# A Survey on Quantum Key Distribution

Laszlo Gyongyosi, Laszlo Bacsardi, *Member, IEEE*, and Sandor Imre, *Senior Member, IEEE*

***Abstract*—Quantum key distribution (QKD) protocols represent an important practical application of quantum information theory. QKD schemes enable legal parties to establish unconditionally secret communication by exploiting the fundamental attributes of quantum mechanics. Here we present an overview of QKD protocols. We review the principles of QKD systems, the implementation basis, and the application of QKD protocols in the standard Internet and the quantum Internet.**

***Index Terms*—Quantum key distribution, quantum cryptography, security, networking.**

## I. Introduction

Security and cryptography are crucial aspects of our everyday network communications. Since traditional networking methods are vulnerable to a variety of attacks, classical data encryption cannot provide unconditional security for legal parties [1]. QKD protocols [2]–[29] enable legal parties to share secret keys with unconditional security. In contrast to traditional cryptographic methods that rely on the computational complexity of mathematical functions, the security of QKD is based on physical laws. Whereas traditional cryptography is vulnerable to computational power [30], QKD systems are resistant against unlimited computational power. QKD can protect our security when quantum computers [31]–[36] become available.

The No-Cloning Theorem [37] is a consequence of the fundamentals of quantum mechanics, stating that it is impossible to make a perfect copy of a quantum system. In a QKD setting, it enables the parties to detect any eavesdropping activity, since the presence of an eavesdropper adds noise to the quantum transmission. The secret key between the sender (Alice) and receiver (Bob) is established over a quantum channel [29], which can be realized by an optical fiber [1], [6]–[22] or by a free-space optical channel [23]–[25], [38], [39].

QKD protocols can be classified into several different classes depending on the applied modulation, the encoding and decoding attributes, and the physical implementation of the quantum channel. Here we review QKD systems and the main attributes of the recent implementations.

This paper is organized as follows. In Section II, the fundamental principles of QKD protocols are discussed. In Section III, the implementation basis is studied. In Section IV, an outlook on quantum Internet scenarios is presented. Finally, Section V concludes the paper.

The research reported in this paper has been supported by the National Research, Development and Innovation Fund (TUDFO/51757/2019-ITM, Thematic Excellence Program). This work was partially supported by the National Research Development and Innovation Office of Hungary (Project No. 2017-1.2.1-NKP-2017-00001), and in part by the BME Artificial Intelligence FIKP grant of EMMI (BME FIKP-MI/SC).

The authors are with the Department of Networked Systems and Services, Budapest University of Technology and Economics, 1117 Budapest, Hungary (e-mail: gyongyosi@hit.bme.hu, bacsardi@hit.bme.hu, imre@hit.bme.hu).

## II. Quantum Key Distribution

The first QKD protocols that were introduced were based on discrete variables (DV), such as photon polarization. These QKD protocols are termed DVQKD systems [1]–[8], [10]–[21]. The first DVQKD protocol that was introduced was the so-called BB84 protocol [2], which used single-photon polarization for the encoding. In the BB84 protocol, the classical random bits are encoded in single-photon polarization photons (qubits) with four random polarization states. The four polarization states belong to two bases: the rectilinear basis and the diagonal basis. In the encoding and decoding phases, these bases are randomly selected to prepare and to measure the photons. After the quantum-level transmission is closed, the parties use a classical authenticated channel (public channel) to compare the bases. In a phase called the basis agreement phase, the parties delete those bits from the key that have different bases. After this step, additional calculations and error-correcting operations are performed on the classical bit string to reduce the possibility that valuable information is leaked to an eavesdropper. This step is the distillation phase. The result of this phase is an absolute secure key between Alice and Bob. A simplified version of the BB84 protocol is the B92 protocol [40], which uses only two polarization states instead of four.

In an entanglement-based QKD protocol, entangled photon pairs are shared between Alice and Bob to generate a secret key [3]. The effectiveness of this protocol can be improved by the application of hyper-entangled states [41] (photon pairs that are entangled simultaneously in multiple degrees of freedom), which can increase the eavesdropping detection probability. QKD protocols motivated the development of other quantum cryptographic protocols in which the primary aim is not the establishment of a secret key, such as quantum dense coding [42], quantum teleportation [43]–[46], quantum secret sharing [47], [48], or quantum-secured blockchain [49].

Since the polarization of single photons cannot be encoded and decoded efficiently because of the technological limitations of current physical devices, continuous-variable (CV) QKD systems were proposed [22], [50]–[63]. In a CVQKD system, the information is encoded in continuous variables (i.e., photon packets) by a Gaussian modulation utilizing the position or momentum quadratures of coherent quantum states. In comparison with DVQKD, the modulation and decoding of continuous variables does not require specialized devices and can be implemented efficiently by standard telecommunication networks and devices that are currently available and in widespread use. As a convenient consequence, CVQKD systems can be integrated into the currently established telecommunication networks by using the present optical fiber networks and optical devices. CVQKD protocols

can be further classified into one-way and two-way systems. In a one-way CVQKD system, Alice transmits her continuous variables to Bob over a quantum channel [29], [62], [63]. In a two-way system, Bob starts the communication, Alice adds her internal secret to the received message, and this is then sent back to Bob (e.g., one mode of the coupled beam that is outputted by a beam splitter is transmitted back to Bob). Two-way CVQKD systems were introduced for practical reasons to overcome the limitations of one-way CVQKD systems, such as low key rates and short communication distances [52]. Two-way CVQKD protocols exploit the benefits of multiple uses of the quantum channel and can leak only less valuable information to the eavesdropper.

The two-field (TF) QKD system [17] is a novel QKD scheme that uses a continuous-wave (CW) laser. In a TF-QKD system, pairs of phase-randomized optical fields are generated at two distant locations, which are then combined at a central measuring station. The fields that convey the same random phase can be used to establish a secret key.

We note that there are several other types of QKD protocols that are not detailed in our paper (such as coherent one-way (COW) QKD [64], differential phase-shift (DPS) QKD [65], six-state QKD [66], and decoy-state QKD systems [7], [67]).

### A. Discrete Variable Quantum Key Distribution

*1) Modulation:* In a DVQKD system, the quantum signal source is a single-photon source (e.g., attenuated laser pulses with telecom wavelengths). In the modulation phase, Alice draws a uniform random bit string that constitutes her raw data, and she then encodes the bits of the raw data into single-polarization photons with four (in BB84 [2]) random polarization states that represent the qubits. In the BB84, these polarization states are $\{\rightarrow, \uparrow, \nearrow, \nwarrow\}$, i.e., the horizontal, vertical, diagonal right, and diagonal left states that encode the logical bits $\{0, 1\}$ in the $B_r = \{\rightarrow, \uparrow\}$ rectilinear and in the $B_d = \{\nearrow, \nwarrow\}$ diagonal basis, respectively. The qubits are therefore modulated via a $B$ random basis selection procedure.

