The Status of Quantum-Key-Distribution-Based Long-Term Secure Internet Communication

Matthias Geihs, Oleg Nikiforov, Denise Demirel, Alexander Sauer, Denis Butin, Felix Günther, Gernot Alber, Thomas Walther, and Johannes Buchmann

Abstract—A large amount of sensitive data must remain accessible for decades or even centuries (e.g, electronic health records, governmental documents). Communicating such data over the Internet requires long-term secure communication channels, which, in turn, require robust key distribution protocols. Currently used key distribution protocols, however, are not designed for long-term security. Their security is either threatened by quantum computers, or, in principle, due to their reliance on computational problems. Quantum key distribution (QKD) protocols are information-theoretically secure and thereby offer long-term security against computational attacks. However, significant obstacles to their real-world use remain. This position paper, which is a multidisciplinary effort of computer scientists and physicists, systematizes knowledge about challenges of and strategies for realizing long-term secure Internet communication from QKD. We first analyze the performance and security of existing point-to-point QKD technology. Then, we discuss several approaches to enabling QKD in large-scale multi-user networks. Finally, we list important challenges that need to be addressed in order to make QKD-based long-term secure communication on the Internet practical.

Index Terms—Communication security, quantum key distribution, confidentiality, long-term security, information-theoretic security

1 Introduction

The Internet is arguably the most important communication medium today, which allows any two clients around the globe to instantly communicate with each other. If sensitive information is about to be communicated (e.g., medical records or governmental documents), secure connections need to be established in order to protect confidentiality, integrity, authenticity of the communicated data. Such secure connection protocols combine a key distribution protocol with a channel protocol, a prominent example being the Transport Layer Security (TLS) protocol [1]. First, the key distribution protocol is run to establish a common secret key unknown to a potential eavesdropper tapping the communication. Then, this key is used in the channel protocol to encrypt and authenticate the transmitted data.

Currently, the most commonly used key distribution protocol is based on the Diffie–Hellman key exchange protocol [2], which provides so-called *computational security*: the protocol is secure only as long as discrete logarithms in large finite fields cannot be computed efficiently. However, it has been shown that quantum computers can efficiently compute such discrete logarithms [3], and thus, Diffie–Hellman key exchange is rendered insecure once quantum computers are available. Recently, alternative key distribution protocols based on lattice cryptography have been proposed (e.g., [4], [5]), which are conjectured secure against quantum computers. However, their security still relies on computational problems, which can be solved given enough computation power and time. Therefore, computationally secure key distribution protocols achieve security only for a limited time period. Once the computational problem is solved, the confidentiality of all transmitted data is lost.

An alternative to computationally secure key distribution is *information-theoretically secure* key distribution. Information-theoretically secure protocols withstand any computational attacks (be it, e.g., advances in quantum computing or brute force attacks) and therefore provide long-term security. Connections providing long-term confidentiality require information-theoretically secure key distribution and encryption. The integrity demands for such a channel are usually only temporary (computational), that is, it is sufficient to guarantee integrity while the data is in transit. Despite substantial efforts to define, understand, and construct computationally secure channels (originating, e.g., from [6]), a thorough understanding of how to construct information-theoretically secure channels achieving standard security goals of confidentiality and integrity as well as replay and reordering protection is still lacking. For information-theoretic encryption, one-time pad encryption [7] is an optimal solution. There exist several candidates for information-theoretically secure key distribution. A naive approach is to distribute keys using a trusted courier that physically delivers a generated key stored on a hard drive. This approach, however, suffers from obvious cost and latency issues as it requires moving hard disks around the globe. Other approaches for information-theoretically secure

- *M. Geihs, O. Nikiforov, D. Demirel, A. Sauer, D. Butin, G. Alber, T. Walther, and J. Buchmann are with the Technische Universität Darmstadt, Darmstadt 64289, Germany. E-mail: {mgeihs, ddemirel, dbutin, buchmann}@cdc.informatik.tu-darmstadt.de, {oleg.nikiforov, alexander.sauer, gernot.alber, thomas.walther}@physik.tu-darmstadt.de.*
- *F. Günther is with the University of California San Diego, La Jolla, CA 92093 USA. E-mail: guenther@cs.tu-darmstadt.de.*

Manuscript received 14 May 2018; revised 25 Mar. 2019; accepted 25 Apr. 2019. Date of publication 30 Apr. 2019; date of current version 5 Mar. 2021.
(Corresponding author: Matthias Geihs.)
Recommended for acceptance by P. Yoo and Z. Tari.
Digital Object Identifier no. 10.1109/TSUSC.2019.2913948

key distribution are protocols in the bounded storage model [8] or the noisy channel model [9]. However, it is currently unclear how to realize them in practice [10]. The most promising approach for information-theoretically secure key distribution currently is quantum key distribution (QKD). The security of QKD is based on the laws of quantum physics and its feasibility has already been demonstrated in many field tests [11], [12], [13]. However, there remain several technical challenges that need to be addressed in order to make QKD-based long-term secure communication on the Internet practical. The performance and security of QKD implementations is still an issue. Furthermore, most QKD technology focuses on the two-party setting, but further technology is required for enabling QKD in large-scale multi-user networks (e.g., the Internet).

In this position paper, we classify and compare the building blocks required for QKD-based Internet communication. Specifically, we split our analysis of the state of the art in two.

1) First, we examine QKD protocols in the two party setting. To this end, we classify point-to-point QKD protocols by functionality, by information preparation method and by the type of variables used for the information carriers. We then compare such protocols in terms of performance and security.
2) Second, we turn to the problem of large-scale communication networks. To be scalable, such networks cannot rely on dedicated communication channels between every two parties. Large networks supporting QKD-based communication thus require *hubs*, i.e., multi-link nodes. Current hub technology does not support QKD. We classify existing QKD-supporting approaches in two categories: trusted-node networks and all-quantum networks. The practicability of both approaches is then compared.

From the above analysis, we derive key challenges that must be solved for large-scale QKD networks to become practical.

The goal of this work is to provide an overview of this (inherently interdisciplinary) topic comprehensible by both computer scientists and physicists. At the same time, we aim for a similar level of detail both for the computer science and physics facets of this topic. Our hope is therefore to offer an accessible overview, fostering interdisciplinary research.

The remainder of this paper is structured as follows. We first discuss the current state of two-party QKD technology with regards to performance and security (Section 2). We then discuss several approaches to enabling QKD in large-scale multi-user networks (Section 3). Finally, we summarize our findings, discuss current standardization and deployment efforts and list challenges remaining to be addressed for QKD-based long-term secure communication on the Internet to be practical (Section 4).

2 QKD Between Two Parties

In this section, we describe the state of the art of point-to-point QKD technology. We first explain relevant concepts of quantum physics. Then, we categorize and summarize prominent QKD protocols. Next, we compare the performance of the protocols and discuss security models and attacks on protocol implementations.

2.1 Quantum Physics Background

QKD protocols rely on fundamental laws of quantum physics: the typical change of state of a quantum object after a measurement (collapse of the wave function) and the impossibility to copy a quantum state without disturbing the state of the original particle (no-cloning theorem). The security of QKD protocols relies on the fact that a potential eavesdropper reveals himself by the process of his attack. Eavesdropping introduces inevitable errors to the exchanged quantum states that can later be detected by communicating parties. At the core of every QKD protocol lies the exchange of quantum states. In contrast to modern optical communication systems, where classical bits are encoded as an absent (0) or present (1) “classical” laser pulse in a certain time interval, QKD uses *qubits*—quantum objects that can carry more than one bit of classical information at a time and exhibit a behavior that cannot be described within classical physics. Very different physical systems can serve as qubits: single photons, weak laser pulses, Fock states and squeezed states of light, half-spin quantum systems as trapped atoms and ions, or Rydberg atoms coupled to a cavity [14]. Quantum information can be encoded using different types of *observables*, i.e., physically measurable properties of qubits. Information can e.g., be encoded using polarization, phase, creation time of single photons, or quadrature, phase and amplitude of multi-photon coherent laser states [14], [15].

