50 km fiber with entanglement swapping in quantum repeater C.

Having quantum repeaters increases the rate of Bell state sharing. In the example of the Figure 7, if the distance between A and B is 100 km, then 99% of the photons are lost for a fiber direct transmission. The Bell state sharing rate between A and B is thus $1/100^{\text{th}}$ of the Bell state creation in node A, instead of $1/10^{\text{th}}$ for 50 km. The decrease is exponential: $1/1000^{\text{th}}$ for 150 km, $1/10000^{\text{th}}$ for 200 km, etc. If we consider an intermediate quantum repeater C in the middle, the Bell state sharing rate between A and C, and between B and C, is $1/10^{\text{th}}$. C can process to entanglement swapping between the qubits he receives from A and the qubits in his buffer that correspond to qubits B received[3]. If we have perfect entanglement swapping and perfect quantum buffers without loss nor decoherence, the Bell state sharing rate between A and C could be then $1/10^{\text{th}}$ of the Bell state creation. For $N \times 50$ km distance with any N, the rate would be always $1/10^{\text{th}}$. We do not have perfect entanglement swapping and perfect quantum buffers, but we hope that, in the future, their performances will be good enough to have sufficient gain vs. direct transmission.

[3]This requires acknowledgment messages from B through the classical network, which implies some additional delays.

V. Discussions

In this section, we discuss the limitations of the QKD and its extensions with QCI and QI, to position it vs. PQC.

A. Current technological bottlenecks for QKD

The technologies for single link QKD and QCI are mature: QKD products commercially exist for fiber distances up to $\sim$100 km, with final key rate of the order of few kbit/s, and QCI solutions rely on classical processing (nothing quantum inside the trusted nodes). QCI solutions are implemented in field trials today.

But the technologies for quantum repeaters are not yet mature. The main bottlenecks are the quantum buffers and the entanglement swapping. Quantum memory and entanglement swapping have been successfully realized in labs to teleport a qubit using three quantum nodes [28], but with performances that are not compatible with the requirements of quantum networks: we need quantum buffer with many qubits (probably ~ 1000 qubits or even more for higher rates), low decoherence (coherence $\sim$ 100 ms), and efficient entanglement swapping (probably $\geq 50\%$, greater will be better). Long term research is still required to improve the technology and get the right performances, before being able to deploy quantum networks.

B. QKD vs. PQC

QKD alone has two main drawbacks today, its distance limitation and its low key creation rate (typically few kbit/s for $\sim$ 50 km fiber). In this regime, the communication is fully secured thanks to the laws of quantum physics. If one wants to use it in a fully secure way with one-time pad encryption of messages, then its usage is limited to short distance ($\sim$ 100 km fiber) and encryption of short messages.

The need for authentication of the classical channel in QKD may be seen as a drawback. This is the case if one uses classical authentication schemes, but an alternative authentication scheme has been proposed, which is provably secure [19].

To be able to encrypt long messages, QKD can be used to create secured symmetric keys that are used in some encryption mechanisms such as AES-256, like represented in Figure 4. This is less secure than QKD with one-time pad encryption, but the encrypted message transmission rate can be increased a lot. The symmetric keys can be renewed periodically to increase the security level.

To increase the distance range, QCI can be used. But the price to pay is that the users of the QCI must trust the QCI provider. Eavesdroppers may attack the trusted nodes which are weak points in the infrastructure. Depending on the use cases, it may be worth to use a QCI. For example, for military

use cases, the nodes can be defended by soldiers, which make the attack of the trusted nodes more difficult.

The best solution to increase the distance would be QI, but the technology is not yet ready. Fortunately, this should evolves in the long term future.

Concerning PQC, there is no limit in distance nor in encryption rate. But PQC solutions may be broken in the future by classical algorithms, like it was the case for some PQC candidates during the NIST competition [5].

C. QKD and PQC

So, what is the best solution for quantum-safe communications? It depends on the use cases. In future Quantum-Safe solution, both QKD and PQC are complementary. The mix ratio depends at which layer of the network the key generation and its distribution are implemented.

Ephemeral connections where the end-points are unknown in advance, which is generally the case for most of consumers' communications, will benefit from PQC, which can run on existing network infrastructures.

For engineered connections that are established in advance, QKD offers a key authenticity where the key is never transported to the encryption end point and therefore never exposed.