*2) Eavesdropping:* The activity of an eavesdropper (Eve) results in detectable noise in the quantum channel, since Eve has no knowledge about the basis of Alice's qubit. As a corollary, for some qubits she will use the same basis as Alice, while for others a different basis is used, which results in detectable noise. The resulting noise of Eve's activity is analogous to a binary symmetric channel (BSC), which allows the use of the well-known channel-coding and error-correction tools in the post-processing phase.

*3) Measurement:* In a DVQKD system, the single-polarization photons are measured in the $B_d$ basis or in the $B_r$ basis in a $B'$ random basis selection procedure at the receiver. In BB84, Bob randomly uses a rectilinear or diagonal basis, and the result of the measurement is a logical bit. These measurement results comprise Bob's raw data. Since Bob has no knowledge about the correct basis for the measurement of a given photon, several bits from his raw data will be uncorrelated with Alice's raw data. These bits are deleted from the raw data in the basis agreement phase, which uses the classical public channel.

*4) Key Distillation:* Key-distillation is a post-processing step that is separated from the transmission of quantum states. It aims to derive the secret key from the correlated raw data at the parties. The logical layer-based post-processing consists of two main phases: error correction and privacy amplification. The aim of the post-processing is to extract as much valuable information from the correlated raw data as possible and to generate an error-free key between Alice and Bob. The privacy amplification operates on the shared, error-corrected common secret to extract the final key between the parties, and the aim of this phase is to reduce to zero the possible knowledge of an eavesdropper from the elements of the key. The raw data shared over the quantum channel is noisy, and this must be corrected to distill the final secret key. Since a large number of raw data bits must be shared between the parties, the complexity of the post-processing phase is a critical point in QKD protocols.

### B. Continuous Variable Quantum Key Distribution

*1) Modulation:* A Gaussian modulation is a robust and easily applicable solution in a practical CVQKD scenario [62], [63]. In particular, Alice draws a random Gaussian vector (Alice's raw data) and encodes the position and momentum quadratures based on it. The quantum signal source is a multi-photon source (e.g., a laser source with telecom wavelengths). In the standard CVQKD coding scenario, Alice modulates and separately transmits a CV coherent quantum state in the phase space. This standard modulation scheme is referred to as single-carrier modulation throughout the paper, consistent with its traditional meaning. In a multicarrier CVQKD [38], [68]–[73], the information is granulated into subcarrier continuous variables in the encoding phase, which are then decoded by a continuous unitary transformation. The aim of multicarrier CVQKD is to improve the secret key rates and the achievable distances.

*2) Eavesdropping:* For any CVQKD protocol, the optimal attack results in Gaussian noise; therefore, the physical link is modeled as an additive white Gaussian noise (AWGN) channel (Gaussian channel). More precisely, the Gaussian noise of the quantum channel models the eavesdropper's optimal entangling-cloner attack, and the channel is referred to as a Gaussian quantum channel. CVQKD schemes use continuous-variable Gaussian modulation, which has been proven to provide optimal key rates against collective attacks at finite-size block lengths, in addition to maximizing the mutual information between Alice and Bob [22], [74]. The security of CVQKD has also been proven against collective attacks in the asymptotic regime with infinite block sizes [62], [63], [75] and against arbitrary attacks in the finite-size regime [62], [63], [76]. Compared with a DVQKD system, a CVQKD system requires several additional physical parameters (transmittance, variance, shot noise, excess noise, the variance of Eve's quantum state, etc.) for the proper description of a Gaussian quantum channel. The performance of the protocol is strongly determined by the excess noise of the quantum channel and the transmittance parameter of the physical link.

*3) Measurement:* The measurement phase is a crucial part of CVQKD protocols. Depending on the measured quadrature types, it can be classified as homodyne or heterodyne measurement [62], [63]. In a homodyne measurement $M_{\text{hom}}$, only one quadrature, the position or the momentum quadrature $x_j$ of a $j$-th coherent state, is measured. In a heterodyne measurement $M_{\text{het}}$, both the position and momentum quadratures are measured. Each quadrature measurement results in a unit in the raw data. Bob's resulting raw data are in the form of a noisy Gaussian vector with additive Gaussian noise. The raw data themselves do not comprise a secret key; they consist only of the results of the random quadrature measurements. The secret key is a uniformly distributed long binary string, which will be combined with the raw data elements in the stage of logical layer manipulations. The post-processing phase uses a classical-authenticated communication channel and classical error-correction algorithms.

*4) Reconciliation:* The reconciliation process of correlated Gaussian variables is a complex problem that requires either tomography in the physical layer, which is intractable in a practical scenario, or high-cost calculations in the multi-dimensional spherical space with strict dimensional limitations. In the reconciliation phase, only uniform distributions can be transmitted over the classical channel; otherwise, the information-theoretic security of the protocol cannot be proven [62], [63]. The raw data follow a Gaussian random distribution because the data arise from a Gaussian random source; however, by applying some trivial operations on the raw data units, the desired uniform distribution can be reached, and the reconciliation can be performed with unconditional security [77]. In the reconciliation phase, a physical-logical channel conversion is made, and the aim is to get a logical channel (reconciliation channel) that is close to a binary Gaussian channel. At low signal-to-noise ratios (SNRs), the capacities of the Gaussian quantum channel and the binary Gaussian channel are close, and the reconciliation channel is analogous to a binary Gaussian channel. The efficiency of the channel conversion procedure can be described by the relevant parameters of the resulting logical binary channel (such as its variance and capacity). This conversion efficiency determines the efficiency of the reconciliation process, i.e., the performance of the protocol.

In Fig. 1, the DVQKD and CVQKD settings are compared. The modulation phase in the DVQKD setting assumes four polarization states of the BB84.

