Quantum Key Distribution: A Networking Perspective

MIRALEM MEHIC, University of Sarajevo, Bosnia and Herzegovina and VSB - Technical University of Ostrava, Czech Republic
MARCIN NIEMIEC, VSB - Technical University of Ostrava, Czech Republic and AGH University of Science and Technology, Poland
STEFAN RASS, Universitaet Klagenfurt, Austria
JIAJUN MA, QuantumCTek Co., Ltd., China
MOMTCHIL PEEV, Huawei Technologies Duesseldorf GmbH, Germany
ALEJANDRO AGUADO, Center for Computational Simulation, Universidad Politécnica de Madrid, Spain
VICENTE MARTIN, Center for Computational Simulation and Dept. LSIIS, ETSIinf, Universidad Politécnica de Madrid, Spain
STEFAN SCHAUER, ANDREAS POPPE, and CHRISTOPH PACHER, AIT Austrian Institute of Technology GmbH, Security & Communication Technologies, Center for Digital Safety & Security, Austria
MIROSLAV VOZNAK, VSB-Technical University of Ostrava, Czech Republic

The convergence of quantum cryptography with applications used in everyday life is a topic drawing attention from the industrial and academic worlds. The development of quantum electronics has led to the practical achievement of quantum devices that are already available on the market and waiting for their first

The research leading to the published results was supported by the project SGS reg. no. SP2020/65 conducted at VSB - Technical University of Ostrava, Czech Republic, partly by the H2020 project OPENQKD under grant agreement No. 857156 and CiViQ under grand agreement No. 820466. This work was also supported by the MONKS Ministry of Education, Science and Youth of Canton Sarajevo, Bosnia and Herzegovina under Grant No. 11/05-14-27719-1/19.
Authors' addresses: M. Mehic, University of Sarajevo, Department of Telecommunications, Faculty of Electrical Engineering, Kampus Univerziteta, Zmaja od Bosne bb, 71000 Sarajevo, Bosnia and Herzegovina, Sarajevo, Bosnia and Herzegovina, 71000, VSB - Technical University of Ostrava, 17.listopadu 15, Ostrava, 70800, Czech Republic; email: miralem.mehic@ieee.org; M. Niemiec, VSB - Technical University of Ostrava, 17.listopadu 15, Ostrava, 70800, Czech Republic, AGH University of Science and Technology, al. Mickiewicza 30, Krakow, Poland; email: niemiec@kt.agh.edu.pl; S. Rass, Universitaet Klagenfurt, Institute of Applied Computer Science, System Security Group, Klagenfurt, Austria; email: Stefan.Rass@aau.at; J. Ma, QuantumCTek Co., Ltd., Anhui, Hefei, China, 230088; email: yinjuan@ustc.edu.cn; M. Peev, Huawei Technologies Duesseldorf GmbH, Riesstraße 25, Munich, Germany; email: momtchil.peev@huawei.com; A. Aguado, Center for Computational Simulation, Universidad Politécnica de Madrid, Campus Montegancedo, Boadilla del Monte, Madrid, 28660, Spain; email: a.aguadom@fi.upm.es; V. Martin, Center for Computational Simulation and Dept. LSIIS, ETSIinf, Universidad Politécnica de Madrid, Campus Montegancedo, Boadilla del Monte, Madrid, 28660, Spain; email: vicente@fi.upm.es; S. Schauer, AIT Austrian Institute of Technology GmbH, Security & Communication Technologies, Center for Digital Safety & Security, Lakeside Science & Technology Park Nr B10a, Klagenfurt, 9020, Austria; email: stefan.schauer@ait.ac.at; A. Poppe and C. Pacher, AIT Austrian Institute of Technology GmbH, Security & Communication Technologies, Center for Digital Safety & Security, Giefinggasse 4, Vienna, 1210, Austria; emails: {andreas.poppe, christoph.pacher}@ait.ac.at; M. Voznak, VSB-Technical University of Ostrava, 17.listopadu 15, Ostrava, 70800, Czech Republic; email: miroslav.voznak@vsb.cz.

0360-0300/2020/09-ART96 $15.00
https://doi.org/10.1145/3402192

application on a broader scale. A major aspect of quantum cryptography is the methodology of Quantum Key Distribution (QKD), which is used to generate and distribute symmetric cryptographic keys between two geographically separate users using the principles of quantum physics. In previous years, several successful QKD networks have been created to test the implementation and interoperability of different practical solutions. This article surveys previously applied methods, showing techniques for deploying QKD networks and current challenges of QKD networking. Unlike studies focusing on optical channels and optical equipment, this survey focuses on the network aspect by considering network organization, routing and signaling protocols, simulation techniques, and a software-defined QKD networking approach.

CCS Concepts: • **Networks** → **Network properties**; **Network security**; *Security protocols*;

Additional Key Words and Phrases: Quantum key distribution, cryptography, network organization, security

ACM Reference format:
Miralem Mehic, Marcin Niemiec, Stefan Rass, Jiajun Ma, Momtchil Peev, Alejandro Aguado, Vicente Martin, Stefan Schauer, Andreas Poppe, Christoph Pacher, and Miroslav Voznak. 2020. Quantum Key Distribution: A Networking Perspective. *ACM Comput. Surv.* 53, 5, Article 96 (September 2020), 41 pages.
https://doi.org/10.1145/3402192

1 INTRODUCTION

Establishing secure cryptographic keys through untrusted networks is one of the most fundamental cryptographic tasks [1]. While the use of public key infrastructure based on computationally complex mathematical problems and assumptions about the computational power of eavesdroppers prevail, these belong to the group of theoretically breakable computational security solutions. They are therefore under threat as computational power continues to increase and as quantum computing algorithms emerge that can break some widely used computationally complex mathematical problems in polynomial time [2, 3]. Quantum Key Distribution, known as QKD [4], is based on the principles of quantum information theory and allows to establish information-secure cryptographic keys that do not depend on these constraints, at least on a protocol level. A suitable message authentication scheme, such as Wegman-Carter [5], should be combined with QKD to this end [6, 7].

QKD networks differ significantly from traditional telecommunication networks due to the specificity of QKD links and network organization. Restrictions such as limited key generation rate and reachable distance (Section 2), present lack of quantum repeaters (Section 3.2), specific routing due to the use of public and quantum channels in quantum links (Section 6), and network organization that for now has to employ a hop-by-hop key transport approach (Section 5.2.2) are the motivations for this survey. Although several studies on QKD link and QKD quantum channels can be found [8–10], this survey focuses on QKD networking, network organization, routing and signaling protocols, and software-defined QKD networking techniques. After reading this survey, interested readers will have an insight into quantum networks from an engineering perspective and be familiar with the modes of functioning, realization, existing solutions, and methods of simulating quantum cryptographic networks. This survey provides a high-level view of QKD networks and is of use and interest to researchers, practitioners of QKD network design, and PhD students in the field of applied quantum cryptography.

The survey is organized as follows: Section 2 introduces the features of QKD links. Section 3 summarizes the limitations and basic characteristics of QKD networks and explains how they are practically implemented. QKD network types are described in Section 4. Section 5 covers previously deployed QKD networks. QKD network routing techniques are discussed in Section 6. Section 7 provides an overview of QKD software-defined networking. Section 8 concludes this survey.

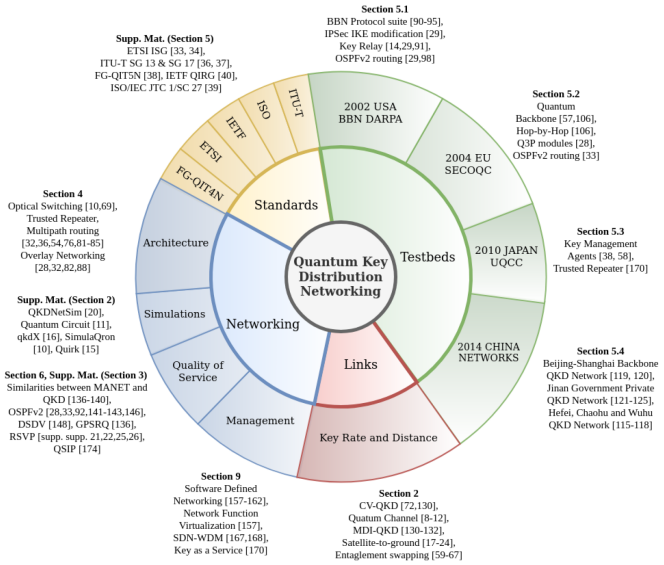


Fig. 1. The graphical outline of the survey with key references.

The survey includes the supplementary material with additional QKD networks listed in Section 1 and simulation techniques discussed in Section 2. Overview of signaling network protocols is given in Section 3, while QKD header and QKD packet encapsulation are discussed in supplementary material, Section 4. Section 5 provides an overview of work in QKD standardization process. The graphical outline of the survey structure is shown in Figure 1.

2 QKD LINKS

A QKD link, or simply, "link," denotes a logical connection between two remote QKD nodes connected by a quantum channel used for transmitting photons and a public channel used for post-processing the exchanged information, respectively. The disadvantage of this type of link is reflected in a limited quantum channel key generation rate, available to the parties connected by a direct optical fiber or free line-of-sight in a point-to-point (P2P) manner over a certain distance. However, it is also a necessary condition for secure key generation.

Although fiber is a good and commonly used medium for transmitting qubits, the installation of a dedicated optical channel for QKD purposes is not practical in all circumstances.[1] A free space link is sometimes convenient, although it has its drawbacks, since it needs suitable atmospheric conditions, a visible light path, and an acceptable signal-to-noise ratio (SNR) that strictly limits usage time. Nevertheless, the results obtained from experiments in Los Alamos [17] and Munich in which a link between the ground and an aircraft flying at 290 km/h was established [18] demonstrated promise with satellite connections [17–23]. After performing a sequence of free space QKD experiments on the ground, China successfully launched the quantum satellite "Micius," which demonstrated a satellite-to-ground QKD over a distance of 645 to 1200 kilometers [24].

The maximum distance, over which key can be generated, decreases with increasing losses and optical detector noise. For a given detector and settings, the detector's dark-count[2] rate is constant,

[1]Some studies, however, analyze the use of bright light for data communication and the quantum signal in a single optical fiber [11–13]. In previously deployed QKD networks, most often dedicated optical connections have been used for QKD purposes [14–16].

[2]A dark count is an event where a single-photon detector clicks even though no photon is present [25].

but key rate decreases with distance due to increase of cumulative losses. In current commercial optical fiber systems, the distance of a QKD link is roughly limited to 100 km, while the key rate is limited to a few tens or hundreds of kbps [26, 27]. Due to the limited key rate, key storage is installed at both endpoints of the corresponding link. This storage is gradually filled with new key material, and the available key material is subsequently used to encrypt/decrypt data flows [28]. The amount of data to be encrypted and the encryption algorithm type determine the rate of key storage discharge, or, simply, the key consumption rate. The key rate of the link is otherwise referred to as the key charging rate [28–31]. The QKD link can be designated "currently unavailable" when no available key material in key storage is found, as no cryptographic operations can be performed [32]. It is also worth noting that an apparently optimal strategy for QKD devices is to continuously generate keys with maximum intensity until the storage is full (which depends on how it is implemented) [28, 33].

A key can be used to encrypt communication over a public channel using a One Time Pad (OTP) cipher and ITS authentication scheme such as Wegman-Carter [34, 35]. Since an OTP cipher requires the same amount of key that corresponds to the length of the message being encrypted and additional keys for ITS authentication, this approach consumes more key material than the message being transmitted. If not enough key material is available, OTP cannot be used, and the use of alternative cryptographic techniques such as Advanced Encryption Standard (AES), which does not require such a large amount of key consumption, is the most common choice [36].

3 QKD NETWORKS

QKD networks are used to extend the range of QKD systems and consist of static nodes that represent secure access points considered to have unlimited processing power and power supply. Because of the point-to-point behavior of the links connecting nodes, previously deployed testbeds [29, 37, 38] have shown that secure keys in QKD networks can be transmitted from node to node in a hop-by-hop manner (Section 5.2.2) or through a key repeater concept (Section 5.1.5). Common to both networks is the assumption that all nodes in a network should be trusted [32, 39]. This assumption can be avoided if multipath communication Quantum Network Coding techniques are used [40]. In this survey, previously deployed QKD networks are briefly discussed, focusing on methods of communication, routing protocols, and network organization.

To facilitate organization, a QKD network has often been described using several layers [41, 42]:

- A quantum layer where a secure symmetrical key is established.
- A key management layer used to verify and manage the previously established key.
- A communication layer where the established key is used to secure data traffic.

As mentioned above, QKD is a key agreement primitive and as such is located in the lowest (basic) layer of the QKD network architecture. Taking into account different rates of key material consumption by different applications, a situation in which not enough key material is available to meet the needs of higher layers is not desirable. The quantum layer therefore needs to continuously establish key material. To provide a guaranteed level of service, the QKD network should have a detailed view in its resources and capacities. Previously deployed QKD networks did not have defined strategies for a quality assurance service. For example, the SECOQC QKD network, discussed in Section 5.2, was committed to the basic *Best Effort* service type, which only defines the average key rate and traffic burst, while the *Guaranteed Key Rate* service type had been suggested for improved versions of QKD networks [33].

Considering the comprehensive and detailed documentation available on quantum optical communications [26, 43–47], the emphasis of this publication is on the two upper layers. These

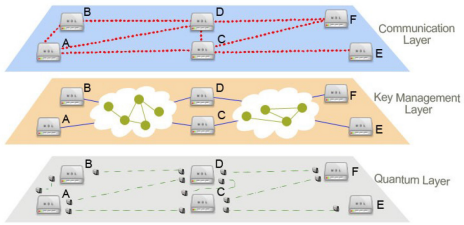


Fig. 2. QKD network hierarchy with quantum, key management, and communication (key usage) layers.

layers can have different and independent network organization, as communication between nodes is achieved through existing standard connections, such as the Internet, where an arbitrary number of intermediate devices can be included (Figure 2). The key management layer is in charge of managing the key storage resources, routing protocols, quality of service (QoS), and so on. The topmost communication layer uses previously established key material to encrypt data traffic by using an existing security protocol suite, such as Internet Protocol Security (IPSec) [14, 48]. However, the described hierarchy distributes the responsibility for security across all three layers.

3.1 QKD Network Attributes

QKD represents a new generation of security solutions that do not rely on the computational assumptions of problems presumed difficult. However, QKD networks must be integrated into the existing environment and need to meet certain criteria and conditions. Some of the most common requirements from QKD networks are listed below.

3.1.1 Key Rate. One of the vital parameters describing a QKD network is the average key rate of a QKD link. Since encryption and decryption operations cannot be performed without sufficient key material, the competition between the rate at which key material is stored in the key storage and the rate at which it is consumed for encryption and decryption operations has a major influence on network performance.

Comparing previously deployed QKD networks and testbeds chronologically, a rapid improvement in the development of quantum equipment is evident. QKD systems implemented in 2002 in the DARPA QKD network could achieve a key rate of approx. 400 bps over 10 km [29]. In 2007, in SECOQC, the maximum key rate was 3.1 kbps over 33 km [37]. The best performed solutions presented in Tokyo in 2009 achieved a key rate of 304 kbps over 45 km [38]. In 2017, China built the 2,000-km Beijing-Shanghai backbone QKD network with devices typically achieving key rates of 250 kbps over 43 km.

In the past 20 years, a steadily increasing secret key rate has been obtained with improved optical components and better electronics mainly in the detectors. For the latest jump to achieve record-high rates of around 10 Mbps [49], digital signal processing in FPGA was optimized. The throughput of measured qubits to enhance key rates has also been enhanced, especially for shorter links, by removing limitations without FPGA. A second race is open to achieving longer single-span transmission distances [50–53] based on protocol enhancements as well as technological improvements leading to detectors with ever-decreasing dark count rates.[3] It could be argued that the development to improve single links on rates at short distances and maximum span will make QKD networks needless. The opposite is true, however, as the opportunity to open a mass market with these improvements at the link level seems low and unlikely to cover broad deployment scenarios specifically using the technical improvements from recent years. What the latest improvements

[3]Note that in this publication (unless otherwise stated) the focus is on the more traditional Discrete Variable QKD modules.

genuinely enable is increased diversity in the links that can be potentially deployed in QKD networks.

It is therefore reasonable to expect that in the future, an optimal solution will significantly exceed the present key rate and distance values, although the race between generation and consumption of key material will remain.

3.1.2 Link Length. The fundamental constraint of a QKD link is the length over which secure key material can be generated (due to scattering and absorption of polarized photons and other factors [27, 44, 45, 54]), which limits the ability of quantum channels (direct optical links or free line-of-sight) to a certain distance. It is interesting to compare the lengths of links in previously built QKD networks.[4] The maximum length in the DARPA QKD network was a 29 km connection through the optical switch between Harvard and Boston Universities [29]. In SECOQC, the maximum length of the link was 82 km between the BREIT and St. Pölten nodes [37], while in Tokyo, the maximum connection between the nodes was a record 90 km between the Koganei-1 and Koganei-2 nodes [58]. In the Beijing-Shanghai Backbone QKD network, the maximum link length is 89.3 km between Hefei and Wuwei.

In current systems with optical fibers, the distance over which QKD links can be effectively applied is limited to roughly 100 km [26, 27].

3.1.3 Protection of Key Material. The main reason for interest in QKD is the privacy of the established key material. This means that the nodes of a QKD network must be secured with a strong probability that the established key material is unique and inaccessible to third parties. The security of key material is evaluated not only when it is established but also when it is managed, stored, and eventually used. It is therefore important to secure each level of the QKD network architecture.

3.1.4 Key Usage. Because of scarce resources (generation key rate), communication in a network is reduced to a minimum, since each additional packet means spending an additional amount of previously established key material. Since communication is usually performed on a hop-by-hop basis that requires the trustworthiness of all nodes in the path, selecting the shortest routing path is necessary to minimize the number of nodes that can potentially be abducted or attacked by an eavesdropper. Also, involving longer paths requires a higher consumption of key material. During network congestion or problems in communication, used key material is deliberately discarded and new key material for retransmission is applied to reduce the risk of leaks [28]. Therefore, minimizing the number of hops is preferable.

3.1.5 Robustness. Because of the cost and manner of implementation, QKD networks will slowly integrate into traditional and everyday telecommunication environments. It is important then to ensure robustness, which is reflected in the gradual and seamless addition of new nodes and establishment of new links. A QKD network needs to provide adequate replacement paths to avoid defective nodes or nodes under severe attack. Regardless of the security techniques, remembering that attackers can easily find ways of terminating optical links and breaking QKD connections is important. A QKD network must have an adequate response to such situations.

[4]Other QKD systems have also been reported, usually with significantly fewer nodes and lower key rates. Some of these systems used a QKD system to secure ballot paper transmissions to counting stations during the federal elections in Switzerland in 2007 [55]; In Durban, South Africa, QKD was used to secure the 2010 Fifa World Cup communications link [56]. Other practical applications of QKD can be found in Reference [57].