2.2 Common Functionality

We now sketch functionality common to all QKD protocols discussed later. These protocols comprise a raw key distribution phase and a post-processing phase.

2.2.1 Raw Key Distribution

The first part of every QKD protocol establishes a raw secret key by transmission of qubits over a special *quantum channel*. Ideally, such a channel should not alter the encoded information due to interaction of qubits with the transport medium (e.g., a change of polarization in a glass fiber). Distortions must be kept low in order to fulfill the requirements for a successful key distribution, because disturbances of the qubit states may have also been caused by an attacker.

During the raw key distribution phase, the communicating partners exchange qubits over the quantum channel. Upon receiving a qubit, the recipient performs a measurement on some observable of the qubit and decodes a classical bit from its result according to a procedure determined by the chosen QKD protocol. Afterward, the communicating partners consult about their measurements using a classical authenticated channel. This procedure is specific to each QKD protocol and the result is a raw secret key. If they deduce that an attacker might have disturbed the quantum information too severely, the key distribution has to be started over.

2.2.2 Post-Processing

After the raw key distribution phase, each of the communicating partners has obtained an individual raw key. Perfectly correlated keys are improbable due to experimental imperfections, so error correction (e.g., *low density parity check* [16], *cascade* [17], or *polar codes* [18]) has to be performed.

Afterward, privacy amplification is applied to generate the final key from the error-corrected raw key. This ensures security even against an eavesdropper that may have observed a

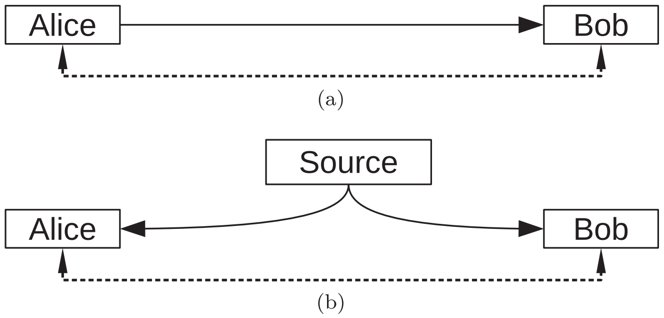

Fig. 1. (a) Prepare-and-measure protocol (e.g., BB84 [30]). (b) Entanglement-based protocol (e.g., E91 [35]). Solid line denotes the quantum channel, dashed line stands for the authenticated classical channel. Arrows denote the direction of information flow.

small number of bits undetected during the raw key exchange or the error correction. The resulting secret key can then be used as a key for one-time pad or Advanced Encryption Standard (AES) encryption.

As described above, QKD requires an authenticated classical channel between the communicating partners. Such an authenticated channel can be established using a short pre-shared secret or by relying on a typical secure connection (e.g., TLS). Recently, it was proposed to realize authenticated channels based on laws of quantum physics [19], [20]. We remark that the authenticated channel used in a QKD protocol needs to remain secure only while the QKD protocol is executed.

2.3 Protocol Families

There are many different ways QKD protocols are implemented. For our analysis, we categorize them by the way information is prepared (prepare-and-measure or entanglement-based) and by the type of variables (discrete variables, continuous variables, or distributed phase reference).

2.3.1 Classification by Information Preparation Method

We describe categories for QKD protocols based on how the quantum states are prepared.

2.3.1.1 Prepare-and-measure: In prepare-and-measure (PaM) protocols (Fig. 1a), a sender Alice actively prepares an information carrier, encodes information within it and sends it to one or more recipients. Prominent representatives of this protocol category are the protocol developed by Bennett and Brassard (BB84) [30] or derived protocols, such as [31], [32].

2.3.1.2 Entanglement-based: In entanglement-based (EB) protocols (Fig. 1b), a source produces *entangled* particles—multiple quantum objects that can be described by a correlated quantum state violating local realism [33]. A measurement on some observable of one of the objects instantly affects the state of the other object. The states of the entangled particles are then measured by the communicating parties. *Bell tests* are performed in order to verify the entanglement of the received particles and to detect eavesdropping [33], [34]. By the non-classical correlation between the particles, Alice and Bob are assured to hold a common secret without direct exchange of information. A prominent representative of this protocol category is the E91 protocol developed by Ekert [35].

2.3.2 Classification by Variable Type

QKD protocols can also be classified by the type of variables used for the information carriers.

2.3.2.1: Discrete variables (DV): For the protocols with discrete variables, the values of the information carrying observables are discrete. Most commonly, qubits are transmitted using single photons or weak laser pulses. In principle, half-spin particles (e.g., electrons) can also be used, but the transmission of such particles is problematic. The information can be encoded, for example, in time, polarization, spin, or phase. The source can be implemented as a prepare-and-measure system or as an entanglement-based system. DV protocols require expensive and inefficient single-photon source and detector devices. Prominent representatives of this protocol category are [30], [31], [35], [36].

2.3.2.2 Continuous variables (CV): Continuous variable protocols are an alternative to DV protocols that, instead of qubits (e.g., single photons and weak laser pulses), use many particle states (e.g., squeezed or coherent states of light). Hereby no discrete variables are detected (e.g., zeros and ones) but the continuous spectrum of the quadrature components of light is observed (e.g., by homodyning techniques [37]).

Quantum states in CV protocols are also detected differently than in DV protocols. Here, standard components for quantum communication are used. For instance, homodyne or heterodyne detection schemes [37] are employed. This is much faster and more efficient than the detection of single photons. Most of the existing CV protocols can be implemented as a prepare-and-measure variant or an entanglement-based variant. Prominent representatives of this protocol category are [38], [39].

2.3.2.3 Distributed phase reference (DPR): A third family of QKD protocols, called distributed phase reference protocols, uses discrete variables for encoding of information, but at the same time the security is guaranteed by observing the coherence of subsequent pulses. Bits may be encoded in a sequence of pairs of pulses [32] or in the phase of subsequent pulses [40]. The two approaches may also be combined into a two dimensional QKD protocol [41], where several bits can be encoded by two subsequent pulses. DPR protocols require similar devices as DV protocols, namely, single photon sources and detectors. Prominent representatives of this protocol category are [32], [40], [41].

2.4 Implementation and Performance

The aforementioned QKD protocols can be run over free space or via glass fibers. Depending on the communication medium, different secret key generation rates and effective distances are achieved. Typical key rates for DV protocols are up to several kbits^{-1} on the distance of several 10 km and up to several bits^{-1} over approximately 100 km distance (cf. Table 1) via optical fiber. For CV protocols the key rate is comparable, i.e., up to 10 kbits^{-1} for channels of a few km and up to 150 km effective distance. In Table 1, we list performance figures of fiber-based QKD technology. For all QKD protocols, the key rate decreases exponentially with the communication distance due to noise and losses in the quantum channel. It has been shown that the maximum achievable key rate of QKD is bounded by a function that solely depends on the channel loss [42], [43]. Free space QKD systems can reach higher distances, since the attenuation coefficient of air is much smaller than that of fiber. Recently, satellite-based QKD technology has achieved important milestones. In 2017, DV-based quantum key distribution via satellite has been demonstrated over a distance of 1200 km at a key rate of 1 kbits^{-1} [44]. In 2018,

TABLE 1
Performance Comparison of Point-to-Point QKD Technology

Experiment	Type	Key rate at 100 km	Maximal distance
Boaron [21] (2018)	PaM-DPR	14 kbit s^{-1}	421 km
Yin [22] (2016)	EB-DV	2 kbit s^{-1}	404 km
Korzh [23] (2015)	PaM-DPR	10 kbit s^{-1}	307 km
Wang [24] (2012)	PaM-DPR	20 kbit s^{-1}	260 km
Stucki [25] (2009)	PaM-DPR	6 kbit s^{-1}	250 km
Grünenfelder [26] (2018)	PaM-DV	50 kbit s^{-1}	200 km
Huang [27] (2016)	PaM-CV	500 bits^{-1}	100 km
Honjo [28] (2007)	EB-DV	0.59 bits^{-1}	100 km
Jouguet [29] (2013)	EB-CV	200 bits^{-1} (80 km)	80 km

TABLE 2
Qualitative Comparison of QKD Protocol Families

	Deployment	Key Rate	Distance	Cost-Effectiveness
DV	+	+	+	+
CV	+	++	+	++
DPR	++	++	++	+

intercontinental QKD via satellite between Graz, Austria, and Shanghai, China, has been demonstrated [45]. Furthermore, standard telecommunication satellites were found capable of implementing CV-based QKD protocols [46].