## III. QKD IMPLEMENTATIONS

### A. QKD over Optical Fiber

The optical fiber infrastructure provides a base ground for the experimental realization of both DVQKD and CVQKD protocols. The currently established optical fiber infrastructure with wavelength division multiplexing (WDM) technique represents an adequate solution for the practical implementation of QKD [8]. A general architecture of a QKD-integrated optical network consists of four layers: a physical layer with the optical fiber architecture (e.g., an optical layer), a QKD layer, a control layer (which can be implemented by software-defined networking, or SDN, to efficiently manage the entire network [6]), and an application layer. In the layer model, the users' service requests are generated in the application layer. Then, the control layer determines a path in the physical network and performs a handshake with the relevant quantum devices and optical nodes through the path. In an abstract manner, the optical layer integrates optical nodes connected by optical fibers, while the QKD layer consists of quantum nodes with quantum channels and public channels between them. The optical layer and the QKD layer share the fiber bandwidth resources with WDM technique [6], [8]. On the problem of wavelength allocation and channel isolation for QKD-integrated optical networks, we refer to [13]. For the model of SDN-controlled optical networks with time-shared QKD, see [15]. On the problem of efficient secret-key allocation in QKD implementations, we suggest [16]. In [20], a method for the implementation of quantum and classical signals over the same optical fiber in QKD networks has been proposed. In [21], the concept of a virtual optical network (VON) is defined for the purpose of efficient energy utilization and security enhancements in practical optical fiber settings.

### B. Free-Space Optical QKD

The fundamental characteristics of optical fiber-based QKD (i.e., channel loss of fibers, propagation losses) limit the achievable point-to-point distances to a few hundred kilometers. The achievable distances in terrestrial free-space-based QKD are also limited because of the exponentially decreasing photon rate with increasing distance. Satellite-based QKD represents a way to overcome these drawbacks and to establish a global-scale QKD network [23]–[25], [38]. The satellite-based solutions exploit the negligible photon loss and decoherence in the empty outer space. In [39], a satellite-to-ground QKD system with an achievable distance of over 1,200 kilometers has been demonstrated. The proposed model integrated a low-Earth-orbit satellite with decoy-state QKD. The reported key rate of the protocol was above 1 kbps. The results also enable us to realize high-efficiency long-distance QKD in a global-scale setting.

Relevant attributes of some recent QKD implementations are summarized in Table I.

### C. QKD in the Traditional Internet

The secret key generated by a QKD system is a random key that can also serve as a one-time pad (OTP) [78], which theoretically provides unconditional security [79]. However, in theory, in an OTP system, the secret-key size must be at least as long as the data size to be encrypted, and novel random keys are required for novel data. It is trivially not implementable in practical scenarios because of the long execution times and large storage requirements. These issues are resolved by the integration of QKD into efficient traditional data encryption algorithms (AES, IPSec, TLS, etc.) [12], [80]. In these integrated, hybrid QKD-traditional encryption systems, the QKD structure provides a practical and significantly shorter key (in comparison with an OTP key) to an efficient encryption method that periodically requires a novel key from the QKD backbone structure [6].

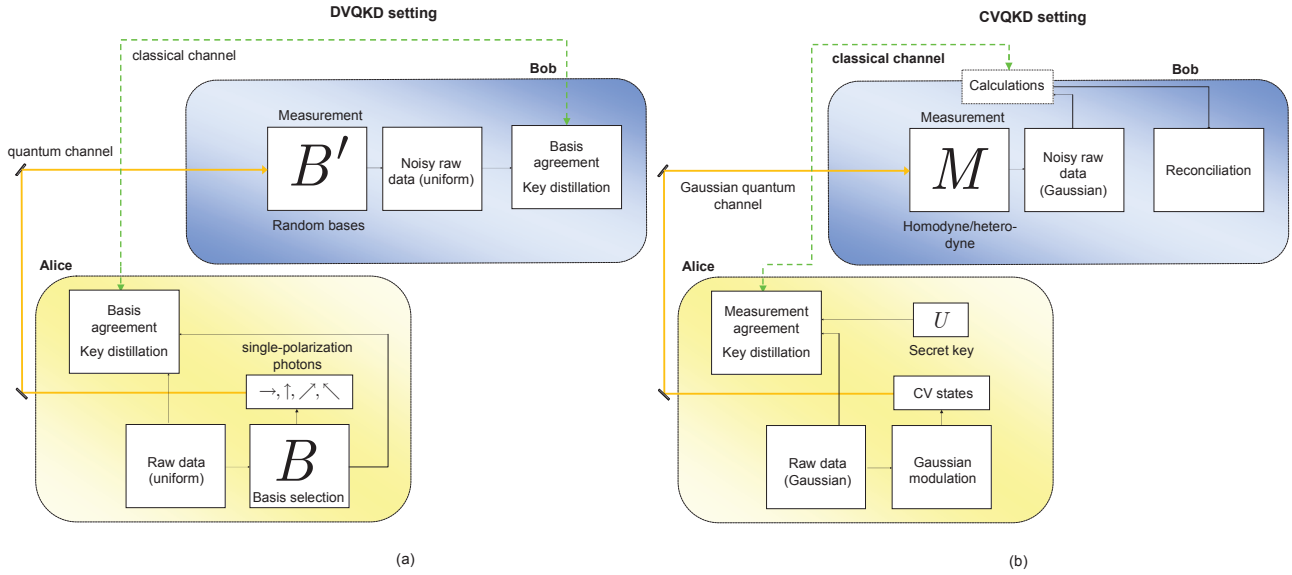


Fig. 1. Comparison of the sender (Alice) and receiver (Bob) model in a DVQKD and a CVQKD setting. (a) DVQKD setting. Alice draws uniform random raw data, which encode her random bits. She modulates all the bits of her raw data into single-polarization photons (qubits). The rectilinear and diagonal polarization states are selected randomly in the $B$ basis selection procedure for the encoding. The qubits are sent through the quantum channel (depicted by the yellow line), where the presence of Eve adds noise to the transmission. Bob measures each qubit in a random basis via the $B'$ basis selection procedure. The results of the measurements are classical bits, which form the noisy raw data. The final key is extracted from the correlated raw data of the parties using the classical public channel (depicted by the green line). (b) CVQKD setting. Alice draws Gaussian random raw data with Gaussian variables. Using her raw data, she modulates the CV quantum states via a Gaussian modulation. The CV quantum states are sent through a quantum channel, where the presence of the eavesdropper adds white Gaussian noise to the transmission. Bob measures the CV states via the $M$ measurement procedure using homodyne or heterodyne measurement. The measurements yield noisy Gaussian raw data. In the post-processing phase, a $U$ secret key (a classical uniform random vector) is drawn at Alice, which will be combined with her raw data. The combined result is transmitted to Bob over the classical channel. Bob applies some local calculations and reconciliation steps to extract the noise-free $U$ secret key on his side.