3.2 Lack of Quantum Repeaters in Practice

Because traffic can be connected and directed between different network domains, network repeaters have a fundamental role in modern networking. Although theoretical and pioneering results in the field of quantum repeaters are available [59–62], in practice they remain unachievable with current technology [10, 27]. The idea behind a quantum repeater is to employ quantum entanglement of photons to communicate over different quantum links. Quantum entanglement is a key aspect in applying quantum communications and quantum information. In short, quantum entanglement implies that multiple particles are connected together in such a manner that the measurement of one particle's quantum state determines the possible quantum states of the other particles. Even when particles are separated by large distances, they still make up a joint quantum system. Entanglement fidelity is a property used to describe how well the entanglement between two subsystems is preserved in a quantum process.

In theory, however, the application of entangled states and entanglement swapping is hindered by two main roadblocks. The first is that the greater the distance between two entangled systems, the lower the fidelity. In fact, the achievable fidelity of a quantum state decreases exponentially with the distance because of lossy quantum channels [27, 63].[5] In this context, the concept of entanglement purification [64, 65] can be used to increase the fidelity of a single entangled state by using a number of noisy entangled states (as described in Reference [60]). However, this increases the number of required resources for transmitting each qubit over a quantum repeater (i.e., the number of entangled states). The second roadblock in achieving a quantum repeater following the scheme, for example, in References [60, 61], is that quantum memory is required a technology that is not practically available as of today. The use of quantum repeaters is essentially based on the idea of creating "chains" of entangled photons using a technique called entanglement swapping. Concepts either with quantum memories [66] or without [67] have been developed. Different building blocks for matching the transfer of the wavelengths of these flying qubits to quantum memory have been practically demonstrated [68, 69]. Internal loss and fidelity need to be improved to implement chains with one or more intermediate nodes working at higher rates. The first work to integrate future quantum repeaters in the overall infrastructure was recently published [70]. Each node in a QDK network therefore acts as a repeater and forwards packets or enanglement states of other nodes to enable quantum information sharing between QKD hosts.

4 QKD NETWORK TYPES

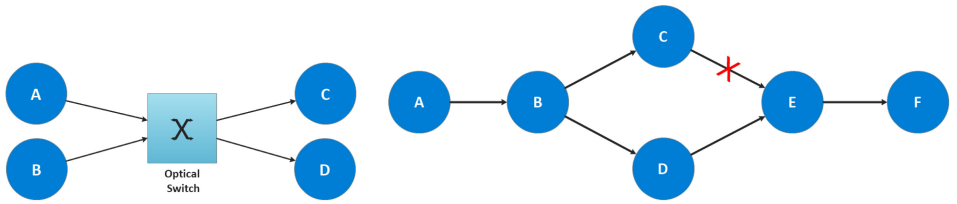
Although many hybrid realizations have been proposed, QKD networks can be grouped into two distinct categories: switched QKD networks and trusted repeater QKD networks.

4.1 Switched QKD Networks

Switched QKD networks consist of nodes connected to a dedicated, fully optical network. This network contains a switching mechanism used to establish a direct optical point-to-point QKD connection between any two nodes in the QKD network. The limitations on distance in point-to-point QKD links restrict these networks to a metropolitan or regional scale [10]. Since every optical switch adds at least several dB of loss to the photonic path, optical switches can significantly reduce a network's range.

The main drawback of switched QKD networks is the requirement of dedicated optical infrastructure for quantum channels, which is often not economically feasible. By contrast, the major advantage of this class of networks is the reliance on an optical switch that allows establishing a connection between two nodes without the active participation of other network nodes (Figure 3(a)).

[5]The usual fiber loss is around 0.21 dB per km for telecommunications wavelengths.



(a) Topology of a switched QKD network.

(b) QKD Network with trusted repeaters.

Fig. 3. QKD Network Types.

Another drawback of switched QKD networks is the consistency of the applied QKD technique. Combining different QKD techniques such as free-space QKD and QKD over fiber is not possible, since no suitable devices that could perform this transformation in the path are available. The first switched all-pass QKD network was described in Reference [71]. Four nodes were connected through an optical switch, and each of the QKD terminals was designed as a transceiver so they could establish a QKD link to one of the other three simultaneously.

4.2 Trusted Repeater QKD Networks

In trusted repeater QKD networks, the security of each node along the transmission path is essential for securely transmitting information (hence the name). Point-to-point communication between two nodes provides identical keys to the nodes and thus enables secure communication (Sections 5.1.5 and 5.2.2). Taking into account the lack of a quantum repeater, nodes are also responsible for routing and forwarding mechanisms (Figure 3(b)). Organizing a network in this manner is its greatest drawback, because the security of transfer depends on the security of all the nodes in the path. However, trusted repeater networks are not limited by distance or node numbers and can be made up of different QKD devices implementing different QKD technologies.

4.3 Security without Trusted Repeaters

Since the quantum channels can be "given" to the eavesdropper without compromising the security of QKD, a rational adversary would rather target the weaker link, being the node. The usual assumption is letting the nodes be "invulnerable," which is the *trusted repeater* hypothesis. However, given that the optical device controls at some point will most likely have a conventional computer control logic, the security of the device is no better than the security of a classic computer running QKD algorithms and its physical protection.

The admittedly strong assumption of fully trusted repeaters can be relaxed in at least three ways: (i) use measurement device independent (MDI) QKD, (ii) use quantum repeaters, and (iii) rely on multiple paths.

This first approach has been described by Reference [72] and adds the assumption of perfect state preparation achievable by communication parties, as well as adding a potentially unstrusted location to the quantum channel. Measurements using Bell states and formal arguments for "unconditional security" have been supported with experimental demonstrations [73, 74]. Of course, the absence of the trusted repeater assumption in these proofs makes security much stronger than those assuming trusted repeater QKD. Note, however, that MDI QKD essentially prolongs the quantum channel but the two sender stations must still be situated in Trusted Repeater Nodes. This also holds true for the other alternatives outlined next (except possibly in the case when end-to-end quantum links could be established without intermediate Trusted Repeater Nodes).

The concept of quantum repeaters was discussed above (see Section 3.2). While practical demonstrations have been presented [61, 66, 67], the spatial distances the technology can overcome (as of today) strongly depend on the amount of fidelity induced by the entanglement swapping and the degree to which it can be handled (Section 3.2).

The third and most practical method today resorts to classic technology and employs multiple paths and threshold cryptographic techniques to mitigate the risk of eavesdropping. Roughly speaking, multipath transmission quantum networks trade trust in the repeaters for the assumption of the repeater being vulnerable to eavesdropping, the attacker being forced to intercept many of the intermediate devices to discover the message. Indeed, it can be shown that in absence of trusted repeaters, multiple paths are a theoretical necessity. At the same time, path redundancy also mitigates the issue of all QKD implementations being vulnerable to denial-of-service attacks (the adversary may passively eavesdrop not to get information, but to make the local quantum key stores run dry to enforce the endpoints to switch to conventional transmission techniques [75]). Advanced routing mechanisms can be put to use to bypass lines with detected eavesdroppers. Indeed, otherwise, attackers could try to break the security, employing passive eavesdropping to redirect traffic over vulnerable repeaters and thus get ahold of the secret key [76]. It can be shown [77, 78] that "end-to-end security" without trusted repeaters in quantum networks (without quantum repeaters) can be restored only under weak assumptions of the attack resilience of nodes [79]. Furthermore, using the same techniques, *simultaneous multi-level security* against other attacks can be achieved along the same lines to an arbitrarily selected level of service quality [80]. The topology of a quantum network generally has a strong impact on achievable security, and despite theoretical and practical progress in the construction of quantum networks, even without trusted repeaters [33, 36, 54], the problem remains computationally (in fact, NP-) hard in its most general form [81]. Methods for foiling covert channels and malicious classical post-processing units have been discussed in Reference [82].

4.4 QKD Overlay Networks

While the previously described QKD network types relate to the organization of quantum channels, the QKD overlay network type refers to public channel realization. The primary goal of the overlay network is achieving the higher hierarchy network with the aim of providing a better QoS and utilizing the resources of lower-level networks. In doing so, the overlay network aims to be independent of the defined paths from Internet Service Providers (ISP). Finding alternative routes that can provide a service with a higher degree of quality and quick rerouting in the case of interrupt detection or using multipath communications are key features of the overlay network approach. The use of multipath connections is an often suggested solution for improving network workloads through protecting against network failures, network load balancing, large bandwidth implementation, low-delay time selection, and more [83–86]. Studies have shown that at least four link-disjoint paths between large ISPs are present in 90% of point-of-presence pairs [87, 88].

It is known that routing between network domains using external routing protocols such as Border Gateway Protocol (BGP) results in slow response and recovery from network outages. Due to the time required to obtain information about interruptions or congestion on network links and the BGP minimum route advertisement interval timer settings, which is usually within minutes, the time needed to obtain a consistent view of the network after a link outage can reach tens of minutes, which is a long period for network applications. BGP also propagates only one route, and detecting the alternative route network nodes need in different situations is difficult [89].

The overlay network can help overcome these challenges by establishing the network with a peer-to-peer approach. The overlay network connects nodes in different domains and allows the use of alternative paths by encapsulating traffic to the traffic in the lower network. When

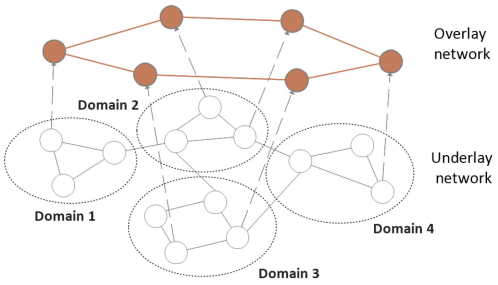


Fig. 4. An overlay network over multiple network domains.

an intermediate node in the path received the packet, the node will unpack the packet, analyze the IP address of the recipient, re-encapsulate packet again, and forward it further to network nodes that may be in other domains. Simply, it is a hop-by-hop approach popularly applied in QKD networking (Figure 4). Considering the encapsulation principle, overlay nodes independently perform link state measurements and can respond more quickly to link congestion by redirecting traffic to other less-congested links. Overlay networks can offer new functionality that is difficult to perform in lower-layer networks. The overlay QKD approach is attractive, since it can be used to bypass "untrusted" nodes and perform quick rerouting when trust in nodes is no longer valid or multipath communication is required [28, 33].

5 PREVIOUSLY DEPLOYED QKD NETWORKS

This section briefly discusses some previously deployed QKD networks. Since much of the literature deals with quantum optical infrastructure, the focus is placed on the logical structure of networks and topology, key storage and management solutions, key usage, and the solution's performance.

5.1 DARPA QKD Network

The world's first QKD network was the DARPA QKD Network, presented in December 2002 by BBN Technologies and Harvard and Boston Universities [14]. Initially, the network consisted of a weak-coherent BB84 transmitter pair (Anna and Alice), a pair of compatible receivers (Boris and Bob) and one 2×2 optical switch that could connect any sender to any receiver (Figure 5). Later, the network was extended with two free space QKD links, and the third planned free space link from QinetiQ (UK) was not explained in any official project documentation. The DARPA QKD network combined two previously explained types in a hybrid solution. The DARPA QKD network laid the foundation for the further development of trusted repeater QKD networks, but it also demonstrated practically the disadvantages of a switched QKD network type.

Two nodes (Alice and Bob) and a switch were located at BBN, while Anna and Boris were located at Harvard and Boston Universities (BU), respectively. BBN designed its own 2×2 optical switch and used it to connect Anna, Alice, Bob, and Boris. This switch was optically passive and therefore did not disturb the quantum state of photons. The switch was constructed by modifying a standard telecommunications facility switch. It operates by moving reflective elements that change the internal light path to produce either a BAR or CROSS connection. It is controlled through a direct line from Alice's optical process computer (OPC) by applying a TTL-level pulse to either the BAR or CROSS pin for 20 ms to switch the activated position. According to Reference [29], switching time was 8 ms and optical loss was less than 1 dB.

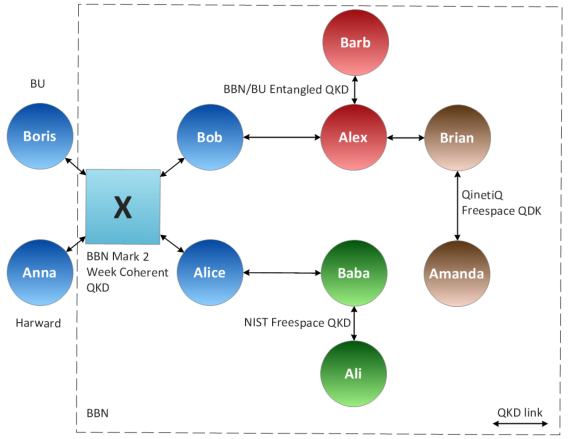


Fig. 5. Connection scheme of the DARPA QKD network in 2005.

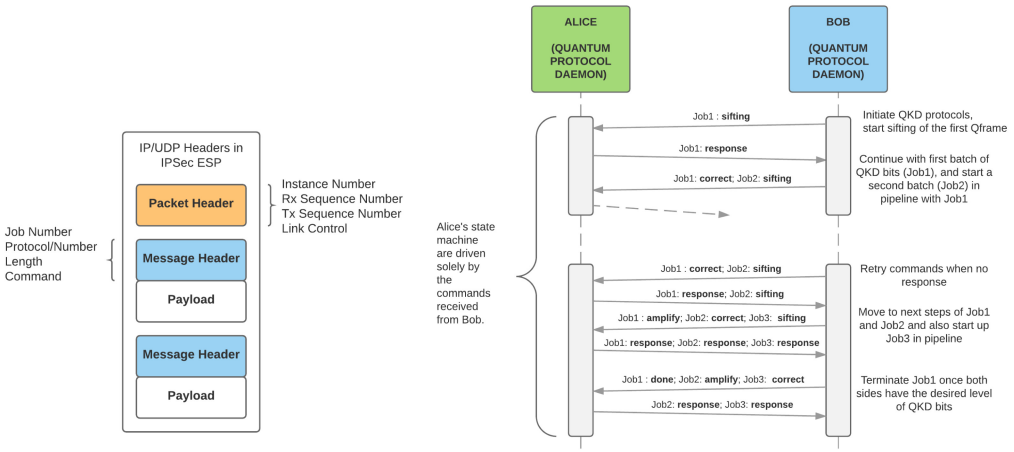
Table 1. The BBN Protocol Suite in Context

QKD Post-processing Stage	Technique Used	Details/Reference
Sifting	SARG04 Sifting	[93]
Error Detection and Correction	Cascade	Traditional
	BBN "Niagara" FEC	[94]
Entropy Estimation (Estimation of Eve's knowledge)	BBSSS	[91]
	Slutsky	[95]
	Myers/Paerson	[96]
	Shor/Preskill	[7]
Privacy Amplification	GF[2^n] universal hash	[92]
Authentication	Hybrid Public Key/ Universal Hash Function	[5] Combination of the Universal Hash Function and Public Key Cryptography

A previously performed set of experiments presented results that measured degradation in the phase-modulated QDK incurred by optical switches [90]. A demonstration of QKD transmission and the results of insertion loss, which was the principal effect on QKD throughput in three different types of optical switches, yielded the following: 2×1 optical-mechanical switch (4.7 dB loss), 2×2 $LiNbO_3$ switch (5.4 dB loss) and four-port MEMS switch (5.3 to 5.9 dB of loss).

5.1.1 BBN Protocol Suite. Considering that the DARPA QKD network was the first QKD network, no predefined protocols could be used for QKD communication over the public channel. BBN therefore developed its own QKD protocol stack in C programming language. All messages were packed in IP datagrams to convey the control messages through the Internet [91].

Table 1 presents only the list of technologies used, while interested readers may refer to References [29, 92]. It can be seen that several techniques were used for different post-processing stages. The aim was to minimize the number of messages exchanged to speed up the key generation rate and reduce congestion caused by the sudden transfer of a large number of packets over a public channel. Figure 6(a) shows the basic format of BBN's QKD Protocol datagram. Each



(a) Datagram Format. (b) Example of messages exchanged.

Fig. 6. BBN's QKD Protocols.

datagram contains a packet header with details of the permitted, reliable, in-order transmission of the message, crash detection, and so on.

The datagram is filled with one or more messages of variable length, carrying the details needed to describe commands or a response to an action. It is important to emphasize that these datagrams are protected by an IPSec security mechanism in standard mode.

The aim was to create a secure tunnel between Quantum Protocol Daemons so all traffic over the public channel was encrypted, authenticated, and integrity-checked. An example of messages exchanged by BBN's QKD Protocol is shown in Figure 6(b).

5.1.2 Key Management and Usage. In the final technical DARPA report [29], details for the originally planned and used technologies are given. It is interesting to note that the authors assumed the Diffie-Hellman (DF) key agreement primitive would be broken by 2015. Since the average key rate of a QKD device was 1 kbps, the goal was to introduce QKD as a new key agreement solution and integrate it with existing IPSec and IKE (Internet Key Exchange) key management protocols. Later, when the key rate of QKD devices increased, IKE could be abandoned and the use of OTP forced, which would lead to a highly secure network architecture.

The authors proposed the use of a QKD network between sensitive areas only, in which the QKD endpoints would be used to further distribute obtained information into private networks (enclaves). The QKD endpoints would have had the same function as border routers in standard IP networks. Connecting the end-user directly to the QKD network was never planned. The main idea was to create a storage "reservoir" at both ends of the corresponding QKD link that would be gradually filled with key material established through QKD. This keying material would later be used with an IPSec protocol suite and employed to encrypt virtual private network (VPN) tunnels. When the traffic was received by the corresponding endpoint at the receiving end of the VPN tunnel, it would be forwarded to a final user located in the private network (enclave).

To simplify the process but also use the software of different platforms and manufacturers, the QKD endpoint was separated into two distinct computers. The first computer, called Optical Process Control (OPC), used the LabView software to control associated QKD equipment, while the other computer was used for IPSec communication, routing, network protocols, and QKD protocols (sifting, privacy amplification, etc.). These two computers used local 100 Mbps Ethernet

connections. For synchronous data exchange, a specialized set of BBN-supplied UDP[6] protocols was used.

Another important issue was synchronization between these computers and synchronization between QKD and the VPN protocol suite. More precisely, solving the management of key material produced by optical devices was necessary. The procedure was as follows:

(1) The OPC computer delivers a fixed-size raw Qframe block of symbols transmitted through optical devices. It contains an indication of the bases that were used to encode the information in photons. These Qframe blocks are further processed by a QKD daemon with the QKD post-processing suite (sifting, QBER, privacy amplification, or similar), producing a Qblock as output.
(2) A Qblock is a fixed-size block of shared bits, each Qblock having its own 16-bit Qblock identifier (ID). Qblocks are stored in a storage reservoir of key material at both ends. These blocks are stored continuously, regardless of consumption.
(3) The IKE daemon uses Qblock IDs to establish a final key, which is then used by IPSec, since both ends have the same key material stored in their respective storage reservoirs.