Besides the key rate and distance, the compatibility of the system with the existing communication infrastructure is important. For example, DV QKD protocols require expensive single photon detectors, single- or entangled-photon sources and precise time measuring devices. Simultaneously, the typical distribution distances and rates for the secret key distribution allow for use only in metropolitan network areas. Imperfections in the single-photon sources make photon number splitting attacks possible (see Section 2.5).

CV protocols are a more recent class of protocols that offer higher secret key rates and lower costs for implementation, because neither single photon sources nor single photon detectors are required. Standard components for optical communication can be used. A recent experiment showed that CV protocols can be applied even in a geostationary satellite for standard optical communication achieving much longer communication distances [46]. However, the security of CV protocols against side-channel attacks is less understood as for DV protocols [37], [47] (cf. Section 2.5).

DPR protocols currently achieve the best performance in terms of maximal key distribution distance (Table 1). Furthermore, multi-dimensional QKD schemes, like DPR protocols, allow to transmit more than one bit of classical information in a single qubit [41].

For all protocol types, the possibility of quantum channel and classical channel integration into a single glass fiber is being investigated [48], [49]. In this setting, qubits are transmitted simultaneously with classical communication pulses at different wavelengths to avoid cross-talk. This would lower the costs for QKD deployment. We summarize our observations about the different QKD protocol families in Table 2.

2.5 Security

A QKD protocol is considered secure if, after a protocol execution, the communication partners, Alice and Bob, know a common secret key, and an eavesdropper on the channel, Eve, could not obtain any information about the key. We now summarize work analyzing the security of QKD protocols and discuss theoretical and practical attacks on implementations of QKD.

2.5.1 Theoretical Analysis

When analyzing the security of a QKD protocol the goal is to show security against a powerful attacker, Eve, that potentially possesses perfect technology. For example, Eve may be able to extract and store qubits for an arbitrary duration and perform any quantum operation or measurement on them. However, according to fundamental quantum physical laws, Eve can neither clone nor measure the state of the system perfectly and resend a new particle without leaving a trace due to the no-cloning theorem [50]. In addition, usually the existence of an authenticated classical channel between the communication partners or a short pre-shared key is assumed. This is necessary to guarantee data integrity and authenticity, so that Eve cannot perform an impersonation attack or change the classical data sent. We stress that the authenticated channel does not need to provide any confidentiality guarantees.

An attack on a QKD system is called *individual* if Eve measures each qubit separately. In a *collective* attack, Eve still interacts with each qubit separately, but she may measure all the auxiliary systems used for the interactions jointly. If Eve is allowed to attack several sent qubits simultaneously, the attack is called *coherent*. Renner et al. [51] prove the security of a wide range of QKD protocols against coherent attacks.

QKD security proofs rely on information theory and do not depend on computational hardness assumptions. This fundamental difference in comparison to currently used key distribution methods guarantees the long-term security of QKD. However, idealized assumptions in QKD security proofs lead to incomplete security models. For realistic security guarantees about actual implementations, more assumptions regarding hardware and software are required. Attacks exploiting imperfect devices and insecure software may be possible, as we describe below. Depending on protocol families, proven security guarantees against theoretical attacks vary. While some DV protocols have been shown to be unconditionally secure [52], [53], similar proofs for CV and DPR protocols are still missing. An overview of security proofs for CV protocols is given by Diamanti, Kogias, Laudenbach and others [37], [47], [54]. A security analysis of DPR protocols is provided by Moroder et al. [55].

As an example, we discuss the security of BB84 against an *intercept-resend attack*, which is a special case of an individual attack. In this attack, Eve chooses a basis randomly and detects the state of particles. She has a probability of 50 percent to choose a wrong basis. Afterward, she prepares a replacement for the detected qubit and sends it to Bob. In that way, she induces a 25 percent QBER in Bob's key. However, as shown by Shor and Preskill, Alice and Bob know the key distribution session might have been compromised [53] if the QBER exceeds 11 percent. Other strategies, for example, detection of not every qubit or detection using an intermediate basis are disadvantageous for Eve, since she obtains less information about the secret key. In the case of entanglement-based protocols, during the measurement of qubits, Eve destroys the non-classical correlations between the particles, so a Bell test during

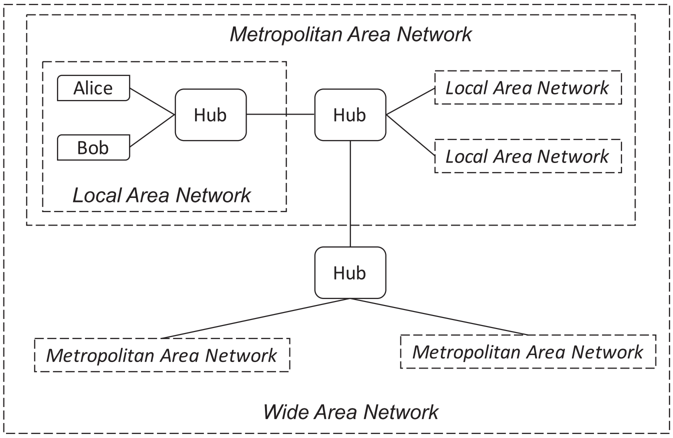

Fig. 2. The various network layers of the Internet that are connected via hubs.

the key processing fails. In summary, security proofs for QKD protocols show that an attacker reveals himself when trying to eavesdrop on the quantum states sent over the network. This is what makes QKD so powerful in comparison to classical key distribution.

2.5.2 Attacks on Implementations

Even for protocols that have been proven unconditionally secure, side-channels and non-perfect setups can lead to weaknesses. Implementations of QKD protocols thus require an extended security analysis. In particular, side-channel vulnerabilities and non-perfect setup assumptions must be considered and therefore security proofs most likely have to be adapted.

As an example, the creation of tailored single photons is non-trivial. In most cases, there is a non-negligible probability for pulses with a photon number larger than 1. Thus, if there is more than one photon in a weak laser pulse, Eve can pick some photons with a beam splitter and gain information without being noticed. This type of attack is called a *photon number splitting attack*. As a countermeasure, protocols have been modified: decoy states have been added to BB84 [56] and new protocols, such as SARG04, have been developed [31].

Hijacking a quantum channel by a *Trojan horse attack*, information about Alice's and Bob's setups can be extracted [57] or even manipulated [58]. For example, if Eve obtains information about Alice's choice of bases in real-time, she can perform a successful intercept-resend attack as she is no longer limited to guessing the bases randomly.

Another possibility is bright illumination of Bob's detectors via the quantum channel. This can allow the attacker to control the measurement results of Bob. Lydersen et al. describe how an attacker could successfully obtain the complete secret key and remain unnoticed [58].

Crucially, all these attacks must be performed physically and during the actual key distribution. This is a fundamental difference to classical key distribution protocols, whose security might be broken by attacks that were unknown at the time of the distribution.

2.5.3 Device-Independent QKD

Device-independent QKD is an approach aiming to dispense with the assumption of trust in the own setup hardware [59]. Hereby, the security of the whole QKD system should be evaluated by a quantum-correlation test, i.e., a Bell test, similar to the E91 protocol [60]. Since purely device-independent protocols are hard to realize, measurement-device-independent QKD protocols have been developed [22], [61], [62].