TABLE I
ATTRIBUTES OF RECENT QKD IMPLEMENTATIONS.

| QKD protocol | Distance | Max. secret-key rate | Quantum channel |
|---|---|---|---|
| BB84 (DV) [8] | 66 km | 5.1 kbps | optical fiber, 1310 nm |
| BB84 (DV) [10] | 150 km | 1 kbps | optical fiber, 1548 nm |
| BB84 (DV) [11] | 80 km | 1 kbps | optical fiber, 1310 nm |
| BB84 (DV) [18] | 50 km | 1.26 Mbps | optical fiber, 1550 nm |
| BB84 (DV) [19] | 404 km | 1.16 bit/hour | optical fiber, 1550 nm |
| Twin-field QKD [17] | 550 km | 0.1 kbps | optical fiber, 1550 nm |
| CV [9] | 20 km | 90 kbps | optical fiber, 1550 nm |
| CV [22] | 80 km | 0.1 kbps | optical fiber, 1550 nm |
| Satellite-to-ground BB84 (DV) [39] | 1,200 km | 1 kbps | free space optical, 850 nm |

The hybrid structure is realizable through the currently established Internet architecture, as depicted in Fig. 2. The QKD devices establish the unconditionally secure key through the quantum channels (auxiliary public channels are not depicted). The keys are then passed via secure local connections to the server (e.g., an HTTP/TLS server) and the web clients. Then, the client-server communication is realized by the TLS protocol with periodically updated quantum-made keys.

## IV. QKD IN THE QUANTUM INTERNET

The quantum Internet [80], [82]–[85] is a global-scale quantum communication network composed of quantum subnetworks and quantum networking components. The quantum Internet utilizes the fundamental concepts of quantum mechanics for networking. The main attributes of the quantum Internet are unconditional security (quantum cryptographic protocols), advanced quantum phenomena and protocols (such as quantum superposition, quantum entanglement, quantum teleportation and quantum coding and an entangled network structure. In contrast to traditional repeaters, quantum repeaters cannot apply the "receive-copy-retransmit" mechanism, because of the No-Cloning Theorem [37]. This fundamental difference between the nature of classical and quantum information not just leads to fundamentally different networking mechanisms, but also requires the definition of novel networking services in a quantum Internet scenario [86]–[90].

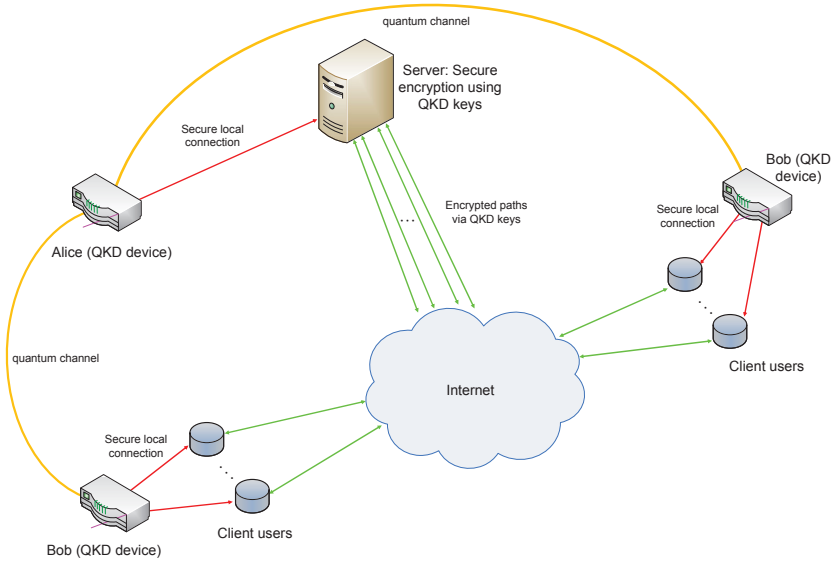


Fig. 2. QKD in a traditional client-server Internet setting. The established paths (green lines) between the clients and the server in the traditional Internet use quantum-made keys. The quantum keys are established via the QKD devices over quantum channels (depicted by yellow lines). The quantum keys are shared with the classical server and the classical clients through secure local connections (red lines).

The core network of the quantum Internet is modeled as an entangled network structure [80], [91], [92], in which the quantum nodes are connected by entangled connections. An entangled connection refers to a shared entangled system (i.e., a Bell state for qubit systems to connect two quantum nodes) between the quantum nodes. In an unentangled network structure, the quantum nodes are not necessarily connected by entanglement [93], [94], and the communication between the nodes is realized in a point-to-point setting. This setting does not allow quantum communication over arbitrary distances, and an unentangled network structure can mostly be used for establishing a point-to-point QKD between the quantum nodes. These short distances can be extended to longer distances by the utilization of free-space quantum channels [23], [24], [80], [95]. However, this solution is auxiliary, since it can be used only at some specific points of the unentangled network structure. Therefore, it does not represent an adequate and fundamental answer to the problem of long-distance quantum communication. Consequently, in an unentangled network structure, the multi-hop settings are weak for experimental, long-distance and global-scale quantum communication. On the other hand, the entangled network structure allows the parties to establish multi-hop entanglement, multi-hop QKD, high-precision sensor networks, advanced distributed computations and cryptographic functions, advanced quantum protocols, and, more importantly, the distribution of quantum entanglement over arbitrary (unlimited, in theory) distances [80]. Entanglement between a distant source and a target node is established through several intermediate repeater nodes [80], [91], [92], [96], [97]. The level of entanglement (i.e., the level of an entangled connection) is defined as the number of nodes (i.e., the hop-distance between entangled nodes) spanned by the shared entanglement, whose range is extended by the basic operation of entanglement swapping (entanglement extension).

The entangled network structure of the quantum Internet formulates a high-complexity network space with several advantages and challenges. Quantum Internet is an adequate answer for the computational power that became available as quantum computers became publicly available. The structure of the quantum Internet keeps the data of users safe for future networking. However, the commercial quantum computers are currently under development and represent tomorrow's problems, the engineering of high-performance and well-designed services and protocols for the quantum Internet is today's tasks. As quantum computers are built and become available, the structure of the quantum Internet also has to be ready to provide a seamless transition from the traditional Internet to the quantum Internet.

### *A. Recent Implementations*

An optical switcher-based QKD implementation has been proposed in [14]. The system model integrates several hop-by-hop QKD settings to realize a long-distance QKD. The optical switchers were implemented for the purpose of time division multiplexing (TDM) on the quantum channels between the QKD devices.

A technical roadmap on the experimental development of the quantum Internet has been provided in [98]. The roadmap is connected to the Quantum Internet Research Group (QIRG) [99], which group is formulated and supported by an international researcher background and collaboration. The authors of [98] address some important capability milestones for the realization of a global-scale quantum Internet. The technical roadmap also addresses important future engineering problems brought up by the quantum Internet, such as the development of a standardized architectural framework for the quantum Internet, standardization and protocols of the quantum Internet,

layer interoperability, advanced services for the quantum Internet, interoperability of the traditional Internet and quantum Internet, connection establishment between the heterogeneous quantum nodes of the quantum Internet, definition of node roles, network coding, multiparty state transfer, entanglement distribution mechanisms and entanglement routing, application programming interface (API) for the quantum Internet, and the definition of the application level of the quantum Internet.