5.1.3 IPSec Protocol Suite. Internet Protocol Security (IPSec) is a protocol suite for the purpose of ensuring the integrity, authenticity, and confidentiality of connections over the public internet. IPSec operates at the Internet Protocol (IP) layer and as a perimeter between protected and unprotected network interfaces by requiring a protection level. By default, IPSec uses the Internet Key Exchange (IKE) method for automatic keying. The basic concept of IKE protocol is simple and takes place in two phases. The first phase establishes an authenticated, bi-directional, secure link (the Internet Security Association) and the Key Management Protocol (ISAKMP) SA by exchanging random *nonce* and half-keys for the Diffie-Hellman key exchange. Authentication of a Phase 1 channel is performed by exchanging messages encrypted with a session key. Random secret bits from Phase 1 that are used to establish ISAKMP are conventionally termed SKEYID. These bits are considered the most sensitive point in IKE points, since they are used as a partial input for creating Phase 2 SA keys and for protecting traffic through a given Phase 2 SA. Replacing these bits from time to time in order not to compromise the system's security is therefore important.

The second phase uses SKEYID bits to negotiate the IPSec SAs between two gateways that carry message traffic for a certain VPN traffic flow. Each IKE security association has a maximum lifetime that limits the use of key material for the previously established association. These limitations can be defined in time (seconds) or in encrypted data (kilobytes) and are stored in SPD entry for a given SA. After the lifetime expires, a new SA must be negotiated with fresh key material. It is important to note that there is no standard for using OTP with IPSec. Various solutions have therefore been proposed, such as References [14, 48, 97].

The DARPA QKD Network employed IKE because at the time of its development (January 2002), IKE was the most widely deployed internet key agreement protocol. Two extensions exist that depend on a later-used type of cipher:

- The Quantum Perfect Forward Secrecy (QPFS) extension, which is based on the use of QKD techniques, for agreeing on secret keys employed as seeds for conventional symmetric ciphers such as AES or 3DES. Since the security of these symmetrical ciphers may be compromised in the following years, continual and automatic reseeding with fresh QKD bits is advisable. In the DARPA QKD network, AES keys were refreshed about once per minute [15]

[6]User Datagram Protocol (UDP) is a message-based transport layer protocol based on the "fire-and-forget" connectionless principle.

by omitting the Phase 1 negotiation and using QKD bits as a direct input to the IKE Phase 2. This solution increased the security of IPSec associations, since the keys were derived from QKD instead of the Diffie-Hellman (DH) key exchange.
- An extension based on the use of QKD techniques for agreeing on secret key bits used with a one-time pad (OTP) cipher. This solution lowers the data rate to the QKD key rate, since the key material in the storage reservoir is charged only by QKD.

To implement the listed extensions, the DARPA QKD network team extended the IKE Phase 2 by adding an option to the QPFS extension that works in the same structural manner as a regular IKE Phase 2 PFS but uses QKD bits rather than bits obtained from the DH key exchange. The solution was implemented in NetBSD with the "raccoon" IKE daemon. The modifications included policy mechanisms to specify when and which extension should be used, with the possibility to specify values (re-key rates, cryptographic algorithms, keys, etc.) for each VPN gateway.

5.1.4 Routing in the DARPA QKD Network. A routing mechanism is required in situations when two nodes do not have a direct point-to-point QKD link between them and therefore need to agree on a path through a trusted repeater network.

Each node has a database of the full link state of the network. For each network node, it keeps the node's ID and a list of neighboring nodes. DARPA modified well-known Open Shortest Path First (OSPF) routing protocol [98] to use the specific QKD networks metric [92]. The idea is that each node exchanges a certain number of bits with its neighboring node, thereby measuring the rate of exchange and the total number of bits exchanged (measuring the quality of the connection) [99]. Link quality is calculated using link metric m and stored in the database of the corresponding node:

$$m = \begin{cases} 100 + \frac{1000}{q-t}, & q > t, \\ \infty, & q \leq t, \end{cases} \tag{1}$$

where q denotes the number of Qblocks expected to be available on the link in one Link State Announcement (LSA) update interval, m is the link metric, and t is the threshold (default value 5) for a minimum number of Qblocks to be maintained on an active link.

Later, when a route between distant nodes is requested, the route with the smallest total metric is selected. For the purposes of finding this path, Dijkstra's algorithm is used. To refresh the records in link-state databases, periodic messages ROUT1_LSA are exchanged [29]. These messages carry the node ID of the sending node, the node ID of the neighboring node, and the corresponding 32-bit link metric. ROUT1_LSA messages are exchanged at every LSA update interval, which is a configurable parameter set to one minute by default. Each node has an individual LSA timer that does not depend on other nodes in the network.

However, it is evident that described modification of OSPFv2 protocol does not take into account the parameters of the public link. The metric m defined in Equation (1) only examines the amount of available key material, without considering other parameters such as link load or delay [99]. Routing protocols are discussed further in Section 6.

5.1.5 BBN's Key Repeater Protocols for Trusted Networks. As noted above, a QKD network is used to overcome the limitations of the length of the QKD link. The DARPA QKD network laid the foundation for the Key Repeater Protocol and represents the first implementation of a Trusted Repeater QKD network. This implementation will be explained briefly here. More details can be found in Reference [29].

When two distant nodes in the QKD network (i.e., node A and node D) want to establish secure communication and no direct point-to-point link exists between them, they need to agree on a path through the network. This path is calculated with a routing protocol, and the nodes use a

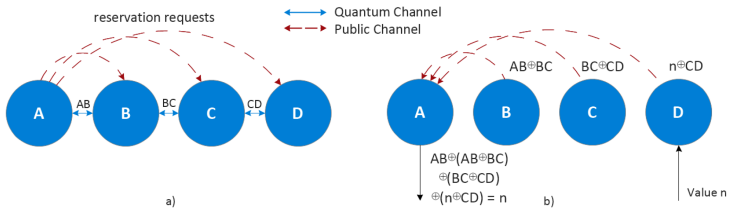


Fig. 7. BBN Key relay architecture.

Table 2. DARPA QKD Network—Brief Summary

Project year	2002–2006
Number of nodes	10
QKD network type	Switched QKD network and trusted repeater
Max. key rate[7]	400 bps
QKD protocol used	BB84
Key references	[14, 29, 92]

Key Repeater strategy to establish key material. The source node is always the node with the higher node ID. The source node (node A in Figure 7(a)) sends reservation requests to each node in the path (intermediate nodes) and to the destination (node D in Figure 7(a)). Each node in the path then negotiates with its predecessor for a Qblock (Figure 7(a)) and informs the source when the negotiation process has been successfully completed. If reservations are successful, the source requests a key from the destination and all the intermediate nodes. The intermediate nodes send the XOR of two Qblocks established with neighboring nodes, while the destination node sends the XOR of the previous hop Qblock and a new random Qblock n (Figure 7(b)). This Qblock n is the final key shared by source node A and destination node D.

From the above, it is obvious that BBN's Key Repeater method of establishing key material takes time and requires the absolute trust of each node involved in communication. Authentication techniques therefore have a special significance in the entire process. As already discussed, the most effective way to circumvent compromised nodes is to use multiple independent paths.

5.1.6 Summary. The DARPA network was the first network to demonstrate QKD networking. The performance achieved by this network (maximum distance of 29 km via the optical switch between Harvard and Boston Universities [91] and maximum key rate of 400 bps) is considered the basis for further QKD deployment. The system involved trusted repeater and switched QKD networking, demonstrating the advantages and disadvantages of both methods. A brief summary of the DARPA QKD network is given in Table 2.

However, the DARPA network was shut down in 2006, and no other field deployments by US government agencies have been reported since. In 2017, the Quantum National Initiative was announced, fueled by China's successful launch of the "Micius" satellite [100, 101]. In 2018, the startup company Quantum Xchange announced plans for the first commercial quantum communication network "Phio" in the USA [102, 103]. Using its own exclusive trusted nodes, Quantum Xchange provides secure key transmission over long distances. This QKD network operates in Washington, D.C., and New York City, including the link connecting financial markets on Wall Street with data

[7]Denotes the key rate of the final material ready for further use and stored in the storage reservoir.

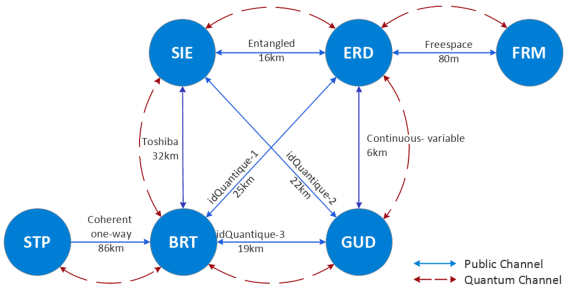


Fig. 8. Connection scheme of the SECOQC QKD network. Solid lines represent quantum connections, while dotted lines represent classic communications connections.

centers in New Jersey [104]. To achieve double network capacity, collaboration with Toshiba was announced [105].

5.2 SECOQC QKD Network

In 2004, the European Commission's (EC) integrated FP6 Project SECOQC (Secure Communication based on Quantum Cryptography) brought together 41 research and industrial partners from 11 European Union countries, Russia, and Switzerland. The main aim of the SECOQC project was to firmly define the practical application of QKD technologies and systematically treat the issue of QKD networks, including their security, design and architecture, communications protocols, implementation, demonstration, and test operation of QKD network protocols.

The SECOQC approach was to define QKD networks as infrastructure based on point-to-point QKD capabilities that aimed for ITS key agreement and secure communication [106]. Taking into account that the first results of the DARPA QKD network were available [92], SECOQC decided to further improve the trusted repeater QKD network type. The "Quantum Backbone" QBB network of metropolitan distance (6–85 km) consisting of seven fiber-bound key distribution links plus one short distance free-space link was deployed for testing purposes in Vienna [57]. Five nodes—SIE, BRT, GUD, FRM, and ERD—were located at the Siemens premises, and the STP node was hosted by a repeater station near St. Pölten on the communications line from Vienna to Munich, Germany.

5.2.1 QBB Links and Nodes. As shown in Figure 8, SECOQC integrated eight links belonging to six different systems:

- Attenuated Laser Pulse — a modified, commercially available "Cerberis" solution implemented by Swiss company idQuantique.
- One-way Weak Coherent Pulse system with decoy states — implemented by Toshiba UK.
- Coherent-One-Way — implemented by the N. Gisin's team at GAP, University of Geneva.
- Entangled photons — provided by the Austrian Research Centers (ARC) and Royal Institute of Technology of Kista KTH, Sweden.
- Continuous Variables — implemented by the CNRS-Thales-ULB consortium from France/Belgium.
- Free Space link — developed by Ludwig Maximilian University of Munich, Germany.

All of these systems had to comply with the following requirements:

- A key rate greater than 1 kbps over 25 km of fibers (6 dB loss with a fiber attenuation of approximately 0.25 dB/km over standard telecommunications fiber).
- Autonomously deliver the key for more than six months without human interaction.

- A latency time of one minute for a new start-up.[8]
- All equipment used must fit into a standard 19" telecommunications rack.
- Each QKD-device must communicate with its peer over a standard interface provided by the node module controlling the share management commands.

SECOQC network included several different QKD solutions:

- The free space QKD system employed the BB84 protocol with decoy states, which resulted in a secure key rate of up to 17 kbps over 80 m between the ERD and FRM nodes.
- The idQuantique QKD system implemented the BB84 and SARG04 protocols using a commercial Cerberis system, which resulted in an almost equal value prescribed by the SECOQC criteria (1 kbps).
- Toshiba Research Europe Ltd (TREL) implemented a weak coherent pulse (WCP) decoy state plus vacuum state BB84 protocol and obtained a 5.7 kbps key rate over a fiber length of 25 km.
- A coherent One-Way (COW) System designed by GAP (Group of Applied Physics at the University of Geneva) achieved a novel distributed phase reference COW protocol, which can be seen as a BB84 modification with phase relations between pulses [28].
- The entanglement-based QKD (ENT) developed by an Austrian-Swedish consortium implemented BBM92 for entangled states between the ERD and SIE nodes over a 16-km fiber and provided a reliable key rate of over 2 kbps.
- The Continuous-Variable (CV) system was developed in cooperation between Charles Fabry de l'Institut d'Optique, THALES Research & Technology France and University Libre de Bruxelles. Their system achieved a distribution rate of 8 kbps over a 6.2-km standard optical fiber (attenuation of the fiber was approximately 2.8 dB, while the length of an equivalent fiber with a loss of 0.2 dB/km would be 14 km).

SECOQC nodes followed the DARPA approach of storing key material in storage reservoirs. Considering that the QKD links between nodes must be achieved in a point-to-point manner, a node needs to possess a dedicated QKD device for each connection to other nodes. Key material from QKD devices is first deployed in *Pickup Stores*. This temporary storage keeps the key material until it is confirmed that the same material is found in both QKD nodes forming the corresponding QKD link. After successfully confirming the existence of the same key material at both ends, the key material is then forwarded to a *Common Store*. There is only a single Common Store for the Q3P link (which can contain one or more QKD links between two nodes), and key material in this storage is uniquely identified by the key material block. When use of the key material is requested, keys are forwarded to *In* or *Out* key buffers and used for encryption or decryption purposes by a *Crypto Engine*. Organizing key storage in a described manner, QKD nodes can tolerate fluctuations in key consumption by buffering the generated key material. More details about *Key Store* organization can be found in References [28, 106].

5.2.2 Hop-by-hop Message Transmission. The SECOQC network has laid bare the basics of the hop-by-hop approach to QKD network communication. This mode is known as the "Store & Forward" technique and implies the use of a separate key for each link in the path. As shown in Figure 9, each node decrypts the message, verifies the authentication tag, and re-encrypts the message using a key that matches the connection to the next node. The procedure is repeated in each node on the path until the message reaches its destination [106].

[8]Time after a total restart of the system.

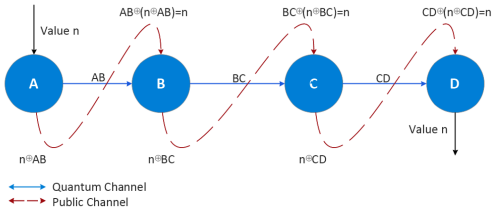


Fig. 9. "Hop-by-hop" message transfer.

5.2.3 Routing in the SECOQC QKD Network. SECOQC suggested using an IPv4 address structure and geographical division of the QKD network in multiple routing areas for the following reasons:

- A QKD network is a private network that has the freedom to use any available area of IPv4 address space.
- Expecting a rapid and extensive spread of the QKD network is not reasonable. IPv4 address space should therefore be enough to address current and future nodes.
- The distance limitations of QKD links do not allow the QKD network to be divided between the backbone and an arbitrary number of autonomous systems. Treating all nodes in the network equally is therefore necessary.
- The current lack of quantum repeaters means QKD nodes must be seen as an access point for end-user applications, not just as forwarding nodes in the network.

To meet the requirements for addressing and routing, SECOQC proposed forming a node with the following components:

- Q3P modules responsible for link-level communication with other nodes.
- A routing module to collect and maintain routing tables.
- A forwarding module to create paths and make forwarding decisions.
- Other modules for node management, random session key generation, security monitoring, and so on.

The function of a routing module is to maintain a local table of routing information and inform other nodes about updates in the network so they can also update their routing tables. Well-known routing protocols can be modified and used in the QKD network, but it is necessary to take into account the lack of a quantum repeaters, which means that each network node must be ready to receive traffic from its neighboring node and forward it along the best path to the requested destination (more details in Section 6). This is the forwarding module's task. The module receives an incoming packet, checks the TTL value and authentication checksum, and depending on the results, decides either to forward or discard the packet.

In SECOQC, a modified version of the OSPFv2 protocol was used. It is interesting that OSPFv2 does not support QoS routing, which is necessary to guarantee the required service type. OSPFv2 was implemented with the aim of accelerating the development process [33]. In the standard OSPF, the forwarding decision is made based on the destination address and the shortest path information in the routing table. However, considering the low key rate of QKD links, other parameters must be taken into account when calculating the best path.

To compute the shortest path tree data structure, the Dijkstra algorithm is used. Each node calculates a unique shortest path tree and uses a modified version of the OSPFv2 to compute the routing table. The main difference is that the modified OSPFv2 calculates multiple paths to each destination instead of a single shortest path. Multiple paths are needed to fulfill the requirements

of load balancing and spare paths. Each QKD node therefore computes as many routing tables as the number of its interfaces. OSPFv2 delivers periodic LSA messages to other nodes in the network with the aim of spreading information about the current state of the network.

Furthermore, each node computes an *Extended Routing Table* in which all costs in increasing magnitude to every other node are listed. This table is used to merge all routing tables in a single place. The table structure is similar to the standard routing table, the difference being that it has as many entries for each destination as the number of outgoing node links [33]. Now, the node can find multiple paths to the destination node, but it also needs to know an approximate load of selected links in the path. If the load of a link is greater than the calculated threshold, the next best link is looked up, and so on. The third *Load State Database* table is computed to store details about the approximate load of each outgoing link. It is used to verify whether the link has sufficient resources for transmitting the message [28]. The approximate load of the outgoing link i at discrete time t is denoted by $L_i(t)$ and calculated using a low-pass filter with Equation (2):

$$L_i(t) = \left(1 - \frac{1}{w}\right) \cdot L_i(t-1) + \frac{1}{w} \cdot l_i(t), \tag{2}$$

where $l_i(t)$ is the instant load of the outgoing link i and w is the filter constant. The instant load $l_i(t)$ is calculated as a ratio of the number of transmitted bits in the previous unit time. More details about routing and forwarding modules can be found in References [33] and [28].

5.2.4 Summary. It should be emphasized that application development was not the SECOQC project's task. SECOQC, however, conducted several experiments to test the solutions created. During the SECOQC QKD conference from October 8–10, 2008, a demonstration of telephone communications and video conferencing was given. A VPN tunnel was established between the nodes and AES encryption was used. The AES key was refreshed every 20 seconds,[9] and at certain moments, AES encryption was replaced by OTP [106]. The main objective was to test routing mechanisms, measure key material consumption and generation, and highlight basic mechanisms of the SECOQC network functionality. It is worth noting that SECOQC investigated the establishment of a QKD connection to the end-user [28].

The SECOQC network has laid the groundwork for a hop-by-hop networking approach that greatly simplifies views on implementing routing decisions. The hop-by-hop approach allows each node to decide which further path to direct the message, which offers more flexibility in implementing routing protocols. However, the BBN key-repeater approach described in Section 5.1.5, requires having a global, up-to-date view of the network before establishing and reserving resources on the path, which can be demanding due to the dynamic consumption of generating key rates. The SECOQC network also demonstrated interoperability between different equipment manufacturers and showed that the QKD network could achieve ranges of almost 100 km (the maximum link length was 82 km between the BREIT and St. Pölten nodes) [37]. A brief summary of the SECOQC network is given in Table 3.

Interest in quantum cryptography in the EU has been accompanied by projects funded under the Quantum Technologies Flagship, QuantEra, COST, and EuraMet programs [107–112]. In 2019, the EU Horizont2020 project OPENQKD with a consortium of 38 partners from industry and academia was announced [113]. OPENQKD aims to lay the foundations for future European quantum infrastructure and the convergence of quantum technology with practical telecommunications systems in Europe within three years.

[9]The key was refreshed every 20 seconds regardless of whether there was traffic to be protected by that key. Although AES encryption with frequent key exchange cannot provide ITS communication, this mode may be acceptable for certain applications that do not require more stringent security criteria.