3 QKD in Large-Scale Networks

So far, we have discussed QKD technology for a setting where two communicating parties are connected directly by a dedicated quantum channel over a short distance. However, in large-scale communication networks (e.g., the Internet), dedicated communication channels usually do not exist between any two parties. Moreover, physical distances between communication partners may be large while low latency and high throughput capabilities are often required. On the Internet, the problem of enabling any two parties to connect and communicate with each other is typically solved by employing network hubs through which the communication is routed (Fig. 2). Routing protocols such as BGP [63] are typically used to this end. However, current hub architecture and protocols do not support QKD and, thus, new technology is required for realizing QKD in large-scale networks. This involves the development of QKD hub architecture and corresponding routing protocols. It also calls for the definition of interfaces between the QKD architecture and the application layer.

In the following, we discuss different approaches for realizing QKD networks and compare them with each other. QKD hubs can be realized using standard telecommunication techniques, e.g., wave- or time-division multiplexing, or active optical switching. However, those methods do not overcome the distance limitations of QKD as discussed in Section 2, but only repeaters can extend the effective range of a QKD connection. Two types of repeaters are being developed: trusted repeaters and quantum repeaters. They enable two fundamentally different types of QKD networks: *trusted-node networks* and *all-quantum networks*.

3.1 Trusted-Node Networks

The trusted node approach requires a chain of repeaters, mutually connected by a two-party QKD system and relaying a secret key to one another step-by-step. Each of the repeaters thus knows the key, so the nodes must be secure and trustworthy. This approach has been investigated for a decade. Prominent examples include the SECOQC Network [12], the Tokyo QKD Network [13].

The technology of trusted-node networks is already beyond the research stage, and is on the threshold of commercial success. In China, a 2000-km-long link connecting Beijing to Jinan, Hefei, and Shanghai was completed in 2017 [64]. The telecommunications operator SK Telecom is currently implementing a trusted-nodes-based network in South Korea. The planned completion date is 2020 [65].

In detail, a trusted-node network works as follows. Each of the communication partners Alice and Bob is connected to a nearby trusted node. The trusted nodes are also connected to each other (Fig. 3). For Alice and Bob to establish a secure connection, a path between them through the trusted-node network layer is established, using routing and load-balancing protocols [66], [67]. They then exchange keys with their respective trusted node. The trusted nodes also exchange keys with each other. Finally, the communication partners

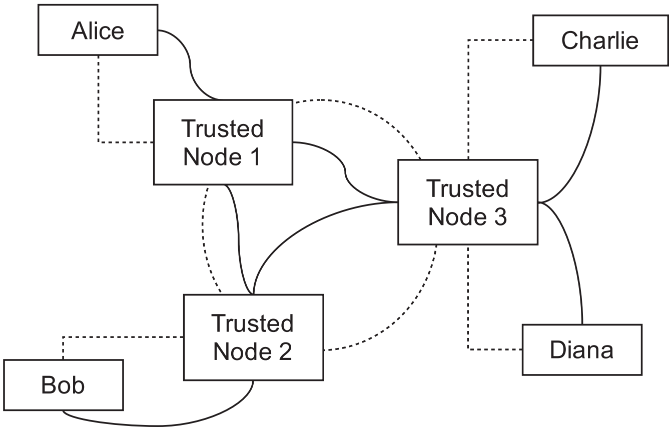

Fig. 3. Scheme of a QKD network link with trusted nodes. Solid lines are quantum channels, dashed lines denote classical channels.

derive a secret key from the key material generated on the communication path [12]. The process of route establishment and key derivation may be aided by additional network layers and so-called *key management services* [67], [68] that perform the key generation independently and hand over the final secret key to the clients.

Trusted-node-based networks overcome the typical distance limitations of current QKD technology, and allow for easy and flexible communication path routing through the network. Assuming sufficiently many trusted nodes, keys can be relayed several times and QKD distance limitations account only for each key relay individually. Furthermore, different types of QKD protocols can be used within one communication path. In addition, a significant amount of work has already been dedicated to developing the necessary routing protocols and application interfaces (e.g., [12], [66], [68]). The main drawback of trusted-node-based hubs is that they do not provide strict end-to-end security. Indeed, the quantum states are destroyed in each hub and confidentiality of the transmitted data is not ensured against the trusted relay nodes. However, the security of trusted-node-based networks can still be guaranteed in the case of some corrupted nodes [69].

3.2 All-Quantum Networks

All-quantum networks are based on quantum hubs and repeaters that allow for the distribution of quantum information between two distant parties, enabling real end-to-end security. Quantum information carriers are routed from Alice to Bob, distributing entanglement to communicating parties. This is achieved by transmission of photons without any distortion or detection, like an optical-electrical-optical conversion in between. Thus, this aim is hard to achieve. The protocol for such a network must be chosen carefully, since it has to be implemented in the whole network and has a decisive impact on the key distribution performance [70]. It should provide the best security against all known attack types and a lack of side-channels. It should also be cost-effective, and scalable.

Already, a number of experiments have been carried out demonstrating the feasibility of all-quantum networks in metropolitan area networks with different topologies and using different QKD protocols:

- *Circle-shaped network [71]:* Hereby, the photons are injected only at one position of the network and all parties share the same quantum channel. That decreases the effective distance between the parties, which makes the setup less interesting for most real world applications.
- *Star-shaped network with PaM [72]:* Hereby, every communicating party is equipped with a quantum state source and a quantum state detector. The distribution of the quantum particles is then achieved by a *Quantum Router*, located in the center of the network and using of one of the standard telecommunication techniques fulfilling no-distortion requirement of quantum states: active optical switches [73] or time-division multiplexing [74]. The establishment of the secure key after the exchange of the qubits is identical to the two-party case. The scalability of the network is bounded by the number of channels the quantum router can handle. The costs of the system are high, since every new recipient has to implement both the source and the detector devices.
- *Star-shaped network with EB [75]:* This approach works similar to a typical two-party entanglement-based QKD protocol, but the number of involved parties is extended to more than two (Fig. 4). The challenging part of this scheme is to design an entangled-pair source, a *quantum hub*, that creates qubits compatible with these techniques and contains the hardware for the routing. Compared to the previously described network design, a benefit is that each recipient needs only a quantum state detector, but no quantum state source. Additionally, since the source is located centrally, the effective distances between the communicating parties are higher. Several experiments have shown the feasibility of entanglement distribution via wavelength-division multiplexing in glass fiber at telecommunication wavelengths [76], [77] and first implementations of such quantum hub sources [78] have been completed. However, the performance of those devices must be increased and remains to be evaluated in larger field tests. Such quantum hub protocols feature the same advantages and drawbacks as typical entanglement-based protocol. They allow for end-to-end secure key exchange, but only for distances up to several tens of kilometers without additional devices such as quantum repeaters. The maximal number of connected recipients is also limited by the method of active or passive routing, limiting this kind of device to metropolitan area networks.

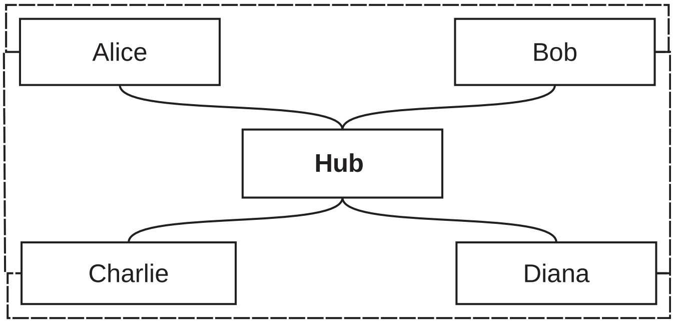

Fig. 4. Scheme of a star-shaped QKD network. Solid lines are quantum channels, dashed lines are classical channels.