To mitigate the current QKD deployment challenges and permit a commercial deployment, the solution mentioned in Subsection II-E allows for a primary quantum-safe key domain based on QKD to operate alongside a secondary one based on classical symmetric distribution of pre-shared keys. This allows high availability of Quantum-Safe key to the application layer, honoring cryptoperiods. This implementation paired with a future QI will provide an undisputed trust level to the key distribution system without distance limitation.

VI. Conclusion

In this paper, we described how QKD systems works and how their distance range can be extended, first with trusted nodes in QCI, then with quantum repeaters in QI. We also discussed their technological bottlenecks and the need for research to improve the technologies for future QI. Comparing QKD and PQC, we explained how they can be complementary. For a large public PQC is more adapted, being deployable in today's Internet. Leveraging a centralized key orchestration combining the quantum physic (QKD) and the classic physic is more secure and adapted to commercial mission critical use cases, when secrecy is a very high requirement.

Acknowledgment

The author thanks his colleagues Rémi Varloot (Bell Labs), Martin Charbonneau (Head of Quantum-Safe Networks) and Sylvain Chenard (Quantum-Safe Networks Solution Leader) with whom he had fruitful discussions on QKD, QCI and QI.

References

[1] C. H. Bennett, G. Brassard, and A. K. Ekert, "Quantum cryptography," *Scientific American*, vol. 267, no. 4, pp. 50–57, 1992.

[2] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[3] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, 1994.

[4] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, pp. 188–194, Sept. 2017.

[5] National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography." Web page, 2016-2024. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

[6] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014. Original paper: *Proceedings of the International Conference on Computers, Systems and Signal Processing*, Bangalore, pp. 175-179, Dec. 1984.

[7] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–559, Feb 1992.

[8] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug. 1991.

[9] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, p. 057902, Jan. 2002.

[10] A. I. Nurhadi and N. R. Syambas, "Quantum key distribution (QKD) protocols: A survey," in *4th International Conference on Wireless and Telematics (ICWT)*, pp. 1–5, 2018.

[11] L. Gyongyosi, L. Bacsardi, and S. Imre, "A survey on quantum key distribution," *InfoCommunications Journal*, vol. 11, no. 2, pp. 14–21, 2019.

[12] M. Campagna *et al.*, "Quantum safe cryptography and security," white paper 8, ETSI, June 2015. See https://www.etsi.org/committee/qkd for the ETSI QKD Industry Standardization Group.

[13] ID Quantique, "Understanding quantum cryptography," white paper, ID Quantique, May 2020.

[14] European Commission, "The European Quantum Communication Infrastructure (EuroQCI) Initiative." Web page "Shaping Europe's digital future", 2019-2024+. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.

[15] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, Oct. 2017.

[16] M. Mehic *et al.*, "Quantum key distribution: A networking perspective," *ACM Computing Surveys*, vol. 53, no. 5, pp. 1–41, 2021.

[17] W. Kozlowski *et al.*, "Architectural principles for a quantum internet," RFC 9340, RFC Editor, March 2023.

[18] J. Cederlof and J. Larsson, "Security aspects of the authentication used in quantum cryptography," *IEEE Transactions on Information Theory*, vol. 54, no. 4, pp. 1735–1741, 2008.

[19] L. Noirie and R. Varloot, "Authentication through error estimation in qkd," in *IEEE Global Communications Conference*, pp. 1369–1374, 2023.

[20] L.-J. Wand *et al.*, "Experimental authentication of quantum key distribution with post-quantum cryptography," *npj Quantum Information*, vol. 7, no. 67, pp. 50–57, 2021.

[21] W. K. Wootters and Z. Wojciech, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, Oct. 1982.

[22] J. S. Bell, "On the Einstein Podolsky Rosen paradox," *Physics Physique Fizika*, vol. 1, pp. 195–200, Nov 1964.

[23] J. F. Clauser, H. Michael A., A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Phys. Rev. Lett.*, vol. 23, pp. 880–884, Oct. 1969.

[24] S.-K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, pp. 43–47, Jan. 2017.

[25] Nokia, "Quantum-safe optical networking," 2024. https://www.nokia.com/networks/optical-networks/secure-optical-transport/.

[26] Nokia, "Nokia and proximus demonstrate future of network security with europe's first live hybrid quantum encryption key trial." Press release, June 2023.

[27] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, Mar. 1993.

[28] S. L. N. Hermans, M. Pompili, H. K. C. Beukers, S. Baier, J. Borregaard, and R. Hanson, "Qubit teleportation between non-neighbouring nodes in a quantum network," *Nature*, vol. 605, pp. 663–668, May 2022.