Table 3. SECOQC QKD Network - Brief Summary

Project year	2004–2008
Number of nodes	6
QKD network type	Trusted repeater
Max. key rate[10]	3.1 kbps over 33 km
QKD protocol used	BB84 (decoy state), SARG04, COW, BBM92, CV-QKD
Key references	[28, 33, 106]

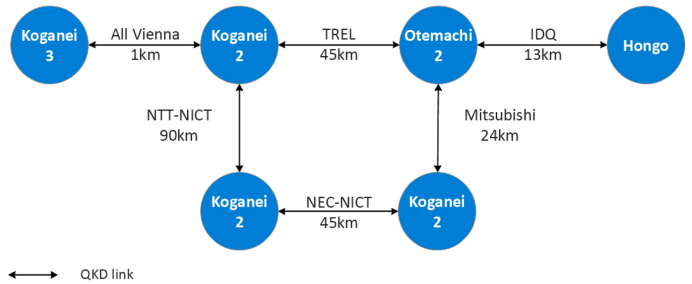


Fig. 10. Topology of the Tokyo UQCC QKD network.

5.3 Tokyo UQCC QKD Network

Two years after SECOQC, nine organizations from Japan and the European Union participated in the Tokyo UQCC QKD testbed network ("Japan Giga Bit Network 2 plus" - JGN2plus). The network consisted of parts of the National Institute of Information and Communications Technology of Japan (NICT) open testbed network called "Japan Giga Bit Network 2 plus" (JGN2plus) [38]. The Tokyo QKD network contained four access points, Hakusan, Hongo, Koganei, and Otemachi, and six nodes connected by commercial optical fibers installed at these access points (Figure 10). Since half of chosen fibers were aerial, large losses occurred on the links. The link between the Kogenei and Otemachi nodes had a loss rate of about 0.3 dB/km, while on other links this rate reached even 0.5 dB/km.

Similarly to SECOQC, the project's participants implemented certain network links, allocated as follows:

- A 24-km link between the Otemachi and Hakusan nodes was provided by the Mitsubishi Electric Corporation and NTT Company. They implemented the BB84 protocol with a maximum key rate of 2 kbps and QBER of 4.5%.
- A 45-km link between the Koganei and Otemachi nodes was provided by NEC, implementing the decoy state BB84 protocol with a NICT superconducting single photon detector (SSPD). The maximum key rate was 81.7 kbps with an average QBER of 2.7%.
- NTT used DPS-QKD on the longest link in the network, which was 90 km between the Koganei-1 and Koganei-2 nodes. They also used an SSPD detector and achieved a maximum key rate of 15 kbps with an average QBER of 2.3% [114].
- Three organizations from Austria, including the AIT, the Institute of Quantum Optics and Quantum Information (IQOQI), and the University of Vienna, formed a single team called "All Vienna." They presented their SECOQC QKD device. This device was based on

[10]Denotes the key rate of the final material ready for use and stored in the storage reservoir.

Table 4. Tokyo UQCC QKD Network - Brief Summary

Project year	2010
Number of nodes	6
QKD network type	Trusted repeater
Max. key rate[11]	304 kbps over 45 km
The most common protocol used	BB84, BBM92
Key references	[38, 114]

entanglement of the QKD BBM92 protocol, which was placed between the Koganei-2 and Koganei-3 nodes with a maximum key rate of 0.25 kbps.

- Toshiba Research Europe Ltd. demonstrated their decoy-state BB84 system with self-differencing avalanche photodiodes (SPAPDs) between the Koganei-2 and Otemachi-2 nodes on a 45-km link. The maximum key rate was a record 304 kbps with an average QBER of 3.8%. This was by far the highest sustained QKD bit rate produced to date.
- Finally, a 13-km link between the Otemachi and Hongo nodes was provided by idQuantique from Switzerland, making use of the SARG04 protocol from their commercial *Cerberis* solution. The maximum key rate was 1.5 kbps.

The Tokyo UQCC QKD network followed a similar three-layer network architecture based on the trusted repeater approach as it was implemented in the SECOQC project. The main difference was the use of a Key Management Server (KMS) for centralized management. The Tokyo QKD network attempted to test a government-chartered network scenario, which often has a central dispatcher or central data server. The KMS was installed in Koganei-1, Koganei-2, Otemachi-1, and Otemachi-2. All nodes implemented Key Management Agents, whose main task was to save the key material and store link statistical data, such as QBER and key generation rate. Later, these statistical data were forwarded to the KMS, which coordinated with all the links in the network [38].

5.3.1 Summary. In October 2010, a live demonstration of secure TV conferencing, eavesdropping detection, and QKD link rerouting on the Tokyo UQCC QKD network was performed. Layer 2-VPN encryption with OTP between the Otemachi-2 and Koganei-1 nodes was established. Two routes were used to demonstrate the routing algorithm when the links were attacked by the eavesdropper. The KMS detected the attacks because of an increase in the QBER and rerouted the communication through a spare link.

As noted in Table 4, the Tokyo QKD network showed that QKD technology can reach speeds of several hundred bits per second. The network also confirmed communication capabilities in QKD link distance, achieving a record link of 90 km between the Koganei-1 and Koganei-2 nodes [58]. However, what sets this network apart is the introduction of a hierarchical view into the organization of QKD networks. The key management servers implement a management layer and have complete insight into the state of the QKD network in their domain. Organization in this manner has brought the QKD network closer to the SDN perspective discussed in Section 7.

5.4 QKD Networks in China

China has been constructing QKD networks on a national scale. These efforts started by constructing testbed metropolitan QKD networks in Hefei, where a three-node network [115] and five-node network [71] were constructed in 2009 and 2010, respectively. Other efforts to construct fiber-based

[11]Denotes the key rate of the final material ready for use and stored in the storage reservoir.

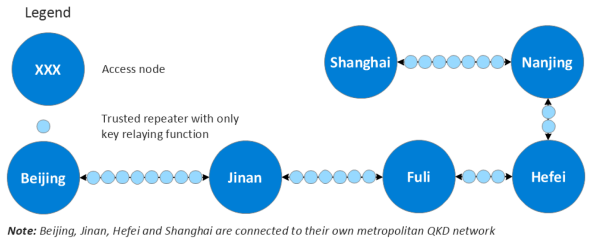


Fig. 11. Topology of the Beijing-Shanghai backbone QKD link.

QKD networks have been reported in References [116–119], and a satellite-based QKD network is also being formed [24]. This section provides an overview of these developments by looking at some recently constructed fiber-based networks.

5.4.1 Beijing-Shanghai Backbone QKD Network. In September 2017, the 2,000 km Beijing-Shanghai backbone QKD network commenced operation [120]. To date, it is the longest QKD network in the world. The project is led by the University of Science and Technology of China (USTC). Other participants include China Cable Television Network Co., Shandong Academy of Information & Communication Technology, Industrial and Commercial Bank of China (ICBC), Xinhua Financial Information Exchange, and others. The network was completed in September 2016 and was tested for one year before commencing operation.

The backbone network consists of 32 physical nodes linearly connected by QKD links (Figure 11). Among these nodes, Beijing, Jinan, Fuli, Hefei, Nanjing, and Shanghai are the access points, while the rest are trusted repeater nodes. The backbone network has 135 links in total. Two to eight multiple QKD links lie between adjacent nodes. To conserve fiber resources, the network uses quantum wavelength division multiplexing technology, which combines four quantum channels into a single fiber. The network rents dark fibers deployed by China Cable Television Network Co. The distance between adjacent nodes along the backbone line varies from 34 km to 89 km, with fiber loss varying from 7.26 dB to 22.27 dB.

The backbone network deploys the QKD devices provided by QuantumCTek Co. The device implements a polarization-coding-based decoy state BB84 protocol. Some of the devices integrate the up-conversion single photon detection technique and thereby achieve a 25% single photon detection rate.

The backbone network is designed to function as a high bandwidth channel that feeds quantum keys between metropolitan and QKD networks located in different cities. Up to now, the backbone network has been connected to the metropolitan QKD networks already established in Beijing, Shanghai, Jian, and Hefei. A wide area QKD network has been thus formed and provides end-users, including banks, government agencies, and large enterprises, with versatile security services [121].

In November 2018, an extension of the Beijing-Shanghai backbone network was completed by establishing a backbone QKD link between Wuhan and Hefei. The purpose was to connect the Wuhan metropolitan QKD network to the backbone network. The Wuhan-Hefei backbone line is operated by CAS Quantum Network Co. In the long term, the backbone network will be further extended to cover a wider area of China.

5.4.2 Jinan Government Private QKD Network. The Jinan government private QKD network commenced construction in April 2017 and was completed in August 2017. The network covers an 8,000 km^2 area of the city and consists of 32 nodes, including a centralized control station node, eight trusted repeater nodes, and 23 end-user nodes. QuantumCTek Co., Ltd provides the QKD systems and the network design solutions, while China Union Shandong Branch provides

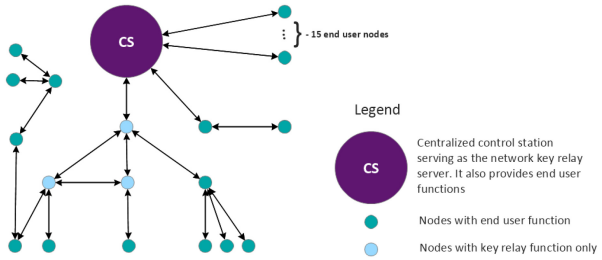


Fig. 12. Topology of the Jinan QKD Network.

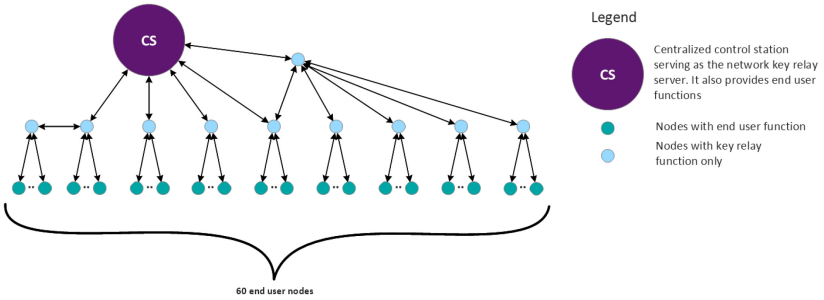


Fig. 13. Topology of the Wuhan metropolitan area QKD Network.

the fiber resources [122, 123]. The network has 33 QKD links in total (Figure 12). The length of the links varies from 1.7 km to 64.7 km, with the fiber loss varying from 1.48 dB to 25.2 dB. The quantum signals are transmitted through dark fibers provided by China Union Shandong Branch. The network deploys QKD systems implementing the polarization-coding- based decoy state BB84 protocol. All systems are provided by QuantumCTek.

The network adopts a salable, self-built service channel, which provides secure data transmission services and a minimum bandwidth of 512 Mbps. The Jinan private network integrates VoIP telephone and video conferencing services supplied with quantum keys. The security service is accessed through repeaters that implement an IPSec VPN protocol supplied with quantum keys. The network supports the OTP and several other symmetric encryption algorithms. The typical key refresh rate of symmetric encryption algorithms is once per second [124].

5.4.3 Wuhan Metropolitan Area QKD Network. The Wuhan metropolitan area QKD network was constructed in 2017 from January to December. The network consists of one command center, one centralized control station, 10 trusted repeater nodes, and 60 end-user nodes (Figure 13).

The network has 74 QKD links in total. The centralized control station and two central trusted repeater nodes are interconnected to form a network ring. Their connections adopt a dual-link structure (two QKD links are established between every other node). The longest QKD link was 16.5 km, and the optical channel loss incurred by the fiber, WDM device, and optical switch was a maximum of 14.6 dB over 6.7 km. This high loss largely results from the complex metropolitan fiber environment. The key rate of the QKD links ranges from 2.8 kbps to 141 kbps. The QKD systems are provided by QuantumCTek [125].

One of the network's features is classic quantum WDM technology [126], which integrates the classic service signal, quantum signal, and classic QKD post-processing signal into a single fiber. The security service is accessed via an encryption repeater that implements an IPSec VPN protocol

supplied with quantum keys. The typical key refresh rate of the symmetric encryption algorithms is once every five seconds.

5.4.4 Hefei, Chaohu, and Wuhu Wide Area QKD Network. A QKD wide area network connecting the cities of Hefei, Chaohu. and Wuhu (HCW) in China was reported in 2014 in Reference [119]. The entire HCW QKD network, which has a complete technical description available, operated for more than 5,000 hours from 21 December 2011 to 19 July 2012 and was installed in the Anhui provincial telecommunications network of China Mobile Ltd., with over 150 km of coverage area.

Thirteen QKD devices over nine nodes were employed in this network [119]. The HCW wide area network consists of two metropolitan networks: the Hefei QKD network, which has five nodes [116, 117], and the Wuhu QKD network [118], which has three nodes. These two networks were connected with an intercity QKD link, which combined Hefei and Wuhu metropolitan area QKD networks through a trusted repeater node at the Chaohu Branch of China Mobile Ltd. [119].

The network deployed QKD systems that implement the phase-coding-based decoy state BB84 protocol. The maximum key rate in the HCW QKD network was 16.15 kbps between the West Campus and North Campus nodes over a 3.1 km link connected to an optical switch located in the Campus Library [119].

5.4.5 Networking Strategies. The Beijing-Shanghai backbone QKD network and several other metropolitan area QKD networks employ a number of networking strategies to improve the performance and robustness of the network:

- Some metropolitan area networks adopt a ring topology in the network's design to improve its disaster tolerance.
- Backbone connections adopt a multiple parallel link networking strategy to improve bandwidth and the network's stability.
- Some core nodes such as the centralized control stations deploy backup devices that reduce the probability of system service interruption caused by a single point of failure.

5.4.6 Network Key Routing. Key routing in the Beijing-Shanghai QKD backbone network, Jinan government-private QKD network, and Wuhan metropolitan area QKD network uses a client-server architecture to maximize channel utilization and provide on-demand quantum keys to end-users.

The centralized control station of each network implements a key routing server that is in charge of managing the routing table for each network node. Based on information collected from the network (the running status of the QKD links, the remaining key storage capacity, and other information), the routing table of each node is periodically updated. The updated routing tables are exchanged with other network nodes to provide information about suitable paths until the next update [127].

The key routing server supports multiple queuing strategies adapted to different network topology structures. In the case of an emergency fault, such as the failure of the key management machine or unavailability of the key, the node device actively reports the event to the routing server. The server then recalculates routing tables for affected nodes. In the Beijing-Shanghai backbone network, key routing is managed by dividing the network into multiple sub-networks. Each sub-network adopts the above client-server structure with the key routing server located at the access nodes [127, 128].

5.4.7 Summary. With a 2,000-km link connecting Shanghai and Beijing and metropolitan networks in Hefei and Jinan, China is currently leading the QKD race in terms of practical developments [129]. In their described methodologies, unique approaches in implementing existing and

Table 5. QKD Networks in China - Brief Summary

Network	Beijing-Shanghai	Jinan	Wuhan	HCW
Project year	2014–2017	2017	2017	2017
Number of nodes	32	32	71	9
QKD network type	Trusted repeater	Trusted repeater	Trusted repeater	Trusted repeater
Max. key rate	250 kbps over 43 km[12]	64.7 kbps over 32 km	141 kbps over 16.5 km	16.15 kbps over 3.1 km
The most common protocol used	Decoy state BB84	Decoy state BB84	Decoy state BB84	Decoy state BB84
Key references	[116, 117, 119]	[122–124]	[125]	[116–119]

available technology can be seen in these QKD networks. However, in addition to using discrete QKD protocols that guarantee high performance but require expensive single-photon detectors, experiments that rely on continuous-variable and measurement-device-independent (MDI) QKD have also been reported. For CV-QKD, results of 5.77 kbps over 50 km have been achieved [73, 130]. The experiments with MDI-QKD have resulted the higher rates (up to the channel attenuation): 98.2 kbps over 49.1 km and up to 1 Mbps over a dozen kilometers' distance [131]. Moreover, QKD systems based on MDI can work efficiently not only in symmetric channels with similar losses, but even with channels with asymmetric losses [132]. The optimization methods [133] can extend the secure transmission distance in such MDI-QKD implementations by more than 20–50 km in standard telecom fiber. A brief summary of the networks described above with publicly available references is listed in Table 5.

Not discussed here for reasons of space, it is, however, important to mention that China is leading in the field of space-oriented quantum technology. In 2017, the 640-kg "Micius" satellite was launched [134]. In a 273-second satellite pass and using a 1-m telescope on the ground, sifted key rates of about 12 kbps at 645 km to 1 kbps at 1,200 km were expected [135]. After post-processing, 1.1 kbps for the secure key was obtained.

6 QUALITY OF SERVICE IN QKD NETWORKS

6.1 Similarities between QKD and Mobile Ad Hoc Network Technologies

The specific QKD issues and constraints described above pose significant challenges in QKD network design. However, analysis of the characteristics of QKD networks has shown similarities in Reference [136] to Mobile Ad Hoc Networks (MANET) and Vehicular Ad Hoc Networks (VANET) [137–139].

The main characteristics of QKD technology from a simple point of view can be listed:

- QKD links such as those described above are always implemented in point-to-point behavior and can be roughly characterized by two features: limited distance and key rate (exponentially) decreasing with distance. Links may become unavailable when there is not enough key material or when the public channel is congested. This is similar to Wi-Fi links, which are limited in range and whose communication speeds depend on the user's distance from the transmitter's antenna.
- One of the main features of current QKD networks is the lack of a quantum repeater (Section 3.2), and communication is therefore usually performed on a hop-by-hop basis.

[12]This key rate is achieved by multiplexing four QKD systems in parallel between the two nodes.

In MANET networks, communication takes place on a hop-by-hop basis, and mobile nodes are typically powered with energy-aware solutions such as batteries. The nodes connect themselves in a self-organizing, decentralized manner with no authority in charge of controlling and network management. The main drawback of MANET networks is the unpredictable mobility of nodes, which can often lead to unstable routing paths [114]. The amount of battery power and the mobility of MANET nodes can be easily linked to the amount of key material in QKD key storage. The limited range of wireless links is much like the limitations in the length of a QKD link. The lack of dedicated network infrastructure (such as routers) is another similarity between these two technologies. The poor mobility of QKD nodes, however, makes it similar to VANET technology, in which communication takes place along a predefined path.