In [100], the authors defined a method for deterministic delivery of quantum entanglement on a quantum network. The results allow us to realize entanglement distribution across multiple remote quantum nodes in a quantum Internet setting.

In [45], the authors demonstrated the quantum teleportation of independent single-photon qubits over 1,400 kilometres. Since an experimental realization of a global-scale quantum Internet requires the application of quantum teleportation over long-distances, the proposed results represent a fundamental of any experimental quantum Internet. In [46], the authors demonstrated quantum teleportation with high fidelity values between remote single-atom quantum memories.

Some other recent results connected to the development of an experimental global-scale quantum Internet are as follows. In [101], the authors demonstrated the Bell inequality violation using electron spins separated by 1.3 kilometres. In [102], the authors demonstrated modular entanglement of atomic qubits using photons and phonons. The quantum repeaters are fundamental networking elements of any experimental quantum Internet. The quantum repeaters are used in the entanglement distribution process to generate quantum entanglement between distant senders and receivers. The quantum repeaters also realize the entanglement purification (entanglement improvement) and the entanglement swapping (entanglement extension) procedures. For an experimental realization of quantum repeaters based on atomic ensembles and linear optics, see [103].

Since quantum channels also have a fundamental role in the quantum Internet, we suggest the review paper of [29], and also the work of [104], for some specialized applications of quantum channels. For a review on some recent results of quantum computing technology, we suggest [105]. Some recent services developed for the quantum Internet can be found in [112]–[116]. The works [91]–[93], [96] are related to the utilization of entanglement for long-distance quantum communications and for a global-scale quantum Internet, and also to the various aspects of quantum networks in a quantum Internet setting.

For some fundamental works on quantum Shannon theory, see [27]–[29], [104], [106]–[109]. For some important works on the experimental implementations of quantum repeaters, entanglement purification and entanglement distribution, see [110]–[112], [117]–[119].

## V. CONCLUSION

Here we provided a brief overview of the recent results of QKD. The review focused on the principles of DVQKD and CVQKD protocols, the main attributes of the recent implementations, and the integration of QKD into traditional and quantum communication networks.

## REFERENCES

[1] Skorin-Kapov, N. et al., Physical-Layer Security in Evolving Optical Networks, *IEEE Commun. Mag.*, vol. 54, no. pp. 110–117. (2016).
[2] Bennett, C. H. and Brassard, G. Quantum cryptography: Public-key distribution and coin tossing. In: *Proceeding of the IEEE International Conference on Computers Systems and Signal Processing*. Washington: IEEE, pp. 175-179 (1984).
[3] Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys Rev Lett*, 67, pp. 661-663 (1991).
[4] Yuen, H. P. Security of quantum key distribution. *IEEE Access*, Vol.4, No.1, pp. 724-749 (2016).
[5] Broadbent, A., and Schaffner, C. Quantum cryptography beyond quantum key distribution. *Designs Codes and Cryptography*, Vol.78, No.1, pp. 351-382 (2016).
[6] Cao, Y. et al. Key as a Service (KaaS) over Quantum Key Distribution (QKD)-Integrated Optical Networks, *IEEE Comm. Mag.* DOI: 10.1109/MCOM.2019.1701375 (2018).
[7] Lo, H.-K. et al., Secure Quantum Key Distribution, *Nature Photon.*, vol. 8, pp. 595–604. (2014)
[8] Mao, Y. et al., Integrating Quantum Key Distribution with Classical Communications in Backbone Fiber Network, *Opt. Express*, vol. 26, no. 5, pp. 6010–6020. (2018).
[9] Karinou, F. et al., Toward the Integration of CV Quantum Key Distribution in Deployed Optical Networks, *IEEE Photon. Technol. Lett.*, vol. 30, no. 7, pp. 650–653. (2018).
[10] Frohlich, B. et al., Long-Distance Quantum Key Distribution Secure Against Coherent Attacks, *Optica*, vol. 4, no. 1, pp. 163–167. (2017).
[11] Wang, L.-J. et al., Long-Distance Copropagation of Quantum Key Distribution and Terabit Classical Optical Data Channels, *Phys. Rev. A*, vol.95, no. 1, pp. 012301. (2017).
[12] Cao, Y. et al., Key on Demand (KoD) for Software-Defined Optical Networks Secured by Quantum Key Distribution (QKD), *Opt. Express*, vol.25, no. 22, pp. 26453–26467 (2017).
[13] Cao, Y. et al., Time-Scheduled Quantum Key Distribution (QKD) over WDM Networks, *J. Lightwave Technol.*, vol. 36, no. 16, pp.3382–3395. (2018).
[14] Peev, M. et al., The SECOQC Quantum Key Distribution Network in Vienna, *New J. Phys.*, vol. 11, no. 7, pp. 075001. (2009).
[15] Aguado, A. et al., Secure NFV Orchestration over an SDN-Controlled Optical Network with Time-Shared Quantum Key Distribution Resources, *J. Lightwave Technol.*, vol. 35, no. 8, pp. 1357–1362. (2017).
[16] Xu, S. et al. Fiber-Wireless Network Virtual Resource Embedding Method Based on Load Balancing and Priority, *IEEE Access*, vol. 6, pp. 33201-33215 (2018).
[17] Lucamarini, M. et al., Overcoming the Rate–Distance Limit of Quantum Key Distribution without Quantum Repeaters, *Nature*, vol. 557, no.7705, pp. 400–403. (2018).
[18] Comandar, L. C. et al. Room temperature singlephoton detectors for high bit rate quantum key distribution. *Appl. Phys. Lett.* 104, 021101 (2014).
[19] Yin, H.-L. et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* 117, 190501 (2016).
[20] Aleksic, S. et al., Towards a Smooth Integration of Quantum Key Distribution in Metro Networks, in *Proc. 16th Int. Conf. on Transparent Optical Networks* (ICTON), Graz, Austria, (2014).
[21] Zhao, Y. et al., Energy Efficiency with Sliceable Multi-Flow Transponders and Elastic Regenerators in Survivable Virtual Optical Networks, *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2539.2550. (2016).
[22] Jouget P. et al. Experimental demonstration of long-distance continuous-variable quantum key distribution, *Nature Photonics* volume 7, pages 378–381 (2013).
[23] Galambos, M. and Bacsardi, L. Comparing Calculated and Measured Losses in a Satellite-Earth Quantum Channel, *Infocomm. Journal* X:3, pp. 14-19., (2018).
[24] Galambos, M. and Bacsardi, L. The Evolution of Free-Space Quantum Key Distribution, *Infocomm. Journal* X:1 pp. 22-30.,(2018).
[25] Bacsardi, L. On the Way to Quantum-Based Satellite Communication, *IEEE Comm. Mag.* 51:(08) pp. 50-55. (2013).
[26] Gyongyosi, L. and Imre, S. Geometrical Analysis of Physically Allowed Quantum Cloning Transformations for Quantum Cryptography, *Information Sciences*, Elsevier, pp. 1-23, DOI: 10.1016/j.ins.2014.07.010 (2014).
[27] Imre, S. and Gyongyosi, L. *Advanced Quantum Communications - An Engineering Approach*. New Jersey, Wiley-IEEE Press (2013).
[28] Petz, D. *Quantum Information Theory and Quantum Statistics*, Springer-Verlag, Heidelberg, Hiv: 6. (2008).