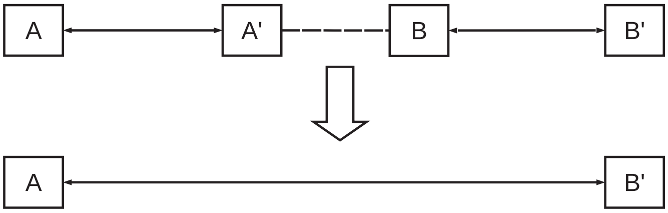

Fig. 5. Schematic structure of a quantum repeater.

Overcoming Distance Limitations. As mentioned above, to overcome the distance limitations, quantum repeaters have been proposed [79] to distribute entangled particles over longer distances. The desired distance is divided into shorter intervals as in Fig. 5. Within every interval, entanglement is shared in a standard way by creating entangled particles $A - A'$ and $B - B'$ and distributing them to the interval ends, where photons A' and B are measured jointly, e.g., by a Bell measurement and some classical information of the measurement is distributed to the remaining pair of particles A and B', such that the entanglement between them becomes established. This procedure is known as *entanglement swapping*. Since the timing is a crucial factor in this process, the photons have to be stored in a *quantum memory*, where the quantum information can be kept for a certain amount of time and retrieved with high fidelity on demand. Required are times from microseconds up to several seconds with the highest possible capacity. Hereby, the timing should be long enough to exchange particles with the closest nodes, perform entanglement swapping, and store and retrieve the qubit from the memory. Moreover, the access to every single particle, stored in the quantum memory, should be provided. How many particles need to be stored simultaneously depends on the type of QKD protocol used and ranges from one to several thousand [35], [80]. Current quantum memory technology allows for storing 665 quantum states of light simultaneously for up to 50 μs and single photons for up to several hours [81]. These numbers and times further need to be improved in order to achieve high throughput QKD networks.

Due to decoherence of quantum states and other quantum noise, quantum repeaters introduce additional noise to the communication channel. Therefore, quantum and classical error correction algorithms are being developed [82] and constitute a vast research area. As already mentioned, there exists an upper bound for key rates as a function of the channel noise for two-party systems. This fundamental limit also applies to all-quantum networks. Those boundaries have been investigated for networks with a chain of quantum repeaters in between [83], [84]. Therefore, the error propagation within the repeater chain was also considered showing the feasibility of such networks.

Combining quantum hubs and quantum repeaters will not only solve the distance limitation problem, but also the problem of supporting only a small number of clients. By swapping entanglement between receivers of different hubs (see Fig. 6) a scalable all-quantum network for arbitrary distances can be established. An integrated setup for a quantum repeater has not yet been finished, although it is supported by different consortia and the EU [85]. An overview of a number of approaches can be found in [86], [87].

Routing. Taking into account that the logical information flow is not parallel to the distribution of the physical particles, the information routing through all-quantum networks is complex. In the example of Fig. 6, entangled particles between Alice and Bob could be distributed using different ways. While the direct way between hubs H1 and H3 needs entanglement swapping only once, the way over hubs H1, H2 and H3 may offer a higher transmission rate, since those hubs may be closer to each other. Therefore, a quantum analogue for the border gateway protocol is required, establishing a connection for the key exchange between Alice and Bob. It has to find the optimal distribution route, and manage the distribution and the timing of all processes in quantum hubs and quantum repeaters in between the end communication parties. Such a protocol has not been developed yet.

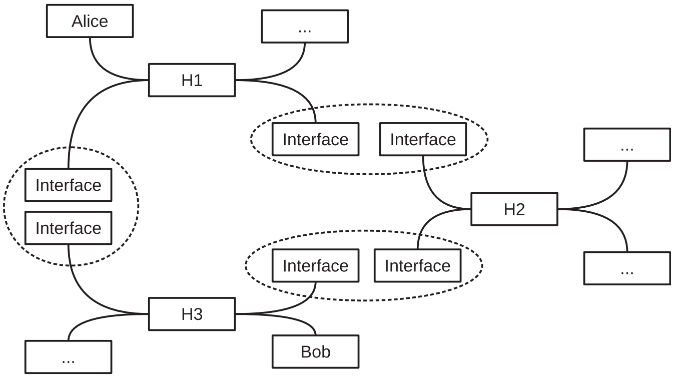

Fig. 6. Schematic structure of an all-quantum network. Circles denote entanglement swapping devices combined with quantum memory within interfaces between different hubs. Classical channels are not shown.

Security. Combining the developed QKD protocols with quantum repeaters requires a complex security analysis of such networks. In that regard, Rass et al. [88] developed a framework for route optimizing in quantum networks which allows for finding the most secure network routes. Moreover, Lee et al. [89] recently showed that there exist Bell inequalities for multi-node networks which allow for enabling device independent security. As in the case of two-party systems, the overall performance and security are considered as well as a system, which security is guaranteed by the non-local correlation of quantum objects, and as classical optimization problem. However, an optimal topology still depends on the potential of quantum repeaters.

4 Conclusions & Outlook

We finally conclude by discussing the current state of trusted-node and all-quantum networks and then deriving open challenges for realizing QKD in large-scale networks.

4.1 Discussion of Current State

A summary of our findings on trusted-node and all-quantum networks can be found in Table 3. In the following, we discuss the comparison criteria in more detail.

Deployment status. In terms of practical deployment, trusted-node-based networks are no longer at a research stage, but on the brink of commercial success. All critical hardware problems are now solved, and the stage of cost optimization and implementation of the key management layers is reached. Hereby, a maximal integration into the classical network systems and establishing an optimal route through the network is desired. For all-quantum networks,

TABLE 3
Summary of Comparison Between Trusted-Nodes Networks and All-Quantum Networks

	Deployment status	Performance	Distance flexibility	Protocol flexibility	Cost-effectiveness	Security
Trusted nodes	+	+	+	+	+	−
All-quantum networks	−	−	−	−	−	+

the required customization of devices makes a fast commercialization improbable in the next ten to twenty years.

Performance. The performance of trusted-node networks is basically determined by the best two-party QKD protocol available. On the other hand, the performance of all-quantum network depends on the performance of additional technology such as quantum memory and quantum repeaters and therefore can be expected to be lower. However, the exact performance loss due to these additional technology has not been quantified yet.

Distance flexibility. A major advantage of the trusted-node approach is that it easily overcomes the inherent distance limitations of QKD technology, albeit at the cost of additional trust assumptions. For all-quantum networks, overcoming the distance limitation remains a major challenge and requires the implementation of quantum routers and quantum memory (Section 3.2). Moreover, recent results suggest that even with quantum repeaters all-quantum networks cannot overcome certain fundamental rate-loss trade-offs.

Protocol flexibility. Regarding flexibility in terms of protocol choice, the trusted-node approach allows for mixing any type of QKD protocol and hardware from any supplier within the same network. On the other hand, all-quantum networks must be designed such that the individual hardware components across the whole network are compatible with each other.

Cost-effectiveness. The question of cost-effectiveness is linked to previously discussed comparison criteria. Since building quantum hubs and repeaters requires tailored setup elements, this results in expensive devices for all-quantum networks. Conversely, the protocol flexibility of trusted-node networks results in cost cuts.

Security. The main disadvantage of trusted-node networks is that confidentiality of the transmitted data is only guaranteed if the relay nodes are fully trusted. This approach may be sufficient if the backbone network is controlled by a single company or a government who is also the main user of the network. On the other hand, the main advantage of all-quantum networks is that they do not require such an assumption. Their security is guaranteed by the laws of quantum physics and the correct implementation of the respective QKD devices.

4.2 Standardization and Deployment

Standardization and deployment are two important factors for transitioning QKD technology from research to practice. In the following we summarize past and ongoing efforts in this regard.

Efforts toward the standardization of QKD components are ongoing [90], [91]. The most intense activity is being carried out by ETSI since 2010, within the QKD Industry Specification Group [92]. In particular, ETSI recently published a white paper on the implementation security of quantum cryptography [93]. Other aspects specified by ETSI include optical component characterization, application interfaces and key delivery APIs. More recently, standardization activity has also started at ITU-T's Study Group 17 [94], with a focus on quantum random number generators in addition to QKD. Furthermore, a Quantum Internet Proposed Research Group has recently been put forward at IETF [95], but only early drafts have been produced so far by the group.