Although at first glance MANET and QKD networks have nothing in common, a simple analysis of the features of these networks reveals their similarity. What clearly distinguishes these two networks, though, is their purpose. MANET networks are designed for fast and straightforward communication in situations where pre-existing installed infrastructure is not available (e.g., search-and-rescue operations during natural disasters or in war zones). By contrast, the primary goal of QKD is to provide ITS communication. This may have a significant impact when choosing network solutions, since a solution required in one situation may not be suitable in another. For example, consider routing solutions based on network flooding. QKD networks rely on the assumption that all nodes are trusted when communication is performed in a hop-by-hop or key-repeating manner [32, 39], and by following this assumption strictly, an eavesdropper is restricted to attacking QKD links only. Because of the nature of QKD, the eavesdropper is not able to gain any information about the key being transported through the link, but service may be denied to disable the communication. Although results have been obtained by combining multiple paths to establish secure key material [27, 82], it is thought that the amount of routing information being sent to the nodes should be reduced to a minimum. To prevent a denial-of-service attack, no node (except source and destination) in a network should know the routing request. Therefore, the number of broadcast packets should be minimized. Furthermore, considering the primary objective of QKD, which is to provide ITS communication, routing packets must be either authenticated and encrypted or at least authenticated [140]. This means that the number of routing packets in the network needs to be minimized (routing overhead) concerning the material to be preserved for the protection of data, which is the primary goal of secure communication. From this, it follows that protocols based on flooding are not preferred in QKD networks.

6.2 Routing Protocols

In previously deployed QKD networks, emphasis was placed on quantum channels. The public channel, though, was largely neglected and assumed that it was somehow achievable without any difficulties. The prioritization of network traffic and signaling protocols were ignored, and the solutions in existing conventional networks have consequently been modified for the needs of QKD networks. The first such solution, which is based on modifying the well-known Open Shortest Path First (OSPF) routing protocol [98], was implemented in the DARPA BBN QKD network built in 2004 in the US [92]. Instead of using the routing hop-count metric, a modified OSPFv2 protocol was used to determine link quality according to the amount of key material in key storage. As discussed in Section 5.1.4, the modified version of the OSPFv2 does not take into account the status of the public channel [99].

A similar approach was offered in Reference [141], where the author proposed using unencrypted and non-authenticated communication to disseminate OSPFv2 routing packets. Obviously, this kind of network is easy prey for an eavesdropper with unlimited resources at their disposal, especially in terms of passive eavesdropping [76]. Since the described solution is based on the use

of key material in key storage as a routing metric, it cannot provide efficient routing because of a lack of information about the state of the public channel.

In the SECOQC network, another modified version of the OSPFv2 protocol was introduced [28, 33]. It was based on a local load-balancing policy calculated as the ratio of the number of transmitted bits over a period of time. As discussed in Section 5.2.3, a solution such as this does not consider the available amount of key material, which means that the algorithm may choose a path with insufficient key material for data transmission.

When the Chinese HCW QKD network was developed, a Quantum Key Reservation Approach (QKDRA) based on the IntServ model was applied [142, 143]. OSPFv2 is used to find the path from the source to the destination node. After the path is determined, the source node issues a key reservation request to all nodes in the path. After receiving a request, the intermediate node responds with a key reservation result message. Finally, the destination node determines the possibility of establishing the connection. Since OSPFv2 focuses on finding the shortest path, hence the name, solutions presented in References [142, 143] find the shortest path between the source and destination and reserve a sufficient amount of key material on a selected path. Note that this path may not be optimal. More specifically, the path is the shortest, but it may not be adequate in terms of QoS. It is known that minimum hop-count (shortest) routing typically finds routes with a significantly lower throughput than the best available [144], since it does not consider other link parameters. OSPFv2 in its original form does not consider QoS constraints; therefore, it cannot guarantee that traffic on the selected path will be adequately served. Reservation of resources on the quantum channel, in this case, does not provide a gain, since the path for the public channel may be inappropriate. However, even an extended version of OSPFv2 that includes QoS constraints [145] may not be optimal for QKD networks. Implementation of OSPFv2 in this way can find the path that has the best characteristics of the public channel but does not consider the parameters of the quantum channel.

Yang proposed using the Dijkstra algorithm to identify multiple paths but without considering the status of the public channel [146]. The idea is to use thresholds to exclude links that have a lower key material amount and periodically flood routing details, such as the amount of available key material.

The impact of public channel states on the key rate can be found in Reference [147]. This study shows that a public channel should not be excluded in route calculations, since the performance of the public channel affects the quantum channel and vice versa. Therefore, novel metrics are introduced to uniquely describe the state of the public and quantum channels as well as the overall QKD link [147, 148]. With the aim of minimizing key consumption, network flooding should be avoided and a single-layer network organization and Greedy Perimeter Stateless Routing Protocol for QKD networks (GPSRQ) was introduced [136]. The GPSRQ routing protocol uses distributed geography and reactive routing to achieve high-level scalability. It is equipped with a caching mechanism and detection of returning loops, enabling forwarding while minimizing key material consumption. However, GPSRQ applications are limited to planar topologies only, because geographic routing in networks with non-planar topologies are not able to quickly determine the shortest path, leading to unnecessary forwarding and increased consumption of scarce key material.

Routing in QKD networks depends primarily on the architecture of the network organization (hierarchical or distributed architecture, overlay or single stack network, hop-by-hop or key-repeater networking). Unlike conventional networks, routing solutions in QKD networks need to take into account both channels of the QKD link. Based on the requirement to minimize key consumption, it is necessary to reduce the amount of routing packets that have to be encrypted and authenticated or at least authenticated to avoid active and passive eavesdropping QKD network attacks [28, 140].

Considering the efforts to extend the QKD network to metropolitan areas, which involves a significant number of network nodes, a hierarchical organization was considered in previously implemented networks [42, 125, 149–151]. This approach, which is based on a key management layer, converges to a software-based network paradigm and is discussed in more detail in Section 7.

7 QKD SOFTWARE DEFINED NETWORKING

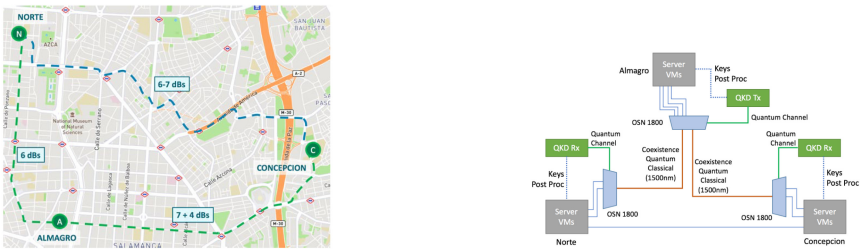
A more evolutionary strategy for adopting QKD in transport networks is taking advantage of the latest developments in networking technologies, more specifically, in network management. Software-defined networking (SDN) [152, 153] allows the control (management) and data (forwarding) planes to be separated. Its popularity has increased in both academic and industrial spheres since its creation in 2008. SDN allows the integration of new technologies and services at a faster pace while enabling centralized management and optimization based on network programmability and configurability principles. Although the approach for SDN has changed over the years from OpenFlow-based device programmability towards open and standard interfaces, this transformation has helped network operators increasingly adopt SDN in their systems to reduce the time-to-market and vendor lock-in.

An SDN network is conceptually organized into three layers. The control and management layer knows the status of the entire network and can optimize its behavior through a centralized entity known as the SDN controller. The controller identifies the capabilities of the devices installed in the infrastructure layer through a set of standard mechanisms (southbound interface). It also knows the requirements of the different applications running in a network through standard interfaces (northbound interface). Its role is to optimize resources and provide the means for devices and services to fulfill their tasks. A QKD system installed in infrastructure can export its requirements to the controller so it can create a specific path with the required optical characteristics (i.e., maximum tolerated noise, attenuation, etc.) to connect the emitter to the receiver (either on a single or multi-hop path) and satisfy an application's requirements. This allows an unprecedented means of creating a fully integrated classic/quantum network and genuinely zero-configuration QKD devices that can be directly plugged into a standard telecommunications network.

Before this technology, demonstrations required either an ad hoc, separate network just for the quantum channel (i.e., typically a network of dark fibers) or specific network modifications for each link [154, 155]. These are very expensive and entirely orthogonal deployments for common telecommunications activities, in which devices are expected to work out of the box and share the fiber with many other conventional communications channels. For QKD to become mainstream, it is critically important that QKD systems follow the trends and architectures used in the transport network segment.

Other projects and demonstrations have shown initial steps towards automating QKD networks. In References [156, 157], the authors implemented a mechanism for automating the switching of a quantum channel between a transmitter and two simulated receivers using optical cross-connect switches that were OpenFlow-enabled. In this sense and despite the enabler, in this case, being a software-defined optical network (SDON) controller, the research focused more on applying secure virtual machine migrations in a distributed data center scenario.

The most advanced contribution towards Software-Defined QKD Networks was presented in References [158–160] (Figure 14(b)). Three production sites in the Telefonica in Spain network were connected. The proposed architecture and demonstrations aimed to demonstrate the technological maturity of QKD systems for integration into production networks. The CV-QKD systems used for the trial were implemented so they could be managed and optimized with software processes and were robust enough to coexist with traditional communications channels. The software integrated the first version of an SDN interface defined by the Industry Specification Group (ISG)



(a) Map with the losses in each link and logical representation of the elements involved in the field trial.

(b) Three of Telefonica's production facilities are connected in a ring.

Fig. 14. Map and topology of the Madrid SDQKD Network.

for QKD at the European Standards Telecommunications Institute (ETSI). With this interface, the QKD systems and the key delivery processes are centrally managed by an SDN controller, allowing quantum channels (via optical switches) to be dynamically instantiated, multi-hop associations to be created, and demands for keys from external applications to be identified. This setup was also designed so any control and data channel could integrate QKD-derived keys to secure communications related to either the QKD network or traditional telecommunications services running in the production network.

QKD can also be seen as an additional security layer for transport networks. The integration of QKD in SDN is a mutually beneficial relationship, since QKD-derived keys can be used to secure the different layers of a transport network. Apart from the demonstration conducted in Reference [157] in which the encryption algorithm (AES) was used to provide security, the authors in Reference [161] showed how existing security protocols used in the control plane could integrate quantum cryptography in a seamless evolutionary manner without affecting current schemes. Being composable in both cryptosystems (QKD and traditional or even post-quantum schemes), the security of the proposed system brings the best of both: certification from traditional schemes is still applicable to the hybrid system, while the security of the resulting solution is the highest possible, because breaking the final key means both cryptosystems must be compromised. This solution is deployed in control channels orchestrating an SDN controller and a network function virtualization (NFV) architecture through SSH and TLS protocols.

The SDN-based experiment of monitoring and mitigation of physical layer attacks was reported [162]. Real-time monitoring of QBER and the secret key rate was used to recalculate routes for the quantum channel establishment.

Other cases have focused more on data plane security and service establishment. Marksteiner presented an integration of QKD-derived keys in IPSec channels, focusing its research on the security and scalability of the solution depending on the service throughput [163]. In addition to this research, the approach reported in Reference [164] focuses on service automation for encrypted channels in an end-to-end network. Automation was suggested for data center scenarios (implementing extensions in OpenFlow) and for transport segments (using MPLS and NETCONF for configuration). This was integrated into virtual network functions implementing the extensions and the security channel using IPSec, as in Reference [163]. Mavromatis demonstrated the usage of QKD for energy-efficient SDN management of Internet of Things devices [165]. We also point out experiments with the use of SDN to control the WDM organization of QKD links [156, 166–168] as well as the use of machine learning (ML) models for the prediction of Ch-QKD quality in QKD-DWDM networks with increasing efficiency of SDN-enabled optical networks [169].

In a broad QKD network where multiple QKD tenants share the same underlying infrastructure, addressing the secure-key assignment is essential for efficient network managment. Cao proposed the SDN-based secret-key rate sharing approach using heuristic algorithm using simulations [170]. The multi-tenant organization can be served using Key as a Service (KaaS) approach where key pools (KP) defined at the control layer of SDN hierarchy mapped to virtual key pools using RESTful API at the application layer.

These results show how SDN must be seen as a technological enabler for QKD's integration into transport networks. At the same time, QKD also benefits the network, since it implements an additional ITS layer for critical infrastructures. This integrative approach allows QKD systems to be smoothly integrated into the network and for QKD to be commercialized at different service levels (self-healed network infrastructures, end-to-end services at different OSI layers, etc.).

8 CONCLUSION

Quantum cryptography is an attractive cryptographic technology that has received the attention of various organizations in academic and industrial communities. In recent years, notable progress in the development of optical equipment has been reflected through a number of successful demonstrations of QKD technology. These demonstrations show great achievements in quantum cryptography and highlight the practical difficulties that still need to be resolved.

We provide a summary of the major key points related to QKD networks in Table 6. Trusted repeaters are necessary to extend the secure transmission distance of quantum channels. Solutions for integrating QKD networks into existing optical communications networks are currently the hot topic in optical research. Real quantum cryptography networks employed by end-users for real-life information transfer applications will be the next milestone. In terms of the industry, standards for security evaluation, production, and application of QKD are already being defined [189, 190].

Currently, a person finding himself in a QKD laboratory and asking for the maximum achievable key rate will receive a response with a question about the distance she/he is looking to cover. As mentioned in Section 3, one of the main drawbacks of QKD links is length limitations. However, the networks discussed in this document demonstrate the significant development in optical equipment in recent times. In 2002, QKD systems achieved a key rate of 1 kbps [29], which was used in the DARPA QKD network. In 2007 in SECOQC, this key rate increased tenfold [37], while in 2011 in the Tokyo QKD network, a key rate of 300 kbps was achieved [38]. This key rate was sufficient to establish a video conference secured with an OTP cipher provided by QKD. It is also interesting to compare the length of links in these networks. The maximum length in the DARPA QKD network was a 29-km connection via the optical switch between Harvard and Boston Universities [91]. In SECOQC, the maximum length of the QKD link was 82 km between the BREIT and St. Pölten nodes [37]. In Tokyo, the maximum distance was a record 90 km between the Koganei-1 and Koganei-2 nodes [171]. In Hefei-Chaohu-Wuhu (HCW) in China, the maximum distance was 85.1 km via the HCW intercity link between Hefei and Chaohu [119, 191].

It is reasonable therefore to expect a higher key rate and longer distances in the coming years. Since optical quantum repeaters are predicted to become available for practical use in the future [57], QKD networks are currently implemented solely through the Trusted Repeater Approach (TRA). TRA is essential for overcoming the distance limitations between QKD links and in providing routing in QKD networks. TRA, however, has several restrictions that will have to be resolved if a QKD network is to be applied in everyday life and integrated with conventional IP networks. One means for widespread application of QKD technology is integration with telecommunications networks using an approach such as SDN-QKD.

Table 6. Summary of Major Key Points of QKD Networking

Work Area	Key References	Key Points
QKD link	[26–28, 59–61]	• The maximum distance of a link decreases with link length • The range of QKD link is roughly limited to 100 km while key rate is limited to a few tens or hundreds of kbps • Key storages used at both endpoints of the corresponding link and gradually filled with new key material • Lack of quantum repeaters in practice
Quantum Networks	[29, 71, 76–78, 83–86]	• Switched fully optical QKD network with limited length • Trusted Repeater networks assuming trusted/invulnerable nodes can increase the QKD range (key repeat or hop-by-hop) • Multipath communication to mitigate the risk of eavesdropping and increase key rates
2002 USA DARPA BBN QKD Network	[14, 29, 92]	• The first QKD network demonstration with 10 nodes in total • Demonstration of switched andTrusted Repeater QKD networking • Maximal key rate: 400 bps; Maximal distance of a single link: 29 km • BB84 protocol mostly used; BBN Protocol Suite • The first modification of IPsec and OSPFv2 for key usage and network routing
2004 EU SEOCQC QKD Network	[28, 33, 37, 106, 113]	• Interoperability of different QKD techniques with six nodes in total • Laid the groundwork for a hop-by-hop networking • Maximal key rate: 3.1 kbps; Maximal distance of a single link: 82 km • BB84 and BBM92 protocols mostly used; Q3P Protocol Suite • Extension of OSFPv2 routing
2010 JAPAN TOKYO UQCC QKD Network	[38, 171]	• Introduction of Key Management Servers (KMS) • Hierarchical management of a network of six nodes in total • Maximal key rate: 3.1 kbps; Maximal distance of a single link: 33 km • BB84 and BBM92 protocols mostly used;
2014 CHINA QKD Networks	[116–119, 122–125]	• Multiple QKD networks deployed: Jinan, Wuhan, Hefei-Chaohu-Wuhu • 2,000 km Beijing-Shanghai longest key-repeater network with 32 hops • Maximal key rate: 250 kbps; Maximal distance of a single link: 43 km • Decoy state BB84 protocol mostly used; OSPFv2 + RSVP modifications
QKD Quality of Service	[99, 136, 144, 164, 172–175]	• Similarities between Trusted Repeater QKD and mobile ad hoc networks • Routing should consider public and quantum channels state • Greedy Perimeter Stateless Routing QKD protocol; OSPFv2 variations • RSVP reservation of key material (QRKA); QSIP in-line signaling
QKD Simulators	[31, 176–181]	• QKD channel performance simulations and QKD network simulations • SimulaQron - API for the implementation of quantum network stack • QCircuit and Quirk - quantum logic circuits simulations • OptiSystem QKD simulations • qkdX OMNET++ performance analysis of practical QKD systems • QKDNetSim - QKD network simulation model based on NS-3
QKD Software Defined Networking	[156, 158, 160, 166–168, 170]	• Centralized network management via SDN controller • SDN centralized monitoring of network state and mitigation of attacks • SDN efficient control of WDM QKD links organization • Key as a service approach in a multi-tenant SDN network • The primary technology for integration of QKD into telecom-based networks
QKD Standards	[10, 182–188]	• ETSI - industry-oriented standardization; IEEE-SA - general standards; • ISO/IEC JTC 1/SC 27 - working standards on security requirements and evaluation of QKD performances; IETF - standardization of QKD protocols; • ITU-T SG 13 - standards regarding cloud computing and trusted network infrastructure; ITU-T SG 17 standards relating to QKD network architectures

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their suggestions on the clarity and coverage of topics in the article. The discussion was strongly improved through their careful reading and constructive input.

REFERENCES

[1] Ueli M. Maurer. 1993. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theor.* 39, 3 (1993), 733–742. DOI: http://dx.doi.org/10.1109/18.256484

[2] Peter W. Shor. 1994. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. IEEE Computer Society Press, 124–134. DOI: http://dx.doi.org/10.1109/SFCS.1994.365700

[3] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Buell, Brian Burkett, Yu Chen, Zijun Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, Edward Farhi, Brooks Foxen, Austin Fowler, Craig Gidney, Marissa Giustina, Rob Graff, Keith Guerin, Steve Habegger, Matthew P. Harrigan, Michael J. Hartmann, Alan Ho, Markus Hoffmann, Trent Huang, Travis S. Humble, Sergei V. Isakov, Evan Jeffrey, Zhang Jiang, Dvir Kafri, Kostyantyn Kechedzhi, Julian Kelly, Paul V. Klimov, Sergey Knysh, Alexander Korotkov, Fedor Kostritsa, David Landhuis, Mike Lindmark, Erik Lucero, Dmitry Lyakh, Salvatore Mandrà, Jarrod R. McClean, Matthew McEwen, Anthony Megrant, Xiao Mi, Kristel Michielsen, Masoud Mohseni, Josh Mutus, Ofer Naaman, Matthew Neeley, Charles Neill, Murphy Yuezhen Niu, Eric Ostby, Andre Petukhov, John C. Platt, Chris Quintana, Eleanor G. Rieffel, Pedram Roushan, Nicholas C. Rubin, Daniel Sank, Kevin J. Satzinger, Vadim Smelyanskiy, Kevin J. Sung, Matthew D. Trevithick, Amit Vainsencher, Benjamin Villalonga, Theodore White, Z. Jamie Yao, Ping Yeh, Adam Zalcman, Hartmut Neven, and John M. Martinis. 2019. Quantum supremacy using a programmable superconducting processor. *Nature* 574, 7779 (Oct. 2019), 505–510. DOI: http://dx.doi.org/10.1038/s41586-019-1666-5

[4] Charles H. Bennett, Gilles Brassard et al. 1984. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Vol. 175. 8. Retrieved from http://www.cs.ucsb.edu/ chong/.