[29] Gyongyosi, L., Imre, S. and Nguyen, H. V. A Survey on Quantum Channel Capacities, *IEEE Communications Surveys and Tutorials*, DOI: 10.1109/COMST.2017.2786748 (2018).

[30] Shor, P. W. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proc. 35th Symposium on Foundations of Computer Science*, 124–134, Los Alamitos, CA, IEEE Computer Society Press (1994).

[31] IBM. *A new way of thinking: The IBM quantum experience*. URL: http://www. Research.ibm. Com/quantum. (2017).

[32] Monz, T. et al. Realization of a scalable Shor algorithm. *Science* 351, 1068-1070 (2016).

[33] Vandersypen, L. M. K. et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature* 414, 883-887 (2001).

[34] Aaronson, S. and Chen, L. Complexity-theoretic foundations of quantum supremacy experiments. *Proceedings of the 32nd Computational Complexity Conference*, CCC '17, pages 22:1-22:67, (2017).

[35] Harrow, A. W. and Montanaro, A. Quantum Computational Supremacy, *Nature*, vol 549, pages 203-209 (2017).

[36] Preskill, J. Quantum Computing in the NISQ era and beyond, *Quantum* 2, 79 (2018).

[37] Wootters, W. and Zurek, W. H. A single quantum cannot be cloned. *Nature*, 299:802–803, doi:10.1038/299802a0. (1982).

[38] Zhao, W., Liao, Q., Huang, D. et al. Performance analysis of the satellite-to-ground continuous-variable quantum key distribution with orthogonal frequency division multiplexed modulation, *Quant. Inf. Proc.* 18: 39. DOI: 10.1007/s11128-018-2147-8 (2019).

[39] Liao, S.-K. et al. Satellite-to-ground quantum key distribution, *Nature* 549, pages 43–47, (2017).

[40] Bennett, C., Quantum cryptography using any two nonorthoganol states, *Phys. Rev. Lett.* 68, pp. 3121-3124. (1992).

[41] Kwiat, P. G. Hyper-entangled states. *J Mod Opt* 44, pp. 2173-2184 (1997).

[42] Klaus, M. et al. Dense coding in experimental quantum communication. *Phys. Rev. Lett.*, 69, pp. 4656-4659 (1992).

[43] Bennett, C. H., Brassard, G., Crepeau, C., et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys Rev Lett*, 70, pp. 1895-1899 (1993).

[44] Bouwmeester, D., Pan, J. W., Mattle, K. et al. Experimental quantum teleportation. *Nature*, 390, pp. 575-579 (1997).

[45] Ren, J.-G. et al. Ground-to-satellite quantum teleportation, *Nature* 549, pages 70–73, (2017).

[46] Noelleke, C. et al, Efficient Teleportation Between Remote Single-Atom Quantum Memories, *Physical Review Letters* 110, 140403, (2013).

[47] Hillery, M., Buzek, V. and Berthiaume, A. Quantum secret sharing. *Phys Rev A*, 59, pp. 1829-1834 (1999).

[48] Jiang, Y. et al. Quantum secret sharing protocol and its modeling checking. *Laser and Optoelectronics Progress* 54(12), 122704, (2017).

[49] Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., Lvovsky, A. I. and Fedorov, A. K. Quantum-secured blockchain, *Quantum Sci. Technol.* 3, 035004 (2018).

[50] Grosshans, F., Cerf, N. J., Wenger, J., Tualle-Brouri, R. and Grangier, P. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quant. Info. and Computation* 3, 535-552 (2003).

[51] Navascues, M. and Acin, A. Security bounds for continuous variables quantum key distribution. *Phys. Rev. Lett*. 94, 020505 (2005).

[52] Pirandola, S., Mancini, S., Lloyd, S. and Braunstein, S. L. Continuous-variable Quantum Cryptography using Two-Way Quantum Communication, *Nature Physics* 4, 726 - 730 (2008).

[53] Pirandola, S., Garcia-Patron, R., Braunstein, S. L. and Lloyd, S. *Phys. Rev. Lett.* 102 050503. (2009).

[54] Pirandola, S., Serafini, A. and Lloyd, S. *Phys. Rev. A* 79 052327. (2009).

[55] Pirandola, S., Braunstein, S. L. and Lloyd, S. *Phys. Rev. Lett.* 101 200504 (2008).

[56] Weedbrook, C., Pirandola, S., Lloyd, S. and Ralph, T. *Phys. Rev. Lett.* 105 110501 (2010).

[57] Weedbrook, C., Pirandola, S., Garcia-Patron, R., Cerf, N. J., Ralph, T., Shapiro, J. and Lloyd, S. *Rev. Mod. Phys.* 84, 621 (2012).

[58] Shieh, W. and Djordjevic, I. *OFDM for Optical Communications*. Elsevier (2010).

[59] Navascues, M., Grosshans, F. and Acin, A. Optimality of Gaussian Attacks in Continuous-variable Quantum Cryptography, *Phys. Rev. Lett.* 97, 190502 (2006).

[60] Garcia-Patron, R. and Cerf, N. J. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Phys. Rev. Lett.* 97, 190503 (2006).

[61] Grosshans, F. Collective attacks and unconditional security in continuous variable quantum key distribution. *Phys. Rev. Lett.* 94, 020504 (2005).

[62] Laudenbach, F., Pacher, C., Fred Fung, C-H., Poppe, A., Peev, M., Schrenk, B., Hentschel, M., Walther, P. and Hubel, H. Continuous-Variable Quantum Key Distribution with Gaussian Modulation - The Theory of Practical Implementations, *Adv. Quantum Technol. 1800011* (2018).