A variety of efforts towards the deployment of QKD systems have been made in the past and are currently ongoing. In the early 2000s, major governmental and research institutions started programs for deploying QKD network prototypes for research purposes [12], [13], [96]. More recently, the feasibility of a QKD-based long-term secure storage system has been demonstrated within the Tokyo QKD Network [97]. In the commercial realm, several companies are developing and selling QKD devices [98], [99], [100]. In particular, several major telecommunication companies have recently started to invest into QKD technology and are now also working on the deployment of QKD system prototypes [101].

4.3 Challenges & Outlook

Long-term secure communication on the Internet is an important goal, and QKD is currently the most promising candidate to achieve it. However, several technical challenges need to be solved in order for realizing QKD in large-scale multi-user networks. In summary, we identify the following open challenges:

- Candidate QKD protocols need to be identified that allow for a secure implementation resistant to known theoretical and practical attacks.
- The data rate of QKD protocols needs to be further improved so that comparable data rates as in classical communication can be achieved.
- Secure connection protocols (e.g., TLS) need to be re-designed to support QKD-based information-theoretically secure key distribution.
- The proposed approaches for realizing quantum hubs need to be implemented and their practicality has to be shown.
- The practicality of quantum repeaters needs to be shown in implementations and it must be shown how they can be combined with quantum hubs. Regarding the quantum memory technology required for quantum repeaters, both the maximal storage capability and the maximal possible storage time must be increased.

- For all-quantum networks, a quantum analogue to the border gateway protocol must be developed to support efficient routing.

Beyond these challenges, additional opportunities are expected. Since all-quantum networks distribute entanglement, i.e., quantum information between any two nodes of it, they can be used beyond key distribution. A European consortium, the Quantum Internet Alliance [102], is planning for 2020 a multi-node all-quantum network connecting quantum computers, increasing their joint computational power.

Acknowledgments

This work has been co-funded by the DFG as part of projects P4, S4, and S6 within the CRC 1119 CROSSING, and through the DFG research fellowship grant GU 1859/1-1.

References

[1] E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446, 2018.

[2] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[3] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.

[4] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, “Post-quantum key exchange—A new hope,” in *Proc. 25th USENIX Conf. Secur. Symp.*, 2016, pp. 327–343.

[5] J. W. Bos, et al., “Frodo: Take off the ring! practical, quantum-secure key exchange from LWE,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 1006–1018.

[6] M. Bellare, T. Kohno, and C. Namprempre, “Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the encode-then-encrypt-and-MAC paradigm,” *ACM Trans. Inf. Syst. Secur.*, vol. 7, no. 2, pp. 206–241, 2004.

[7] C. E. Shannon, “Communication theory of secrecy systems,” *The Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[8] U. M. Maurer, “Conditionally-perfect secrecy and a provably-secure randomized cipher,” *J. Cryptology*, vol. 5, no. 1, pp. 53–66, 1992.

[9] A. D. Wyner, “The wire-tap channel,” *The Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[10] J. Braun, J. Buchmann, C. Mullan, and A. Wiesmaier, “Long term confidentiality: A survey,” *Des. Codes Cryptography*, vol. 71, no. 3, pp. 459–478, 2014.

[11] T. Chapuran, et al., “Optical networking for quantum key distribution and quantum communications,” *New J. Phys.*, vol. 11, no. 10, 2009, Art. no. 105001.

[12] M. Peev, et al., “The SECOQC quantum key distribution network in Vienna,” *New J. Phys.*, vol. 11, no. 7, 2009, Art. no. 075001.

[13] M. Sasaki, et al., “Field test of quantum key distribution in the Tokyo QKD network,” *Opt. Express*, vol. 19, no. 11, pp. 10387–10409, 2011.

[14] D. Bouwmeester, A. Ekert, and A. Zeilinger, *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*. Berlin, Germany: Springer, 2000, vol. 3.

[15] V. Scarani, et al., “The security of practical quantum key distribution,” *Rev. Modern Phys.*, vol. 81, no. 3, 2009, Art. no. 1301.

[16] R. Gallager, “Low-density parity-check codes,” *IRE Trans. Inf. Theory*, vol. 8, no. 1, pp. 21–28, 1962.

[17] G. Brassard and L. Salvail, “Secret-key reconciliation by public discussion,” in *Proc. Workshop Theory Appl. Cryptographic Techn.*, 1993, vol. 765, pp. 410–423.

[18] P. Jouguet and S. Kunz-Jacques, “High performance error correction for quantum key distribution using polar codes,” *Quantum Inf. Comput.*, vol. 14, no. 3/4, pp. 329–338, 2014.

[19] S. A. Goorden, et al., “Quantum-secure authentication with a classical key,” *Optica*, vol. 1, no. 6, pp. 421–424, 2013.

[20] G. M. Nikolopoulos and E. Diamanti, “Continuous-variable quantum authentication of physical unclonable keys,” *Sci. Rep.*, vol. 7, 2017, Art. no. 46047.

[21] A. Boaron, et al., “Secure quantum key distribution over 421 km of optical fiber,” *Phys. Rev. Lett.*, vol. 121, 2018, Art. no. 190502.

[22] H. L. Yin, et al., “Measurement-device-independent quantum key distribution over a 404 km optical fiber,” *Phys. Rev. Lett.*, vol. 117, 2016, Art. no. 190501.

[23] B. Korzh, et al., “Provably secure and practical quantum key distribution over 307 km of optical fibre,” *Nature Photonics*, vol. 9, no. 3, pp. 163–168, 2015.

[24] S. Wang, et al., “2 GHz clock quantum key distribution over 260 km of standard telecom fiber,” *Opt. Lett.*, vol. 37, no. 6, pp. 1008–1010, 2012.

[25] D. Stucki, et al., “High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres,” *New J. Phys.*, vol. 11, no. 7, 2009, Art. no. 075003.

[26] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, “Simple and high-speed polarization-based QKD,” *Appl. Phys. Lett.*, vol. 112, no. 5, 2018, Art. no. 051108.

[27] D. Huang, P. Huang, D. Lin, and G. Zeng, “Long-distance continuous-variable quantum key distribution by controlling excess noise,” *Sci. Rep.*, vol. 6, 2016, Art. no. 19201.

[28] T. Honjo, et al., “Long-distance entanglement-based quantum key distribution over optical fiber,” *Opt. Express*, vol. 16, no. 23, pp. 19118–19126, 2008.

[29] P. Jouguet, et al., “Experimental demonstration of long-distance continuous-variable quantum key distribution,” *Nature Photonics*, vol. 7, no. 5, pp. 378–381, 2013.

[30] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proc. Int. Conf. Circuits Syst. Signal Process.*, 1984. vol. 175, pp. 175–179.

[31] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations,” *Phys. Rev. Lett.*, vol. 92, 2002, Art. no. 057901.

[32] D. Stucki, et al., “Fast and simple one-way quantum key distribution,” *Appl. Phys. Lett.*, vol. 87, no. 19, 2005, Art. no. 194108.

[33] J. S. Bell, “On the Einstein Podolsky Rosen paradox,” *Phys.*, vol. 1, no. 3, pp. 195–200, 1964.

[34] V. Scarani and N. Gisin, “Quantum communication between N partners and Bell’s inequalities,” *Phys. Rev. Lett.*, vol. 87, no. 11, 2001, Art. no. 117901.

[35] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Phys. Rev. Lett.*, vol. 67, no. 6, 1991, Art. no. 661.

[36] C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without Bell’s theorem,” *Phys. Rev. Lett.*, vol. 68, no. 5, pp. 557–559, 1992.

[37] E. Diamanti and A. Leverrier, “Distributing secret keys with quantum continuous variables: Principle, security and implementations,” *Entropy*, vol. 17, no. 9, pp. 6072–6092, 2015.