[5] Mark N. Wegman and J. Lawrence Carter. 1981. New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.* 22, 3 (1981), 265–279. DOI: http://dx.doi.org/10.1016/0022-0000(81)90033-7

[6] Dominic Mayers. 2001. Unconditional security in quantum cryptography. *J. ACM* 48, 3 (2001), 351–406. DOI: http://dx.doi.org/10.1145/382780.382781

[7] Peter W. Shor and John Preskill. 2000. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* 85, 2 (July 2000), 441–444. DOI: http://dx.doi.org/10.1103/PhysRevLett.85.441 arxiv:quant-ph/0003004.

[8] Laszlo Gyongyosi, Sandor Imre, and Hung Viet Nguyen. 2017. A survey on quantum channel capacities. *IEEE Commun. Surv. Tutor.* c (2017), 1–58. DOI: http://dx.doi.org/10.1109/COMST.2017.2786748

[9] Vicente Martin, Jesus Martinez-Mateo, and Momtchil Peev. 2017. Introduction to quantum key distribution. In *Wiley Encyclopedia of Electrical and Electronics Engineering*. John Wiley & Sons, Inc., Hoboken, NJ, 1–17. DOI: http://dx.doi.org/10.1002/047134608X.W8354

[10] R. Alleaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Langer, N. Lutkenhaus, C. Monyk, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger. 2014. Using quantum key distribution for cryptographic purposes: A survey. *Theoret. Comput. Sci.* 560, P1 (Dec. 2014), 62–81. DOI: http://dx.doi.org/10.1016/j.tcs.2014.09.018

[11] Slavisa Aleksic, Dominic Winkler, Gerald Franzl, Andreas Poppe, Bernhard Schrenk, and Florian Hipp. 2013. Quantum key distribution over optical access networks. In *Proceedings of the 18th European Conference on Network and Optical Communications & 8th Conference on Optical Cabling and Infrastructure (NOC-OC&I'13)*. 11–18. DOI: http://dx.doi.org/10.1109/NOC-OCI.2013.6582861

[12] K. Patel, J. Dynes, I. Choi, A. Sharpe, A. R. Dixon, Z. Yuan, R. Penty, and A. Shields. 2012. Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Phys. Rev. X* 2, 4 (Nov. 2012), 41010. Retrieved from http://link.aps.org/doi/10.1103/PhysRevX.2.041010.

[13] Sima Bahrani, Mohsen Razavi, and Jawad A. Salehi. 2018. Wavelength assignment in hybrid quantum-classical networks. *Sci. Rep.* 8, 1 (2018), 1–13. DOI: http://dx.doi.org/10.1038/s41598-018-21418-6

[14] Chip Elliott, David Pearson, and Gregory Troxel. 2003. Quantum cryptography in practice. In *Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'03)*. 227. DOI: http://dx.doi.org/10.1145/863981.863982

[15] Andreas Poppe, Momtchil Peev, and Oliver Maurhart. 2008. Outline of the SECOQC quantum-key-distribution network in Vienna. *J. Quant. Inf.* 6, 2 (Apr. 2008), 10. DOI: http://dx.doi.org/10.1142/S0219749908003529

[16] Robert J. Runser, Thomas Chapuran, Paul Toliver, Nicholas A. Peters, Matthew S. Goodman, Jon T. Kosloski, Nnake Nweke, Scott R. McNown, Richard J. Hughes, Danna Rosenberg, Charles G. Peterson, Kevin P. McCabe, Jane E. Nordholt, Kush Tyagi, Philip A. Hiskett, and Nicholas Dallmann. 2007. Progress toward quantum communications networks: Opportunities and challenges. In *Optoelectronic Integrated Circuits IX*. 64760I–64760I–15. DOI: http://dx.doi.org/10.1117/12.708669

[17] T. Schmitt-Manderbach, H. Weier, M. Furst, R. Ursin, F. Tiefenbacher, Th. Scheidl, J. Perdigues, Z. Sodnik, Ch. Kurtsiefer, J. Rarity, A. Zeilinger, and H. Weinfurter. 2007. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. In *Proceedings of the European Conference on Lasers and Electro-Optics and the International Quantum Electronics Conference*. IEEE, 1–1. DOI: http://dx.doi.org/10.1109/CLEOE-IQEC.2007.4386755

[18] Sebastian Nauerth, Florian Moll, Markus Rau, Christian Fuchs, Joachim Horwath, Stefan Frick, and Harald Weinfurter. 2013. Air-to-ground quantum communication. *Nat. Photon.* 7, 5 (Mar. 2013), 382–386. DOI: http://dx.doi.org/10.1038/nphoton.2013.46

[19] Erik Kerstel, Arnaud Gardelein, Mathieu Barthelemy, Matthias Fink, Siddarth Koduru Joshi, and Rupert Ursin. 2018. Nanobob: A CubeSat mission concept for quantum communication experiments in an uplink configuration. *EPJ Quant. Technol.* 5, 1 (2018), 1–30. DOI: http://dx.doi.org/10.1140/epjqt/s40507-018-0070-7

[20] Nedasadat Hosseinidehaj, Zunaira Babar, Robert Malaney, Soon Xin Ng, and Lajos Hanzo. 2018. Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook. *IEEE Commun. Surv. Tutor.* PP (2018), 1. DOI: http://dx.doi.org/10.1109/COMST.2018.2864557

[21] Laszlo Bacsardi. 2013. On the way to quantum-based satellite communication. *IEEE Commun. Mag.* 51, 8 (Aug. 2013), 50–55. DOI: http://dx.doi.org/10.1109/MCOM.2013.6576338

[22] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi. 2009. Some aspects on the feasibility of satellite quantum key distribution. *New J. Phys.* 11, 4 (2009), 45017. DOI: http://dx.doi.org/10.1088/1367-2630/11/4/045017

[23] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight. 2002. Ground to satellite secure key exchange using quantum cryptography. *New J. Phys.* 4, 1 (2002), 82. DOI: http://dx.doi.org/10.1088/1367-2630/4/1/382

[24] Sheng Kai Liao, Jin Lin, Ji Gang Ren, Wei Yue Liu, Jia Qiang, Juan Yin, Yang Li, Qi Shen, Liang Zhang, Xue Feng Liang, Hai Lin Yong, Feng Zhi Li, Ya Yun Yin, Yuan Cao, Wen Qi Cai, Wen Zhuo Zhang, Jian Jun Jia, Jin Cai Wu, Xiao Wen Chen, Shan Cong Zhang, Xiao Jun Jiang, Jian Feng Wang, Yong Mei Huang, Qiang Wang, Lu Ma, Li Li, Ge Sheng Pan, Qiang Zhang, Yu Ao Chen, Chao Yang Lu, Nai Le Liu, Xiongfeng Ma, Rong Shu, Cheng Zhi Peng, Jian Yu Wang, and Jian Wei Pan. 2017. Space-to-ground quantum key distribution using a small-sized payload on Tiangong-2 space lab. *Chin. Phys. Lett.* 34, 9 (2017), 1–6. DOI: http://dx.doi.org/10.1088/0256-307X/34/9/090302

[25] Alexander V. A. V. Sergienko. 2005. *Quantum Communications and Cryptography*. Vol. 2005. CRC Press. 249 pages.

[26] Miloslav Dusek, Norbert Lutkenhaus, and Martin Hendrych. 2006. Quantum cryptography. In *Progress in Optics*. Vol. 49. Elsevier, 381–454. DOI: http://dx.doi.org/10.1016/S0079-6638(06)49005-3

[27] Louis Salvail, Momtchil Peev, Eleni Diamanti, Romain Alléaume, Norbert Lütkenhaus, and Thomas Länger. 2010. Security of trusted repeater quantum key distribution networks. *J. Comput. Sec.* 18, 1 (Jan. 2010), 61–87. DOI: http://dx.doi.org/10.3233/JCS-2010-0373

[28] Christian Kollmitzer and Mario Pivk. 2010. *Applied Quantum Cryptography*. Vol. 797. Springer Science & Business Media. DOI: http://dx.doi.org/10.1007/978-3-642-04831-9

[29] Chip Elliott and H. Yeh. 2007. *DARPA Quantum Network Testbed*. Technical Report. BBN Technologies Cambridge, New York, New York. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord.

[30] Miralem Mehic, Marcin Niemiec, and Miroslav Voznak. 2015. Calculation of the key length for quantum key distribution. *Elektron. Elektrotech.* 21, 6 (Dec. 2015), 81–85. DOI: http://dx.doi.org/10.5755/j01.eie.21.6.13768

[31] Miralem Mehic, Oliver Maurhart, Stefan Rass, Miroslav Voznak, Mehic Miralem, Maurhart Oliver, Rass Stefan, and Miroslav Voznak. 2017. Implementation of quantum key distribution network simulation module in the network simulator NS-3. *Quant. Inf. Proc.* 16, 10 (Oct. 2017), 253. DOI: http://dx.doi.org/10.1007/s11128-017-1702-z

[32] Chip Elliott. 2002. Building the quantum network. *New J. Phys.* 4 (July 2002), 346. DOI: http://dx.doi.org/10.1088/1367-2630/4/1/346

[33] Mehrdad Dianati, Romain Alléaume, Maurice Gagnaire, and Xuemin (Sherman) Shen. 2008. Architecture and protocols of the future European quantum key distribution network. *Sec. Commun. Netw.* 1, 1 (Jan. 2008), 57–74. DOI: http://dx.doi.org/10.1002/sec.13

[34] Aysajan Abidin and Jan-Åke Larsson. 2011. Security of authentication with a fixed key in quantum key distribution. Retrieved from http://arxiv.org/abs/1109.5168.

[35] Christopher Portmann. 2014. Key recycling in authentication. *IEEE Trans. Inf. Theor.* 60, 7 (2014), 4383–4396. DOI: http://dx.doi.org/10.1109/TIT.2014.2317312

[36] Stefan Rass, Angelika Wiegele, and Peter Schartner. 2010. Building a quantum network: How to optimize security and expenses. *Springer J. Netw. Syst. Manag.* 18, 3 (2010), 283–299. DOI: http://dx.doi.org/10.1007/s10922-010-9162-0

[37] Romain Alleaume, Jan Bouda, Cyril Branciard, Thierry Debuisschert, Mehrdad Dianati, Nicolas Gisin, Mark Godfrey, Philippe Grangier, Thomas Langer, Anthony Leverrier, Norbert Lutkenhaus, Philippe Painchault, Momtchil Peev, Andreas Poppe, Thomas Pornin, John Rarity, Renato Renner, Gregoire Ribordy, Michel Riguidel, Louis Salvail, Andrew Shields, Harald Weinfurter, and Anton Zeilinger. 2007. SECOQC white paper on quantum key distribution and cryptography. *arXiv preprint quant-ph/0701168* (2007).

[38] Masahide Sasaki. 2011. Tokyo QKD network and the evolution to secure photonic network. In *Proceedings of the Conference on Laser Applications to Photonic Applications (CLEO'11)*, Vol. 1. OSA, Washington, D.C., JTuC1. DOI: http://dx.doi.org/10.1364/CLEO_AT.2011.JTuC1

[39] Michael Marhoefer, Ilse Wimberger, and Andreas Poppe. 2007. Applicability of quantum cryptography for securing mobile communication networks. *Long-Term and Dynamical Aspects of Information Security: Emerging Trends in Information and Communication Security*. Nova Science Publishers, 97–111.

[40] Masahito Hayashi, Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, and Shigeru Yamashita. 2007. Quantum network coding. In *Lecture Notes in Computer Science (Lecture Notes in Computer Science)*, Wolfgang Thomas and Pascal Weil (Eds.), Vol. 4393. Springer Berlin, 610–621. DOI: http://dx.doi.org/10.1007/978-3-540-70918-3 arxiv:quant-ph/0601088.

[41] Romain Alléaume, François Roueff, Oliver Maurhart, Norbert Lütkenhaus, and Ecole Nationale. 2006. Architecture, security and topology of a global quantum key distribution network. In *2006 Digest of the LEOS Summer Topical Meetings*. IEEE, 38–39. DOI: http://dx.doi.org/10.1109/LEOSST.2006.1694006

[42] Piotr K. Tysowski, Xinhua Ling, Norbert Lütkenhaus, and Michele Mosca. 2017. The engineering of a scalable multi-site communications system utilizing quantum key distribution (QKD). *Quant. Sci. Technol.* 3, 2 (2017). DOI: http://dx.doi.org/10.1088/2058-9565/aa9a5d

[43] G. Gilbert and M. Hamrick. 2000. Practical quantum cryptography: A comprehensive analysis (part one). Retrieved from http://arxiv.org/abs/quant-ph/0009027.

[44] Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. 2002. Quantum cryptography. *Rev. Mod. Phys.* 74, 1 (Jan. 2002), 145–195. DOI: http://dx.doi.org/10.1103/RevModPhys.74.145

[45] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. 2009. The security of practical quantum key distribution. *Rev. Mod. Phys.* 81, 3 (Sept. 2009), 1301–1350. DOI: http://dx.doi.org/10.1103/RevModPhys.81.1301

[46] Hoi Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. 2014. Secure quantum key distribution. DOI: http://dx.doi.org/10.1038/nphoton.2014.149

[47] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. 2019. Quantum cryptography with realistic devices. Retrieved from http://arxiv.org/abs/1903.09051.

[48] Stefan Marksteiner. 2014. *An Approach to Securing IPsec with Quantum Key Distribution (QKD) Using the AIT QKD Software*. Ph.D. Dissertation. CAMPUS 02 University of Applied Sciences, Graz, Austria. Retrieved from https://smarksteiner.files.wordpress.com/2014/05/marksteiner-an-approach-to-securing-ipsec-with-quantum-key-distribution-2014.pdf.

[49] Zhiliang Yuan, Alan Plews, Ririka Takahashi, Kazuaki Doi, Winci Tam, Andrew Sharpe, Alexander Dixon, Evan Lavelle, James Dynes, Akira Murakami, Mamko Kujiraoka, Marco Lucamarini, Yoshimichi Tanizawa, Hideaki Sato, and Andrew J. Shields. 2018. 10-Mb/s quantum key distribution. *J. Lightw. Technol.* 36, 16 (2018), 3427–3433. DOI: http://dx.doi.org/10.1109/JLT.2018.2843136

[50] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten. 2009. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.* 11, 7 (2009), 075003. DOI: http://dx.doi.org/10.1088/1367-2630/11/7/075003

[51] Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti et al. 2015. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat. Photon.* 9, 3 (Feb. 2015), 163–168. DOI: http://dx.doi.org/10.1038/nphoton.2014.327

[52] 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. 2018. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.* 121, 19 (2018), 1–4. DOI: http://dx.doi.org/10.1103/PhysRevLett.121.190502

[53] Shuang Wang, Wei Chen, Jun-Fu Guo, Zhen-Qiang Yin, Hong-Wei Li, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han. 2012. 2 GHz clock quantum key distribution over 260 km of standard telecom fiber. *Opt. Lett.* 37, 6 (2012), 1008. DOI: http://dx.doi.org/10.1364/OL.37.001008

[54] Romain Alleaume, Francois Roueff, Eleni Diamanti, and Norbert Lutkenhaus. 2009. Topological optimization of quantum key distribution networks. *New J. Phys.* 11, 7 (July 2009), 75002. DOI: http://dx.doi.org/10.1088/1367-2630/11/7/075002

[55] Morgen Peck. 2007. Geneva Vote Will Use Quantum Cryptography. Retrieved from http://spectrum.ieee.org/computing/networks/geneva-vote-will-use-quantum-cryptography.
[56] Abdul Mirza and Francesco Petruccione. 2010. Realizing long-term quantum cryptography. *J. Opt. Soc. Amer. B* 27, 6 (June 2010), A185. DOI: http://dx.doi.org/10.1364/JOSAB.27.00A185
[57] Thomas Langer. 2013. *The Practical Application of Quantum Key Distribution*. Ph.D. Thesis. University of Lausanne.
[58] Kaoru Shimizu, Toshimori Honjo, Mikio Fujiwara, Toshiyuki Ito, Kiyoshi Tamaki, Shigehito Miki, Taro Yamashita, Hirotaka Terai, Zhen Wang, and Masahide Sasaki. 2014. Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of Tokyo metropolitan area. *J. Lightw. Technol.* 32, 1 (Jan. 2014), 141–151. DOI: http://dx.doi.org/10.1109/JLT.2013.2291391
[59] D. Collins, N. Gisin, and H. de Riedmatten. 2005. Quantum relays for long-distance quantum cryptography. *J. Mod. Opt.* 52 (2005), 735–753. DOI: http://dx.doi.org/10.1080/09500340412331283633
[60] Wolfgang Dur, Hans-J. Briegel, J. I. Cirac, and Peter Zoller. 1999. Quantum repeaters based on entanglement purification. *Phys. Rev. A* 59, 1 (1999), 169–181. DOI: http://dx.doi.org/10.1103/PhysRevA.59.169
[61] Zhen-Sheng Yuan, Yu-Ao Chen, Bo Zhao, Shuai Chen, Jörg Schmiedmayer, and Jian-Wei Pan. 2008. Experimental demonstration of a BDCZ quantum repeater node. *Nature* 454, 7208 (2008), 1098–1101. DOI: http://dx.doi.org/10.1038/nature07241
[62] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. 1998. Quantum repeaters for communication. Retrieved from http://arxiv.org/abs/quant-ph/9803056.
[63] S. J. van Enk. 1998. Photonic channels for quantum communication. *Science* 279, 5348 (Jan. 1998), 205–208. DOI: http://dx.doi.org/10.1126/science.279.5348.205
[64] Dirk Bouwmeester, Artur K. Ekert, and Anton Zeilinger. 2010. *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*. Springer Science & Business Media.
[65] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters. 1996. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.* 76, 5 (Jan. 1996), 722–725. DOI: http://dx.doi.org/10.1103/PhysRevLett.76.722
[66] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller. 2001. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* 414, 6862 (Nov. 2001), 413–418. DOI: http://dx.doi.org/10.1038/35106500
[67] Zheng-Da Li, Rui Zhang, Xu-Fei Yin, Li-Zheng Liu, Yi Hu, Yu-Qiang Fang, Yue-Yang Fei, Xiao Jiang, Jun Zhang, Li Li, Nai-Le Liu, Feihu Xu, Yu-Ao Chen, and Jian-Wei Pan. 2019. Experimental quantum repeater without quantum memory. *Nat. Photon.* 13, 9 (Sept. 2019), 644–648. DOI: http://dx.doi.org/10.1038/s41566-019-0468-5
[68] Matthias Bock, Pascal Eich, Stephan Kucera, Matthias Kreis, Andreas Lenhard, Christoph Becher, and Jürgen Eschner. 2018. High-fidelity entanglement between a trapped ion and a telecom photon via quantum frequency conversion. *Nat. Commun.* 9, 1 (2018), 1–7. DOI: http://dx.doi.org/10.1038/s41467-018-04341-2
[69] V. Krutyanskiy, M. Meraner, J. Schupp, V. Krcmarsky, H. Hainzer, and B. P. Lanyon. 2019. Light-matter entanglement over 50 km of optical fibre. *npj Quant. Inf.* 5, 1 (2019). DOI: http://dx.doi.org/10.1038/s41534-019-0186-3
[70] Axel Dahlberg, Julio de Oliveira Filho, Ronald Hanson, Stephanie Wehner, Matthew Skrzypczyk, Tim Coopmans, Leon Wubben, Filip Rozpędek, Matteo Pompili, Arian Stolk, Przemysław Pawełczak, and Robert Knegjens. 2019. A link layer protocol for quantum networks. In *Proceedings of the ACM Special Interest Group on Data Communication*. ACM, 159–173. DOI: http://dx.doi.org/10.1145/3341302.3342070
[71] Teng-Yun Chen, Jian Wang, Hao Liang, Wei-Yue Liu, Yang Liu, Xiao Jiang, Yuan Wang, Xu Wan, Wei-Qi Cai, Lei Ju, Luo-Kan Chen, Liu-Jun Wang, Yuan Gao, Kai Chen, Cheng-Zhi Peng, Zeng-Bing Chen, and Jian-Wei Pan. 2010. Metropolitan all-pass and inter-city quantum communication network. *Opt. Expr.* 18, 26 (2010), 27217–27225. DOI: http://dx.doi.org/10.1364/OE.18.027217
[72] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. 2012. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* 108, 13 (Mar. 2012), 130503. DOI: http://dx.doi.org/10.1103/PhysRevLett.108.130503
[73] Yan Lin Tang, Hua Lei Yin, Qi Zhao, Hui Liu, Xiang Xiang Sun, Ming Qi Huang, Wei Jun Zhang, Si Jing Chen, Lu Zhang, Li Xing You, Zhen Wang, Yang Liu, Chao Yang Lu, Xiao Jiang, Xiongfeng Ma, Qiang Zhang, Teng Yun Chen, and Jian Wei Pan. 2016. Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Phys. Rev. X* (2016). DOI: http://dx.doi.org/10.1103/PhysRevX.6.011024
[74] Xiao-Long Hu, Yuan Cao, Zong-Wen Yu, and Xiang-Bin Wang. 2018. Measurement-device-independent quantum key distribution over asymmetric channel and unstable channel. *Sci. Rep.* 8, 1 (Dec. 2018), 17634. DOI: http://dx.doi.org/10.1038/s41598-018-35507-z
[75] P. Schartner and S. Rass. 2010. Quantum key distribution and denial-of-service: Using strengthened classical cryptography as a fallback option. In *Proceedings of the ICS Workshop of Information Security*. IEEE, 131–136.
[76] Stefan Rass and S. König. 2012. Turning quantum cryptography against itself: How to avoid indirect eavesdropping in quantum networks by passive and active adversaries. *Int. J. Adv. Syst. Meas.* 5, 1 (2012), 22–33. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.261.3614.