[63] Diamanti, E. and Leverrier, A. Distributing Secret Keys with Quantum Continuous Variables: Principle, Security, *Entropy*, 17, 6072-6092; doi:10.3390/e17096072 and Implementations (2015).

[64] Stucki, D. et al. High speed coherent one-way quantum key distribution prototype, *Optics Express*, Vol. 17, Issue 16, pp. 13326-13334 (2009).

[65] Inoue, K., Takesue, H. and Honjo, T. DPS quantum key distribution and related technologies, *SPIE Proceedings* Vol 7236, Quantum Communications Realized II; 72360I (2009).

[66] Enzer, D., Hadley, P., Gughes, R., Peterson, C. and Kwiat, P., Entangled-photon six-state quantum cryptography, *New Journal of Physics*, pp 45.1-45.8 (2002).

[67] Lo, H., Ma, X. and Chen, K. Decoy state quantum key distribution, *Phys. Rev. Lett*. 94, 230504, http://arxiv.org/pdf/quant-ph/0411004 (2005).

[68] Gyongyosi, L. and Imre, S. Adaptive multicarrier quadrature division modulation for long-distance continuous-variable quantum key distribution, *Proc. SPIE 9123, Quantum Information and Computation XII*, 912307; doi:10.1117/12.2050095, From Conference Volume 9123, Quantum Information and Computation XII, Baltimore, Maryland, USA (2014).

[69] Gyongyosi, L. and Imre, S. Secret Key Rate Proof of Multicarrier Continuous-Variable Quantum Key Distribution, *Int. J. Commun. Syst*. (Wiley), DOI: 10.1002/dac.3865, (2018).

[70] Gyongyosi, L. and Imre, S. Multiple Access Multicarrier Continuous-Variable Quantum Key Distribution, *Chaos, Solitons and Fractals*, Elsevier, DOI: 10.1016/j. Chaos.2018.07.006, ISSN: 0960-0779, (2018).

[71] Gyongyosi, L. and Imre, S. Gaussian Quadrature Inference for Multicarrier Continuous-Variable Quantum Key Distribution, *Quantum Studies: Mathematics and Foundations*, Springer Nature, DOI: 10.1007/s40509-019-00183-9, (2019).

[72] Gyongyosi, L. and Imre, S. Diversity Space of Multicarrier Continuous-Variable Quantum Key Distribution, *Int. J. Commun. Syst.* (Wiley), ISSN: 1099-1131, (2019).

[73] Zhang, H., Mao, Y., Huang, D., Li, J., Zhang, L. and Guo, Y. Security analysis of orthogonal-frequency-division-multiplexing-based continuous-variable quantum key distribution with imperfect modulation, *Phys. Rev. A* 97, 052328 (2018).

[74] Jouguet, P. Kunz-Jacques, S. and Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation, *Phys. Rev. A* 84, 062317. (2011).

[75] Renner, R. and Cirac, J. I. de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography, *Physcal Review Letters* 102, 110504 (2009).

[76] Leverrier, A., García-Patron, R., Renner, R. and Cerf, N. J. Security of Continuous-Variable Quantum Key Distribution Against General Attacks, *Physcal Review Letters* 110, 030502. (2013).

[77] Gyongyosi, L. and Imre, S. Low-Dimensional Reconciliation for Continuous-Variable Quantum Key Distribution, *Appl. Sci.,* doi: 10.3390/app8010087, ISSN 2076-3417, (2018).

[78] Vernam, G. S. Cipher printing telegraph systems for secret wire and radio telegraphic communications, *Transactions of the American Institute of Electrical Engineers*, Vol. XLV, No.2, pp. 295-301 (1926).

[79] Shannon, C. E. Communication theory of secrecy systems. *Bell Syst Technol J*, 28, pp. 656-715 (1949).

[80] Van Meter, R. *Quantum Networking*. ISBN 1118648927, 9781118648926, John Wiley and Sons Ltd (2014).

[81] Lloyd, S., Shapiro, J. H., Wong, F. N. C., Kumar, P., Shahriar, S. M. and Yuen, H. P. Infrastructure for the quantum Internet. *ACM SIGCOMM Computer Communication Review*, 34, 9–20 (2004).

[82] Kimble, H. J. The quantum Internet. *Nature*, 453:1023–1030 (2008).

[83] Caleffi, M., Cacciapuoti, A. S. and Bianchi, G. Quantum Internet: from Communication to Distributed Computing, *aXiv:1805.04360* (2018).

[84] Castelvecchi, D. The quantum internet has arrived, *Nature*, News and Comment, https://www. Nature. Com/articles/d41586-018-01835-3, (2018).

[85] Cacciapuoti, A. S., Caleffi, M., Tafuri, F., Cataliotti, F. S., Gherardini, S. and Bianchi, G. Quantum Internet: Networking Challenges in Distributed Quantum Computing, *arXiv:1810.08421* (2018).