[38] F. Grosshans and P. Grangier, “Continuous variable quantum cryptography using coherent states,” *Phys. Rev. Lett.*, vol. 88, no. 5, 2002, Art. no. 057902.

[39] T. C. Ralph, “Continuous variable quantum cryptography,” *Phys. Rev. A*, vol. 61, no. 1, 1999, Art. no. 010303.

[40] K. Inoue, E. Waks, and Y. Yamamoto, “Differential-phase-shift quantum key distribution using coherent light,” *Phys. Rev. A*, vol. 68, no. 2, 2003, Art. no. 022317.

[41] D. Bacco, et al., “Two-dimensional distributed-phase-reference protocol for quantum key distribution,” *Sci. Rep.*, vol. 6, 2016, Art. no. 36756.

[42] M. Takeoka, S. Guha, and M. M. Wilde, “Fundamental rate-loss tradeoff for optical quantum key distribution,” *Nature Commun.*, vol. 5, 2014, Art. no. 5235.

[43] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, “Fundamental limits of repeaterless quantum communications,” *Nature Commun.*, vol. 8, 2017, Art. no. 15043.

[44] S. K. Liao, et al., “Satellite-to-ground quantum key distribution,” *Nature*, vol. 549, no. 7670, 2017, Art. no. 43.

[45] S. K. Liao, et al., “Satellite-relayed intercontinental quantum network,” *Phys. Rev. Lett.*, vol. 120, 2018, Art. no. 030501.

[46] K. Günthner, et al., “Quantum-limited measurements of optical signals from a geostationary satellite,” *Optica*, vol. 4, no. 6, pp. 611–616, 2017.

[47] F. Laudenbach, et al., “Continuous-variable quantum key distribution with Gaussian modulation—The theory of practical implementations,” *arXiv preprint quant-ph/ 1703.09278*, 2017.

[48] Y. Mao, et al., “Integrating quantum key distribution with classical communications in backbone fiber network,” *Opt. Express*, vol. 26, no. 5, pp. 6010–6020, 2018.

[49] I. Choi, et al., “Field trial of a quantum secured 10Gb/s DWDM transmission system over a single installed fiber,” *Opt. Express*, vol. 22, no. 19, pp. 23121–23128, 2014.

[50] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, pp. 145–195, 2002.

[51] R. Renner, N. Gisin, and B. Kraus, “Information-theoretic security proof for quantum-key-distribution protocols,” *Phys. Rev. A*, vol. 72, no. 1, 2005, Art. no. 012332.

[52] H. K. Lo and H. F. Chau, “Unconditional security of quantum key distribution over arbitrarily long distances,” *Sci.*, vol. 283, no. 5410, pp. 2050–2056, 1999.

[53] P. W. Shor and J. Preskill, “Simple proof of security of the BB84 quantum key distribution protocol,” *Phys. Rev. Lett.*, vol. 85, no. 2, 2000, Art. no. 441.

[54] I. Kogias, Y. Xiang, Q. He, and G. Adesso, “Unconditional security of entanglement-based continuous-variable quantum secret sharing,” *Phys. Rev. A*, vol. 95, no. 1, 2017, Art. no. 012315.

[55] T. Moroder, et al., “Security of distributed-phase-reference quantum key distribution,” *Phys. Rev. Lett.*, vol. 109, 2012, Art. no. 260501.

[56] H. K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” *Phys. Rev. Lett.*, vol. 94, no. 23, 2005, Art. no. 230504.

[57] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, “Trojan-horse attacks on quantum-key-distribution systems,” *Phys. Rev. A*, vol. 73, no. 2, 2006, Art. no. 022320.

[58] L. Lydersen, et al., “Hacking commercial quantum cryptography systems by tailored bright illumination,” *Nature Photonics*, vol. 4, no. 10, pp. 686–689, 2010.

[59] D. Mayers and A. Yao, “Quantum cryptography with imperfect apparatus,” in *Proc. 39th Annu. Symp. Found. Comput. Sci.*, 1998, pp. 503–509.

[60] U. Vazirani and T. Vidick, “Fully device-independent quantum key distribution,” *Phys. Rev. Lett.*, vol. 113, no. 14, 2014, Art. no. 140501.

[61] H. K. Lo, M. Curty, and B. Qi, “Measurement-device-independent quantum key distribution,” *Phys. Rev. Lett.*, vol. 108, no. 13, 2012, Art. no. 130503.

[62] Y. L. Tang, et al., “Measurement-device-independent quantum key distribution over 200 km,” *Phys. Rev. Lett.*, vol. 113, 2014, Art. no. 190501.

[63] Y. Rekhter, T. Li, and S. Hares, “A border gateway protocol 4 (BGP-4),” RFC 4271, 2006.

[64] State Council of the People’s Republic of China: China opens 2,000-km quantum communication line, 2017. [Online]. Available: http://english.gov.cn/news/photos/2017/09/30/content_281475894651400.htm, Accessed on: Mar. 14, 2019

[65] Photonics Media: Quantum Networks: Photons Hold Key to Data Security, 2017. [Online]. Available: https://www.photonics.com/Articles/Quantum_Networks_Photons_Hold_Key_to_Data/a60541, Accessed on: Mar. 14, 2019

[66] Y. Tanizawa, R. Takahashi, and A. R. Dixon, “A routing method designed for a quantum key distribution network,” in *Proc. 8th Int. Conf. Ubiquitous Future Netw.*, 2016, pp. 208–214.

[67] M. Mehic, et al., “A novel approach to quality of service provisioning in trusted relay quantum key distribution networks,” *arXiv: 1810.03857*, 2018.

[68] P. K. Tysowski, X. Ling, N. Lütkenhaus, and M. Mosca, “The engineering of a scalable multi-site communications system utilizing quantum key distribution (QKD),” *Quantum Sci. Technol.*, vol. 3, no. 2, 2018, Art. no. 024001.

[69] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger, “Security of trusted repeater quantum key distribution networks,” *J. Comput. Secur.*, vol. 18, no. 1, pp. ‘61–87, 2010.

[70] C. Jones, D. Kim, M. T. Rakher, P. G. Kwiat, and T. D. Ladd, “Design and analysis of communication protocols for quantum repeater networks,” *New J. Phys.*, vol. 18, no. 8, 2016, Art. no. 083015.

[71] T. Nishioka, H. Ishizuka, T. Hasegawa, and J. Abe, “‘Circular type’ quantum key distribution,” *IEEE Photonics Technol. Lett.*, vol. 14, no. 4, pp. 576–578, Apr. 2002.

[72] W. Chen, et al., “Field experiment on a “star type” metropolitan quantum key distribution network,” *IEEE Photonics Technol. Lett.*, vol. 21, no. 9, pp. 575–577, May 2009.

[73] T. Y. Chen, et al., “Metropolitan all-pass and inter-city quantum communication network,” *Opt. Express*, vol. 18, no. 26, pp. 27217–27225, 2010.

[74] X. Y. Chang, et al., “Experimental realization of an entanglement access network and secure multi-party computation,” *Sci. Rep.*, vol. 6, 2016, Art. no. 29453.

[75] I. Herbauts, et al., “Demonstration of active routing of entanglement in a multi-user network,” *Opt. Express*, vol. 21, no. 23, pp. 29013–29024, 2013.

[76] J. Ghalbouni, I. Agha, R. Frey, E. Diamanti, and I. Zaquine, “Experimental wavelength-division-multiplexed photon-pair distribution,” *Opt. Lett.*, vol. 38, no. 1, pp. 34–36, 2013.

[77] D. Y. Cao, et al., “Multiuser-to-multiuser entanglement distribution based on 1550 nm polarization-entangled photons,” *Sci. Bulletin*, vol. 60, no. 12, pp. 1128–1132, 2015.

[78] W. T. Fang, et al., “On-chip generation of time-and wavelength-division multiplexed multiple time-bin entanglement,” *Opt. Express*, vol. 26, no. 10, pp. 12912–12921, 2018.