[77] S. Rass and P. Schartner. 2011. A unified framework for the analysis of availability, reliability and security, with applications to quantum networks. *IEEE Trans. Syst. Man Cyber.- Part C: Applic. Rev.* 41, 1 (2011), 107–119. DOI: http://dx.doi.org/10.1109/TSMCC.2010.2050686

[78] Stefan Rass and Peter Schartner. 2009. Game-theoretic security analysis of quantum networks. In *Proceedings of the 3rd International Conference on Quantum, Nano and Micro Technologies*. IEEE Computer Society, 20–25.

[79] Stefan Rass and Peter Schartner. 2011. Information-leakage in hybrid randomized protocols. In *Proceedings of the International Conference on Security and Cryptography (SECRYPT'11)*, Javier Lopez and Pierangela Samarati (Eds.). SciTePress – Science and Technology Publications, 134–143.

[80] Stefan Rass. 2013. On game-theoretic network security provisioning. *J. Netw. Syst. Manag.* 21, 1 (2013), 47–64. DOI: http://dx.doi.org/10.1007/s10922-012-9229-1

[81] S. Rass. 2014. Complexity of network design for private communication and the P-vs-NP question. *Int. J. Adv. Comput. Sci. Applic.* 5, 2 (2014), 148–157.

[82] Marcos Curty and Hoi-Kwong Lo. 2019. Foiling covert channels and malicious classical post-processing units in quantum key distribution. *npj Quant. Inf.* 5, 1 (Dec. 2019), 14. DOI: http://dx.doi.org/10.1038/s41534-019-0131-5

[83] Ali C. Begen, Yucel Altunbasak, Ozlem Ergun, and Mostafa H. Ammar. 2005. Multi-path selection for multiple description video streaming over overlay networks. *EURASIP J. Sig. Proc. Image Commun.* 20, 1 (2005), 39–60. DOI: http://dx.doi.org/10.1016/j.image.2004.09.002

[84] Zheng Ma, Huai-Rong Shao, and Chia Shen. 2004. A new multi-path selection scheme for video streaming on overlay networks. In *Proceedings of the IEEE International Conference on Communications*, Vol. 3. IEEE, 1330–1334. DOI: http://dx.doi.org/10.1109/ICC.2004.1312728

[85] Chiping Tang and P. K. McKinley. 2005. Improving multipath reliability in topology-aware overlay networks. In *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems*. 82–88. Retrieved from http://ieeexplore.ieee.org/iel5/9817/30953/01437160.pdf?arnumber=1437160.

[86] Shu Tao, Kuai Xu, Antonio Estepa, Teng Fei, Lixin Gao, Roch Guerin, Jim Kurose, Don Towsley, and Zhi Li Zhang. 2005. Improving VoIP quality through path switching. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM'05)*. 2268–2278. DOI: http://dx.doi.org/10.1109/INFCOM.2005.1498514

[87] Brice Augustin, Timur Friedman, and Renata Teixeira. 2011. Measuring multipath routing in the Internet. *IEEE/ACM Trans. Netw.* 19, 3 (2011), 830–840. DOI: http://dx.doi.org/10.1109/TNET.2010.2096232

[88] Renata Teixeira, Keith Marzullo, Stefan Savage, and Geoffrey M. Voelker. 2003. Characterizing and measuring path diversity of internet topologies. *SIGMETRICS Perform. Eval. Rev.* 31, 1 (2003), 304–305. DOI: http://dx.doi.org/10.1145/781064.781069

[89] C. Labovitz, A. Ahuja, R. Wattenhofer, and S. Venkatachary. 2001. The impact of internet policy and topology on delayed routing convergence. In *Proceedings of the IEEE 20th Annual Joint Conference of the IEEE Computer and Communications Society (INFOCOM'01)*. 537–546. DOI: http://dx.doi.org/10.1109/INFCOM.2001.916775

[90] P. Toliver, R. J. Runser, T. E. Chapuran, J. L. Jackel, T. C. Banwell, M. S. Goodman, R. J. Hughes, C. G. Peterson, D. Derkacs, J. E. Nordholt, L. Mercer, S. McNown, A. Goldman, and J. Blake. 2003. Experimental investigation of quantum key distribution through transparent optical switch elements. *IEEE Photon. Technol. Lett.* 15, 11 (Nov. 2003), 1669–1671. DOI: http://dx.doi.org/10.1109/LPT.2003.818687

[91] Alexander Sergienko. 2005. *Quantum Communications and Cryptography*. Vol. 2005. CRC Press. Retrieved from http://books.google.com/books?hl=en.

[92] Chip Elliott, Alexander Colvin, David Pearson, Oleksiy Pikalo, John Schlafer, and Henry Yeh. 2005. Current status of the DARPA quantum network. In *Proc. SPIE 5815, Quantum Information and Computation III,* Eric J. Donkor, Andrew R. Pirich, and Howard E. Brandt (Eds.), Vol. 5815. 138–149. DOI: http://dx.doi.org/10.1117/12.606489 arxiv:quant-ph/0503058.

[93] Valerio Scarani, A. Acin, Grégoire Ribordy, and Nicolas Gisin. 2004. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* 92 (2004), 057901. DOI: http://dx.doi.org/10.1103/PhysRevLett.92.057901

[94] David Pearson. 2004. High-speed QKD reconciliation using forward error correction. In *Quantum Communication, Measurement and Computing*, Vol. 734. AIP, 299–302. DOI: http://dx.doi.org/10.1063/1.1834439

[95] Boris Slutsky, Ramesh Rao, Pan-Cheng Sun, Ljubiša Tancevski, and Shaya Fainman. 1998. Defense frontier analysis of quantum cryptographic systems. *Appl. Opt.* 37, 14 (May 1998), 2869. DOI: http://dx.doi.org/10.1364/AO.37.002869

[96] John M. Myers, Tai T. Wu, and David S. Pearson. 2004. Entropy estimates for individual attacks on the BB84 protocol for quantum key distribution. In *Defense and Security*, Eric Donkor, Andrew R. Pirich, and Howard E. Brandt (Eds.). International Society for Optics and Photonics, 36–47. DOI: http://dx.doi.org/10.1117/12.542534

[97] Ming Zhang and Sun Yongmei. 2008. A VPN key management scheme based on quantum key. In *Proceedings of the 4th International Conference on Semantics, Knowledge and Grid*. 453–456. DOI: http://dx.doi.org/10.1109/SKG.2008.85

[98] John T. Moy. 1991. OSPF Version 2. *Internet Req. Comm.* RFC 1247 (1991), 1–124. DOI: http://dx.doi.org/10.1017/CBO9781107415324.004 arxiv:arXiv:1011.1669v3.

[99] Barnum Pearson Brig and David Elliott Spencer. 2010. Systems and methods for implementing routing protocols and algorithms for quantum cryptographic key transport. Retrieved from http://www.google.com/patents/US7706535.

[100] Christopher Monroe, Michael G. Raymer, and Jacob Taylor. 2019. The U.S. national quantum initiative: From act to action. *Science* 364, 6439 (May 2019), 440–442. DOI: http://dx.doi.org/10.1126/science.aax0578

[101] John Costello. 2017. Chinese efforts in quantum information science: Drivers, milestones, and strategic implications. Retrieved from https://www.uscc.gov/sites/default/files/John%20Costello_Written%20Testimony_Final2.pdf.

[102] SiliconAngle. 2018. Quantum Xchange to build first quantum network in U.S. offering "unbreakable encryption." Retrieved from https://siliconangle.com/2018/06/26/quantum-xchange-build-first-quantum-network-u-s-offering-unbreakable-encryption/.

[103] QuantumXchange. 2019. Meet the first commercial quantum communication network in the United States. Retrieved from https://quantumxc.com/quantum-communication-network/.

[104] ID Quantique. 2019. Quantum Xchange and ID Quantique make ultra-secure quantum networks a reality for leading U.S. industries. Retrieved from https://www.idquantique.com/quantum-xchange-and-id-quantique-make-ultra-secure-quantum-networks-a-reality-for-leading-us-industries/.

[105] SPIE. 2019. Quantum Xchange tests Toshiba's QKD network and doubles capacity. Retrieved from https://optics.org/news/10/4/50.

[106] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J. D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J. B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger. 2009. The SECOQC quantum key distribution network in Vienna. *New J. Phys.* 11, 7 (July 2009), 75001. DOI: http://dx.doi.org/10.1088/1367-2630/11/7/075001

[107] Quantum Support Action. 2018. Supporting Quantum Technologies beyond H2020. (2018).

[108] Max F. Riedel, Daniele Binosi, Rob Thew, and Tommaso Calarco. 2017. The European quantum technologies flagship programme. *Quant. Sci. Technol.* 2, 3 (Sept. 2017), 030501. DOI: http://dx.doi.org/10.1088/2058-9565/aa6aca

[109] Inga Vesper. 2018. Chief of Europe's €1-billion brain project steps down. *Nature* (Aug. 2018). DOI: http://dx.doi.org/10.1038/d41586-018-06020-0

[110] A. Touzalin. 2016. Quantum manifesto: A new area of technology. Retrieved from http://Qurope.Eu/Manifesto.

[111] Max Riedel, Matyas Kovacs, Peter Zoller, Jürgen Mlynek, and Tommaso Calarco. 2019. Europe's quantum flagship initiative. *Quant. Sci. Technol.* 4, 2 (Feb. 2019), 020501. DOI: http://dx.doi.org/10.1088/2058-9565/ab042d

[112] COST Action CA 15220. Quantum technology in space. Retrieved from http://qtspace.eu/.

[113] E. H2020-SU-ICT-2018-3. 2020. Open European quantum key distribution testbed. Retrieved from https://www.openqkd.eu/.

[114] Kumar Sarkar, T. G. Basavaraju, and C. Puttamadappa. 2008. *Ad Hoc Mobile Wireless Networks.* Vol. 1. CRC Press.

[115] Teng-Yun Chen, Hao Liang, Yang Liu, Wen-Qi Cai, Lei Ju, Wei-Yue Liu, Jian Wang, Hao Yin, Kai Chen, Zeng-Bing Chen, Cheng-Zhi Peng, and Jian-Wei Pan. 2009. Field test of a practical secure communication network with decoy-state quantum cryptography. *Opt. Expr.* 17, 8 (Apr. 2009), 6540. DOI: http://dx.doi.org/10.1364/OE.17.006540 arxiv:0810.1264.

[116] F. X. Xu, W. Chen, S. Wang, Z. Q. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. B. Zhao, H. W. Li, D. Liu, Z. F. Han, and G. C. Guo. 2009. Field experiment on a robust hierarchical metropolitan quantum cryptography network. *Chin. Sci. Bull.* 54, 17 (2009), 2991–2997. DOI: http://dx.doi.org/10.1007/s11434-009-0526-3

[117] Zheng-fu Han, Fang-Xing Xu, Wei Chen, Shuang Wang, Zhen-Qiang Yin, Yang Zhang, Yun Liu, Zheng Zhou, Hong-Wei Li, Dong Liu, and Guang-Can Guo. 2010. An application-oriented hierarchical quantum cryptography network test bed. In *Proceedings of the Optical Fiber Communication Conference.* DOI: http://dx.doi.org/10.1364/OFC.2010.OTuK4

[118] Shuang Wang, Wei Chen, Zhen-Qiang Yin, Yang Zhang, Tao Zhang, Hong-Wei Li, Fang-xing Xu, Zheng Zhou, Yang Yang, Da-Jun Huang, Li-Jun Zhang, Fang-Yi Li, Dong Liu, Yong-Gang Wang, Guang-Can Guo, and Zheng-Fu Han. 2010. Field test of wavelength-saving quantum key distribution network. *Opt. Lett.* 35, 14 (2010), 2454–2456. DOI: http://dx.doi.org/10.1364/OL.35.002454 arxiv:1203.4321.

[119] Shuang Wang, Wei Chen, Zhen-Qiang Yin, Hong-Wei Li, De-Yong He, Yu-Hu Li, Zheng Zhou, Xiao-Tian Song, Fang-Yi Li, Dong Wang, Hua Chen, Yun-Guang Han, Jing-Zheng Huang, Jun-Fu Guo, Peng-Lei Hao, Mo Li, Chun-Mei Zhang, Dong Liu, Wen-Ye Liang, Chun-Hua Miao, Ping Wu, Guang-Can Guo, and Zheng-Fu Han. 2014. Field and

long-term demonstration of a wide area quantum key distribution network. *Opt. Expr.* 22, 18 (Sept. 2014), 21739. DOI: http://dx.doi.org/10.1364/OE.22.021739

[120] Qiang Zhang, Feihu Xu, Yu-Ao Chen, Cheng-Zhi Peng, and Jian-Wei Pan. 2018. Large scale quantum key distribution: Challenges and solutions [Invited]. *Opt. Expr.* 26, 18 (Sep. 2018), 24260. DOI: http://dx.doi.org/10.1364/oe.26.024260

[121] Jane Qiu. 2014. Quantum communications leap out of the lab. *Nature* 508, 7497 (Apr. 2014), 441–442. DOI: http://dx.doi.org/10.1038/508441a

[122] European Commission. 2017. China to launch world's first quantum communication network. Retrieved from https://cordis.europa.eu/article/id/122516.trending-science-china-to-launch-worlds-first-quantum-communication-network/en.

[123] ChinaDaily. 2017. Quantum tech to link Jinan governments. Retrieved from http://www.chinadaily.com.cn/china/2017-07/11/content_30065215.htm.

[124] Martino Travagnin and Adam Lewis. 2019. Quantum key distribution in field implementations. pp. EUR 29865 EN. Retrieved from https://op.europa.eu/en/publicationdetail/-/publication/e93e5bf9-efc3-11e9-a32c-01aa75ed71a1/language-en.

[125] Yong Zhao. 2019. The integration of QKD and security services. In *Proceedings of the ITU QIT4N Workshop Shanghai*. Retrieved from https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Yong.

[126] Yingqiu Mao, Bi-Xiao Wang, Chunxu Zhao, Guangquan Wang, Ruichun Wang, Honghai Wang, Fei Zhou, Jimin Nie, Qing Chen, Yong Zhao et al. 2018. Integrating quantum key distribution with classical communications in backbone fiber network. *Opt. Expr.* 26, 5 (2018), 6010–6020.

[127] Chenhui Ma, Yixi Guo, Jinhai Su, and Chao Yang. 2016. Hierarchical routing scheme on wide-area quantum key distribution network. In *Proceedings of the 2nd IEEE International Conference on Computer and Communications (ICCC'16)*, Vol. 1. IEEE, 2009–2014. DOI: http://dx.doi.org/10.1109/CompComm.2016.7925053

[128] Chenhui Ma, Yixi Guo, and Jinhai Su. 2017. A multiple paths scheme with labels for key distribution on quantum key distribution network. In *Proceedings of the IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC'17)*, Vol. 7. IEEE, 2513–2517. DOI: http://dx.doi.org/10.1109/IAEAC.2017.8054476

[129] Qiang Zhang, Feihu Xu, Li Li, Nai Le Liu, and Jian Wei Pan. 2019. Quantum information research in China. *Quant. Sci. Technol.* 4, 4 (2019). DOI: http://dx.doi.org/10.1088/2058-9565/ab4bea

[130] Yichen Zhang, Zhengyu Li, Ziyang Chen, Christian Weedbrook, Yijia Zhao, Xiangyu Wang, Yundi Huang, Chunchao Xu, Xiaoxiong Zhang, Zhenya Wang, Mei Li, Xueying Zhang, Ziyong Zheng, Binjie Chu, Xinyu Gao, Nan Meng, Weiwen Cai, Zheng Wang, Gan Wang, Song Yu, and Hong Guo. 2019. Continuous-variable QKD over 50 km commercial fiber. *Quant. Sci. Technol.* 4, 3 (2019), 035006. DOI: http://dx.doi.org/10.1088/2058-9565/ab19d1

[131] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields. 2016. Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nat. Photon.* 10, 5 (May 2016), 312–315. DOI: http://dx.doi.org/10.1038/nphoton.2016.50

[132] Wenyuan Wang, Feihu Xu, and Hoi-Kwong Lo. 2019. Asymmetric protocols for scalable high-rate measurement-device-independent quantum key distribution networks. *Phys. Rev. X* 9, 4 (Oct. 2019), 041012. DOI: http://dx.doi.org/10.1103/PhysRevX.9.041012

[133] Mamta Agiwal, Abhishek Roy, and Navrati Saxena. 2016. Next generation 5G wireless networks: A comprehensive survey. *IEEE Commun. Surv. Tutor.* 18, 3 (2016), 1617–1655. DOI: http://dx.doi.org/10.1109/COMST.2016.2532458

[134] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai Al., Wei-Yue Liu, Hui Dai Bo Li, Guang-Bing Li, Qi-Ming Lu, Yun-Hong Gong, Yu Xu, Shuang-Lin Li, Feng-Zhi Li, Ya-Yun Yin, Zi-Qing Jiang, Ming Li, Jian-Jun Jia, Dong He Ge Ren, Yi-Lin Zhou, Xiao-Xiang Zhang, Na Wang, Xiang Chang, Zhen-Cai Zhu, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. 2017. Satellite-based entanglement distribution over 1200 kilometers. *Science* 356, 6343 (2017), 1140–1144. DOI: http://dx.doi.org/10.1126/science.aan3211

[135] Tom Vergoossen, Sergio Loarte, Robert Bedington, Hans Kuiper, and Alexander Ling. 2019. Satellite constellations for trusted node QKD networks. Retrieved from https://arxiv.org/pdf/1903.07845.pdf.