[86] Caleffi, M. End-to-End Entanglement Rate: Toward a Quantum Route Metric, 2017 *IEEE Globecom*, DOI: 10.1109/GLOCOMW.2017.8269080, (2018).
[87] Caleffi, M. Optimal Routing for Quantum Networks, *IEEE Access*, Vol 5, DOI: 10.1109/ACCESS.2017.2763325 (2017).
[88] Liao, S.-K., Wen-Qi, C., Handsteiner, J. et al. Satellite-Relayed Intercontinental Quantum Network. *Phys. Rev. Lett*. 120, 030501, (2018).
[89] Muralidharan, S., Kim, J., Lutkenhaus, N., Lukin, M. D. and Jiang. L. Ultrafast and Fault-Tolerant Quantum Communication across Long Distances, *Phys. Rev. Lett*. 112, 250501 (2014).
[90] Rozpedek, F., Schiet, T., Thinh, L., Elkouss, D., Doherty, A., and S. Wehner, Optimizing practical entanglement distillation, *Phys. Rev. A* 97, 062333 (2018).
[91] Van Meter, R., Ladd, T. D., Munro, W. J. and Nemoto, K. System Design for a Long-Line Quantum Repeater, *IEEE/ACM Transactions on Networking* 17(3), 1002-1013, (2009).
[92] Van Meter, R., Satoh, T., Ladd, T. D., Munro, W. J. and Nemoto, K. Path selection for quantum repeater networks, *Networking Science*, Volume 3, Issue 1–4, pp 82–95, (2013).
[93] Pirandola, S., Laurenza, R., Ottaviani, C. and Banchi, L. Fundamental limits of repeaterless quantum communications, *Nature Communications*, 15043, doi:10.1038/ncomms15043 (2017).
[94] Muralidharan, S., Kim, J., Lutkenhaus, N., Lukin, M. D. and Jiang. L. Ultrafast and Fault-Tolerant Quantum Communication across Long Distances, *Phys. Rev. Lett*. 112, 250501 (2014).
[95] Bacsardi, L. On the Way to Quantum-Based Satellite Communication, *IEEE Comm. Mag.* 51:(08) pp. 50-55. (2013).
[96] Van Meter, R. and Devitt, S. J. Local and Distributed Quantum Computation, *IEEE Computer* 49(9), 31-42 (2016).
[97] Pirandola, S. Capacities of repeater-assisted quantum communications, *arXiv:1601.00966* (2016).
[98] Wehner, S., Elkouss, D., and R. Hanson. Quantum internet: A vision for the road ahead, *Science* 362, 6412, (2018).
[99] Quantum Internet Research Group (QIRG), web: https://datatracker.ietf.org/rg/qirg/about/ (2018).
[100] Humphreys, P. et al., Deterministic delivery of remote entanglement on a quantum network, *Nature* 558, (2018).
[101] Hensen, B. et al., Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, *Nature* 526, (2015).
[102] Hucul, D. et al., Modular entanglement of atomic qubits using photons and phonons, *Nature Physics* 11(1), (2015).
[103] Sangouard, N. et al., Quantum repeaters based on atomic ensembles and linear optics, *Reviews of Modern Physics* 83, 33, (2011).
[104] Pirandola, S., Braunstein, S. L., Laurenza, R., Ottaviani, C., Cope, T. P. W., Spedalieri, G. and Banchi, L. Theory of channel simulation and bounds for private communication, *Quantum Sci. Technol*. 3, 035009 (2018).
[105] Gyongyosi, L. and Imre, S. A Survey on Quantum Computing Technology, *Computer Science Review*, Elsevier, DOI: 10.1016/j. Cosrev.2018.11.002, ISSN: 1574-0137, (2018).
[106] Lloyd, S. Capacity of the noisy quantum channel. *Physical Rev. A*, 55:1613–1622 (1997).
[107] Gisin, N. and Thew, R. Quantum Communication. *Nature Photon.* 1, 165-171 (2007).
[108] Leung, D., Oppenheim, J. and Winter, A. *IEEE Trans. Inf. Theory* 56, 3478-90. (2010).
[109] Kobayashi, H., Le Gall, F., Nishimura, H. and Rotteler, M. Perfect quantum network communication protocol based on classical network coding, *Proceedings of 2010 IEEE International Symposium on Information Theory* (ISIT) pp 2686-90. (2010).
[110] Goebel, A. M., Wagenknecht, G., Zhang, Q., Chen, Y., Chen, K., Schmiedmayer, J. and Pan, J. W. Multistage Entanglement Swapping. *Phys. Rev. Lett.* 101, 080403 (2008).
[111] Xiao, Y. F., Gong, Q. Optical microcavity: from fundamental physics to functional photonics devices. *Science Bulletin*, 61, 185-186 (2016).
[112] Gyongyosi, L. and Imre, S. Decentralized Base-Graph Routing for the Quantum Internet, *Physical Review A*, American Physical Society, DOI: 10.1103/PhysRevA.98.022310 (2018).
[113] Gyongyosi, L. and Imre, S. Multilayer Optimization for the Quantum Internet, *Scientific Reports*, Nature, DOI:10.1038/s41598-018-30957-x, (2018).
[114] Gyongyosi, L. and Imre, S. Entanglement Availability Differentiation Service for the Quantum Internet, *Scientific Reports*, Nature, (DOI:10.1038/s41598-018-28801-3), https://www.nature.com/articles/s41598-018-28801-3 (2018).
[115] Gyongyosi, L. and Imre, S. Entanglement-Gradient Routing for Quantum Networks, *Scientific Reports*, Nature, (DOI:10.1038/s41598-017-14394-w), https://www.nature.com/articles/s41598-017-14394-w (2017).
[116] Gyongyosi, L. and Imre, S. Opportunistic Entanglement Distribution for the Quantum Internet, *Scientific Reports*, Nature, DOI:10.1038/s41598-019-38495-w, (2019).
[117] Chou, C., Laurat, J., Deng, H., Choi, K. S., de Riedmatten, H., Felinto, D. and Kimble, H. J. Functional quantum nodes for entanglement distribution over scalable quantum networks. *Science*, 316(5829):1316–1320 (2007).
[118] Zhang, W. et al. Quantum Secure Direct Communication with Quantum Memory. *Phys. Rev. Lett.* 118, 220501 (2017).
[119] Rozpedek, F., Schiet, T., Thinh, L., Elkouss, D., Doherty, A., and S. Wehner, Optimizing practical entanglement distillation, *Phys. Rev. A* 97, 062333 (2018).

**Laszlo Gyongyosi** received degrees from the Budapest University of Technology and Economics (BME). He receives the D.Sc. degree from the Hungarian Academy of Sciences (MTA) in 2019. His research interests include quantum computation and communications, quantum information, and quantum Shannon theory. He is a research scientist at the Department of Networked Systems and Services at the BME, in contribution with the University of Southampton (Soton), U.K., and Hungarian Academy of Sciences.

**Sandor Imre** (M'93–SM'12) received the Dr.Univ. degree in probability theory and statistics in 1996, the Ph.D. degree in 1999, and the D.Sc. degree from the Hungarian Academy of Sciences in 2007. He is a Professor and the Head of the Department of Networked Systems and Services at the Budapest University of Technology (BME). He is chairman of Telecommunication Scientific Committee of Hungarian Academy of Sciences. He was invited to join the Mobile Innovation Centre as R&D Director in 2005. His research interests include mobile and wireless systems, quantum computing, and communications. He has contributed to different wireless access technologies, mobility protocols and their game theoretical approaches, reconfigurable systems, and quantum computing based algorithms and protocols.

**Laszlo Bacsardi** received his M.Sc. degree in 2006 in Computer Engineering from the Budapest University of Technology and Economics (BME). He wrote his PhD thesis on the possible connection between space communications and quantum communications at the BME Department of Telecommunications in 2012. From 2009, he works at the University of Sopron, Hungary (formerly known as University of West Hungary). He holds an associate professor position at the Institute of Informatics and Economics, University of Sopron. He is Research Fellow at the Department of Networked Systems and Services, BME. His current research interests are quantum computing, quantum communications and ICT solutions developed for Industry 4.0. He is the Vice President of the Hungarian Astronautical Society (MANT), which is the oldest Hungarian non-profit space association founded in 1956. Furthermore, he is member of IEEE, AIAA and the HTE as well as alumni member of the UN established Space Generation Advisory Council (SGAC). In 2017, he won the IAF Young Space Leadership Award.