[79] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, “Quantum repeaters: The role of imperfect local operations in quantum communication,” *Phys. Rev. Lett.*, vol. 81, no. 26, 1998, Art. no. 5932.

[80] F. Furrer and W. J. Munro, “Repeaters for continuous-variable quantum communication,” *Phys. Rev. A*, vol. 98, 2018, Art. no. 032335.

[81] M. Parniak, M. Dąbrowski, M. Mazelanik, A. Leszczyński, M. Lipka, and W. Wasilewski, “Wavevector multiplexed atomic quantum memory via spatially-resolved single-photon detection,” *Nature Commun.*, vol. 8, no. 1, 2017, Art. no. 2140.

[82] B. M. Terhal, “Quantum error correction for quantum memories,” *Rev. Mod. Phys.*, vol. 87, pp. 307–346, 2015.

[83] K. Azuma, A. Mizutani, and H. K. Lo, “Fundamental rate-loss trade-off for the quantum Internet,” *Nature Commun.*, vol. 7, 2016, Art. no. 13523.

[84] S. Guha, et al., “Rate-loss analysis of an efficient quantum repeater architecture,” *Phys. Rev. A*, vol. 92, 2015, Art. no. 022357.

[85] Quantum Coordination and Support Action (QSA): Quantum Flagship, 2018. [Online]. Available: https://qt.eu, Accessed on: Mar. 14, 2019

[86] T. E. Northup and R. Blatt, “Quantum information transfer using photons,” *Nature Photonics*, vol. 8, no. 5, pp. 356–363, 2014.

[87] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, “Inside quantum repeaters,” *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, pp. 78–90, May/Jun. 2015.

[88] S. Rass and P. Schartner, “Security in quantum networks as an optimization problem,” in *Proc. Int. Conf. Availability Rel. Secur.*, 2009, pp. 493–498.

[89] C. M. Lee and M. J. Hoban, “Towards device-independent information processing on general quantum networks,” *Phys. Rev. Lett.*, vol. 120, 2018, Art. no. 020504.

[90] T. Länger and G. Lenhart, “Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD,” *New J. Phys.*, vol. 11, no. 5, 2009, Art. no. 055051.

[91] R. Alléaume, et al., “Worldwide standardization activity for quantum key distribution,” in *Proc. IEEE Globecom Workshops*, 2014, pp. 656–661.

[92] European Telecommunications Standards Institute (ETSI): Industry Specification Group (ISG) on Quantum Key Distribution for Users (QKD), 2019. [Online]. Available: https://www.etsi.org/committee/qkd, Accessed on: Mar. 14, 2019.

[93] European Telecommunications Standards Institute (ETSI): White Paper 27: Implementation Security of Quantum Cryptography, 2018. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf, Accessed on: Mar. 14, 2019.

[94] ID Quantique: Quantum Alliance Initiative and ID Quantique aim for QRNG and QKD standardisation, 2019. [Online]. Available: https://www.idquantique.com/quantum-alliance-initiative-and-id-quantique-aim-for-qrng-and-qkd-standardisation/, Accessed on: Mar. 14, 2019.

[95] IETF: Quantum Internet Proposed Research Group (QIRG), 2019. [Online]. Available: https://datatracker.ietf.org/rg/qirg/about/, Accessed on: Mar. 14, 2019.

[96] C. Elliott, “Building the quantum network,” *New J. Phys.*, vol. 4, no. 46, pp. 1–12, 2002.

[97] J. Braun, J. Buchmann, D. Demirel, M. Geihs, M. Fujiwara, S. Moriai, M. Sasaki, and A. Waseda, “LINCOS: A storage system providing long-term integrity, authenticity, and confidentiality,” in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, 2017, pp. 461–468.

[98] [Online]. Available: https://www.idquantique.com, Accessed on: Mar. 15, 2019.

[99] [Online]. Available: https://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information/Quantum-Key-Distribution/Toshiba-QKD-system/, Accessed on: Mar. 20, 2019.

[100] [Online]. Available: http://www.quantum-info.com/English/, Accessed on: Mar. 20, 2019.

[101] [Online]. Available: https://www.telekom.com/en/media/media-information/archive/quantum-alliance-486280, Accessed on: Mar. 15, 2019.

[102] Quantum Internet Alliance: Quantum Internet Alliance, 2017. [Online]. Available: http://quantum-internet.team/, Accessed on: Mar. 14, 2019.

Matthias Geihs is a post-doctoral researcher with the group of Prof. Dr. Johannes Buchmann at TU Darmstadt, Germany. His research focuses on the design and analysis of long-term secure cryptographic systems, with a particular interest in long-term secure archiving systems.

Oleg Nikiforov is working toward the PhD degree in the group Laser- and Quantum Optics of Prof. Thomas Walther, TU Darmstadt. His main research interests are quantum cryptography, with a focus on development of multi-party quantum key distribution systems.

Denise Demirel received the diploma degree in computer science from TU Darmstadt, in 2010. She worked as a doctoral researcher from 2010 to 2013, on constitutional compliant electronic voting. In December 2013, she received the doctorate degree from TU Darmstadt. Her thesis focused on cryptographic aspects, verifiability, and (everlasting) privacy of electronic voting schemes. Since December 2013, she has worked as a postdoctoral researcher with the field of everlasting confidentiality, long-term integrity and authenticity, verifiable computing, cloud computing, and long-term secure archiving.

Alexander Sauer is working toward the PhD degree in physics at TU Darmstadt and member of Prof. Gernot Alber's theoretical quantum physics group. His research interests are Bell nonlocality and its use in quantum cryptography, with a particular focus on the effects of imperfect devices on Bell tests.

Denis Butin is a researcher with the Cryptography and Computer Algebra Group, TU Darmstadt. His current research area is long-term security. Earlier, he investigated practical aspects of hash-based signatures. He also worked on accountability for design and security policy languages at Inria, France, and on the analysis of security protocols using formal methods at DCU, Ireland.

Felix Günther is a postdoctoral researcher with the Security and Cryptography Group, UC San Diego. His research interests are applied cryptography and computer security, with a particular focus on provable security, key exchange, and secure channel protocols. His work aims at narrowing the gap between theoretical understanding and practical security of real-world cryptographic systems.

Gernot Alber received the PhD degree in physics from the University of Innsbruck, Austria, in 1985. From 1983 to 1985, he was a research associate with the Joint Institute for Laboratory Astrophysics in Boulder, working with John Cooper. Subsequently, he returned to the University of Innsbruck to work as a postdoctoral research fellow with the research group of Peter Zoller. In 1987, he was awarded an Alexander von Humboldt research fellowship with which he moved to the University of Freiburg in Breisgau. In 1991 and 1994, he received habilitations in theoretical physics. He joined the research group of Wolfgang Schleich at the University of Ulm in 1997. In 2002, he moved to TU Darmstadt, Germany, as a full professor for theoretical physics. In 2007, he received the gold medal of the Czech Technical University. Currently, he is member of the editorial board of *Physical Review A*.

Thomas Walther received the PhD degree at the University of Zurich. He is a full professor of physics at TU Darmstadt. His field of research is laser development, atom trapping, exploitation of coherent effects, quantum cryptography as well as applications of lasers in spectroscopy and remote sensing.

Johannes Buchmann received the PhD degree from the Universität zu Köln, Germany, in 1982. From 1985 to 1986, he was a postdoc at the Ohio State University on a fellowship of the Alexander von Humboldt Foundation. From 1988 to 1996, he was a professor of computer science at the Universität des Saarlandes in Saarbrücken. Since 1996, he has been a professor of computer science and mathematics at TU Darmstadt. From 2001 to 2007, he was vice president of research at TU Darmstadt. In 1993, he received the Leibniz-Prize of the German Science Foundation (DFG) and in 2017 the Konrad Zuse Medal of the German Informatics Society (GI). He is a member of the German Academy of Science and Engineering Acatech and of the German Academy of Science Leopoldina.