[136] Miralem Mehic, Peppino Fazio, Stefan Rass, Oliver Maurhart, Momtchil Peev, Andreas Poppe, Jan Rozhon, Marcin Niemiec, and Miroslav Voznak. 2020. A novel approach to quality-of-service provisioning in trusted relay quantum key distribution networks. *IEEE/ACM Trans. Netw.* 28, 1 (Feb. 2020), 168–181. DOI: http://dx.doi.org/10.1109/TNET.2019.2956079

[137] Peppino Fazio, Floriano De Rango, and Cesare Sottile. 2016. A predictive cross-layered interference management in a multichannel MAC with reactive routing in VANET. *IEEE Trans. Mobile Comput.* 15, 8 (Aug. 2016), 1850–1862. DOI: http://dx.doi.org/10.1109/TMC.2015.2465384

[138] Peppino Fazio, Mauro Tropea, Floriano De Rango, and Miroslav Voznak. 2016. Pattern prediction and passive bandwidth management for hand-over optimization in QoS cellular networks with vehicular mobility. *IEEE Trans. Mobile Comput.* 1233, c (2016), 1. DOI: http://dx.doi.org/10.1109/TMC.2016.2516996

[139] F. De Rango and P. Fazio. 2014. A new distributed application and network layer protocol for VoIP in mobile ad hoc networks. *IEEE Trans. Mobile Comput.* 13, 10 (2014), 2185–2198. Retrieved from http://ieeexplore.ieee.org/xpls/abs.

[140] O. Maurhart, T. Lorunser, T. Langer, C. Pacher, M. Peev, and A. Poppe. 2009. Node modules and protocols for the Quantum-Back-Bone of a quantum-key-distribution network. In *Proceedings of the 35th European Conference on Optical Communication*. 3–4.

[141] Yoshimichi Tanizawa, Ririka Takahashi, and Alexander R. Dixon. 2016. A routing method designed for a quantum key distribution network. In *Proceedings of the International Conference on Ubiquitous and Future Networks (ICUFN'16)*. 208–214. DOI: http://dx.doi.org/10.1109/ICUFN.2016.7537018

[142] Jin-ying Sun, Jun Lang, Chengqiang Miao, Nan Yang, and Shenquan Wang. 2012. A digital watermarking algorithm based on hyperchaos and discrete fractional Fourier transform. In *Proceedings of the 5th International Congress on Image and Signal Processing*. 552–556. DOI: http://dx.doi.org/10.1109/CISP.2012.6469677

[143] Cheng Xianzhu, Sun Yongmei, and Ji Yuefeng. 2011. A QoS-supported scheme for quantum key distribution. In *Proceedings of the International Conference on Advanced Intelligence and Awareness Internet (AIAI'11)*. IET, 220–224. DOI: http://dx.doi.org/10.1049/cp.2011.1461

[144] Douglas S. J. De Couto, Daniel Aguayo, John Bicket, and Robert Morris. 2005. A high-throughput path metric for multi-hop wireless routing. *Wirel. Netw.* 11, 4 (July 2005), 419–434. DOI: http://dx.doi.org/10.1007/s11276-005-1766-z

[145] George Apostolopoulos, Roch Guerin, and Sanjay Kamat. 1999. Implementation and performance measurements of QoS routing extensions to OSPF. In *Proceedings of the IEEE 18th Annual Joint Conference of the Computer and Communications Societies (INFOCOM'99)*, Vol. 2. IEEE, 680–688. DOI: http://dx.doi.org/10.1109/INFCOM.1999.751454

[146] Chao Yang, Hongqi Zhang, and Jinhai Su. 2017. The QKD network: Model and routing scheme. *J. Mod. Opt.* 64, 21 (2017), 2350–2362. DOI: http://dx.doi.org/10.1080/09500340.2017.1360956

[147] Miralem Mehic, Oliver Maurhart, Stefan Rass, Dan Komosny, Filip Rezac, and Miroslav Voznak. 2017. Analysis of the public channel of quantum key distribution link. *IEEE J. Quant. Electron.* 53, 5 (Oct. 2017), 1–8. DOI: http://dx.doi.org/10.1109/JQE.2017.2740426

[148] Miralem Mehic, Peppino Fazio, Miroslav Voznak, and Erik Chromy. 2016. Toward designing a quantum key distrubution network. *Adva. Electric. Electron. Eng.* 14, 4 Special Issue (2016), 413–420. DOI: http://dx.doi.org/10.15598/aeee.v14i4.1914

[149] Matthias Geihs, Oleg Nikiforov, Denise Demirel, Alexander Sauer, Denis Butin, Felix Gunther, Gernot Alber, Thomas Walther, and Johannes Buchmann. 2019. The status of quantum-key-distribution-based long-term secure internet communication. *IEEE Trans. Sustain. Comput.* 3782, c (2019), 1–1. DOI: http://dx.doi.org/10.1109/tsusc.2019.2913948

[150] Wang Hua and Zhao Yongli. 2019. Overview of quantum key distribution metropolitan optical networking technology. *J. Commun.* 40, 2018 (2019), 1–7. DOI: http://dx.doi.org/10.11959/j.issn.1000-436x.2019210

[151] Hua Wang, Yongli Zhao, Xiaosong Yu, Zhangchao Ma, Jianquan Wang, Avishek Nag, Longteng Yi, and Jie Zhang. 2019. Protection schemes for key service in optical networks secured by quantum key distribution (QKD). *J. Optic. Commun. Netw.* 11, 3 (2019), 67–78. DOI: http://dx.doi.org/10.1364/JOCN.11.000067

[152] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. 2008. OpenFlow: Enabling innovation in campus networks. *ACM SIGCOMM Comput. Commun. Rev.* 38, 2 (2008), 69. DOI: http://dx.doi.org/10.1145/1355734.1355746

[153] Open Networking Foundation (ONF). 2014. *SDN Architecture Issue 1*. Technical Report. ONF–TR–502. Retrieved from https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR.

[154] Fotini Karinou, Hans H. Brunner, Chi Hang Fred Fung, Lucian C. Comandar, Stefano Bettelli, David Hillerkuss, Maxim Kuschnerov, Spiros Mikroulis, Dawei Wang, Changsong Xie, Momtchil Peev, and Andreas Poppe. 2018. Toward the integration of CV quantum key distribution in deployed optical networks. *IEEE Photon. Technol. Lett.* 30, 7 (2018), 650–653. DOI: http://dx.doi.org/10.1109/LPT.2018.2810334

[155] Yuan Cao, Yongli Zhao, Yu Wu, Xiaosong Yu, and Jie Zhang. 2018. Time-scheduled quantum key distribution (QKD) over WDM networks. *J. Lightw. Technol.* 36, 16 (2018), 3382–3395. DOI: http://dx.doi.org/10.1109/JLT.2018.2834949

[156] R. Nejabati, R. Wang, A. Bravalheri, A. Muqaddas, N. Uniyal, T. Diallo, R. Tessinari, R. S. Guimaraes, S. Moazzeni, E. Hugues-Salas, G. T. Kanellos, and D. Simeonidou. 2019. First demonstration of quantum-secured, inter-domain 5G service orchestration and on-demand NFV chaining over flexi-WDM optical networks. In *Optical Fiber Communication Conference Postdeadline Papers 2019*. OSA, Washington, D.C., Th4C.6. DOI: http://dx.doi.org/10.1364/OFC.2019.Th4C.6

[157] Alejandro Aguado, Emilio Hugues-Salas, Paul Anthony Haigh, Jaume Marhuenda, Alasdair B. Price, Philip Sibson, Jake E. Kennard, Christopher Erven, John G. Rarity, Mark Gerard Thompson, Andrew Lord, Reza Nejabati, and Dimitra Simeonidou. 2016. First experimental demonstration of secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources. In *Proceedings of the 42nd European Conference on Optical Communication (ECOC'16)*. VDE, Dusseldorf, Germany.

[158] Alejandro Aguado, Victor Lopez, Diego Lopez, Momtchil Peev, Andreas Poppe, Antonio Pastor, Jesus Folgueira, and Vicente Martin. 2019. The engineering of software-defined quantum key distribution networks. *IEEE Commun. Mag.* 57, 7 (July 2019), 20–26. DOI: http://dx.doi.org/10.1109/MCOM.2019.1800763

[159] Alejandro Aguado, Emilio Hugues-Salas, Paul Anthony Haigh, Jaume Marhuenda, Alasdair B. Price, Philip Sibson, Jake E. Kennard, Chris Erven, John G. Rarity, Mark Gerard Thompson, Andrew Lord, Reza Nejabati, and Dimitra Simeonidou. 2017. Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources. *J. Lightw. Technol.* 35, 8 (2017), 1357–1362. DOI: http://dx.doi.org/10.1109/JLT.2016.2646921

[160] Vicente Martin, Alejandro Aguado, Diego Lopez, Momtchil Peev, Victor Lopez, Antonio Pastor, Andreas Poppe, Hans Brunner, Stefano Bettelli, Fred Fung, David Hillerkuss, Lucian Comandar, and Wang Dawei. 2018. The Madrid SDN-QKD network. In *Proceedings of the International Conference on Quantum Cryptography (QCrypt'18).*

[161] Alejandro Aguado, Victor Lopez, Jesus Martinez-Mateo, Thomas Szyrkowiec, Achim Autenrieth, Momtchil Peev, Diego Lopez, and Vicente Martin. 2017. Hybrid conventional and quantum security for software defined and virtualized networks. *J. Optic. Commun. Netw.* 9, 10 (Oct. 2017), 819. DOI: http://dx.doi.org/10.1364/JOCN.9.000819

[162] Emilio Hugues-Salas, Foteini Ntavou, Dimitris Gkounis, George T. Kanellos, Reza Nejabati, and Dimitra Simeonidou. 2019. Monitoring and physical-layer attack mitigation in SDN-controlled quantum key distribution networks. *J. Optic. Commun. Netw.* 11, 2 (2019), A209–A218. DOI: http://dx.doi.org/10.1364/JOCN.11.00A209

[163] Stefan Marksteiner and Oliver Maurhart. 2015. A protocol for synchronizing quantum-derived keys in IPsec and its implementation. In *Proceedings of the 9th International Conference on Quantum, Nano/Bio, and Micro Technologies (ICQNM'15).* 35–40. DOI: http://dx.doi.org/10.13140/RG.2.1.4756.4001

[164] Alejandro Aguado, Victor Lopez, Jesus Martinez-Mateo, Momtchil Peev, Diego Lopez, and Vicente Martin. 2018. Virtual network function deployment and service automation to provide end-to-end quantum encryption. *J. Optic. Commun. Netw.* 10, 4 (Apr. 2018), 421. DOI: http://dx.doi.org/10.1364/JOCN.10.000421

[165] Alex Mavromatis, Foteini Ntavou, Emilio Hugues Salas, George T. Kanellos, Reza Nejabati, and Dimitra Simeonidou. 2018. Experimental demonstration of quantum key distribution (QKD) for energy-efficient software-defined internet of things. In *Proceedings of the European Conference on Optical Communication (ECOC'18).* 1–3. DOI: http://dx.doi.org/10.1109/ECOC.2018.8535267

[166] Yongli Zhao, Yuan Cao, Wei Wang, Hua Wang, Xiaosong Yu, Jie Zhang, Massimo Tornatore, Yu Wu, Mukherjee, and Biswanath. 2018. Resource allocation in optical networks secured by quantum key distribution. *IEEE Commun. Mag.* 56, 8 (2018), 130–137. DOI: http://dx.doi.org/10.1109/MCOM.2018.1700656

[167] Yuan Cao, Yongli Zhao, Carlos Colman-Meixner, Xiaosong Yu, and Jie Zhang. 2017. Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD). *Opt. Expr.* 25, 22 (2017), 26453. DOI: http://dx.doi.org/10.1364/oe.25.026453

[168] Yuan Cao, Yongli Zhao, Jianquan Wang, Xiaosong Yu, Zhangchao Ma, and Jie Zhang. 2019. Cost-efficient quantum key distribution (QKD) over WDM networks. *J. Optic. Commun. Netw.* 11, 6 (2019), 285–298. DOI: http://dx.doi.org/10.1364/JOCN.11.000285

[169] Y. Ou, E. Hugues-Salas, F. Ntavou, R. Wang, Y. Bi, S. Y. Yan, G. Kanellos, R. Nejabati, and D. Simeonidou. 2018. Field-trial of machine learning-assisted quantum key distribution (QKD) networking with SDN. In *Proceedings of the European Conference on Optical Communication (ECOC'18).* 1–3. DOI: http://dx.doi.org/10.1109/ECOC.2018.8535497

[170] Yuan Cao, Yongli Zhao, Rui Lin, Xiaosong Yu, Jie Zhang, and Jiajia Chen. 2019. Multi-tenant secret-key assignment over quantum key distribution networks. *Opt. Expr.* 27, 3 (2019), 2544. DOI: http://dx.doi.org/10.1364/oe.27.002544

[171] Masahide Sasaki, Mikio Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, Alexander R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger. 2011. Field test of quantum key distribution in the Tokyo QKD network. *Opt. Expr.* 19, 11 (May 2011), 10387. http://www.opticsexpress.org/abstract.cfm?URI=oe-19-11-10387

[172] Giovanni Giambene. 2014. *Queuing Theory and Telecommunications.* Springer US, Boston, MA.

[173] A. Aguado, V. Lopez, M. Peev, D. Lopez, and V. Martin. 2017. GMPLS network control plane enabling quantum encryption in end-to-end services. In *Proceedings of the IEEE International Conference on Optical Network Design and Modeling (ONDM'17).* Retrieved from http://ieeexplore.ieee.org/document/7958519/.

[174] Miralem Mehic, Almir Maric, and Miroslav Voznak. 2017. QSIP: A quantum key distribution signaling protocol. In *Communications in Computer and Information Science*, Vol. 785. 136–147. DOI: http://dx.doi.org/10.1007/978-3-319-69911-0_11

[175] Oliver Maurhart, Christoph Pacher, Andreas Happe, Thomas Lor, Cristina Tamas, Andreas Poppe, and Momtchil Peev. 2013. New release of an open source QKD software: Design and implementation of new algorithms, modularization and integration with IPSec. In *Proceedings of the International Conference on Quantum Cryptography (QCRYPT'13).*

[176] Miralem Mehic, Dan Komosny, Oliver Mauhart, Miroslav Voznak, and Jan Rozhon. 2016. Impact of packet size variation in overlay quantum key distribution network. In *Proceedings of the International Symposium on Telecommunications (BIHTEL'16)*. IEEE, 1–6. DOI: http://dx.doi.org/10.1109/BIHTEL.2016.7775711

[177] QuTech. 2018. SimulaQron. Retrieved from http://www.simulaqron.org/.

[178] A. Pereszlenyi. 2005. Simulation of quantum key distribution with noisy channels. In *Proceedings of the 8th International Conference on Telecommunications (ConTEL'05)*, Vol. 1. IEEE, 203–210. DOI: http://dx.doi.org/10.1109/CONTEL.2005.185853

[179] Shuang Zhao and Hans De Raedt. 2008. Event-by-event simulation of quantum cryptography protocols. *J. Computat. Theoret. Nanosci.* 5, 7 (2008), 1251–1254.

[180] Craig Gidney. 2016. Quirk: Quantum circuit simulator. A drag-and-drop quantum circuit simulator. Retrieved from https://algassert.com/quirk.

[181] Logan O. Mailloux, Jeffrey D. Morris, Michael R. Grimaila, Douglas D. Hodson, David R. Jacques, John M. Colombi, Colin V. Mclaughlin, and Jennifer A. Holes. 2015. A modeling framework for studying quantum key distribution system implementation nonidealities. *IEEE Access* 3 (2015), 110–130. DOI: http://dx.doi.org/10.1109/ACCESS.2015.2399101

[182] ETSI. 2020. ETSI official. Retrieved from www.etsi.org.

[183] IEEE Standards Association. 2016. Software-defined quantum communication working group. Retrieved from www.standards.ieee.org/project/1913.html.

[184] ITU-T Study Group. 2000. Specification and description language (SDL). *Telecomm. Standard. Sect. ITU* 100 (2000), 246. Retrieved from https://www.itu.int/ITU-T/studygroups/com10/languages/Z.100.

[185] ITU-T. 2020. ITU-T Study Group 17 - Security. Retrieved from https://www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx.

[186] ITU-T. 2019. ITU-T focus group on quantum information technology for networks (FG-QIT4N). Retrieved from https://www.itu.int/md/T17-TSB-CIR-0201.

[187] ISO/IEC. 2006. ISO/IEC 7812-1:2006 Identification cards – Identification of issuers – Part 1: Numbering system. Retrieved from http://www.iso.org.

[188] IETF. 2018. Quantum Internet proposed research group (QIRG). Retrieved from https://datatracker.ietf.org/rg/qirg/about/.

[189] Thomas Länger and Gaby Lenhart. 2009. Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD. *New J. Phys.* 11, 5 (May 2009), 055051. DOI: http://dx.doi.org/10.1088/1367-2630/11/5/055051

[190] Gaby Lenhart. 2012. QKD standardization at ETSI. In *Quantum Africa 2010: Theoretical and Experimental Foundations of Recent Quantum Technology*, Vol. 57. 50–57.

[191] Hong Xiang and Zheng-Fu Han. 2015. *The Chinese QKD Networks 3rd ETSI Quantum Safe Cryptography*. Technical Report. Seoul, Korea. Retrieved from https://docbox.etsi.org/Workshop/2015/201510.

Received March 2019; revised April 2020; accepted May 2020