Towards Global Quantum Key Distribution

Haoran Zhang[1,2*], Haotao Zhu[1,2*], Ruihua He[2], Yan Zhang[2], Chao Ding[2], Lajos Hanzo[3†] and Weibo Gao[1,2,4,5†]

[1]School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, Singapore

[2]Division of Physics and Applied Physics, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore, Singapore

[3]School of Electronics and Computer Science, University of Southampton, Southampton, U.K.

[4]Centre for Quantum Technologies, Nanyang Technological University, Singapore, Singapore

[5]Quantum Science and Engineering Centre (QSec), College of Engineering, Nanyang Technological University, Singapore, Singapore

[*]These authors contributed equally: Haoran Zhang, Haotao Zhu

[†]Email: hanzo@soton.ac.uk, wbgao@ntu.edu.sg

The final formatted version of this paper can be found at:

https://www.nature.com/articles/s44287-025-00238-7?utm_source=rct_congratemailt&utm_medium=email&utm_campaign=nonoa_20251112&utm_content=10.1038/s44287-025-00238-7

[H1] **ABSTRACT**

Quantum Key Distribution (QKD) is a cryptographic technology that supports the negotiation and sharing of private keys with unconditional security between authorized parties. As QKD scales to a global level, it must address performance limitations, high costs, and practical security concerns. In this Review, we outline the key technical challenges, applications, and prospective developments toward a global QKD network. Advances such as satellite-based QKD and newly developed protocols offer promising solutions for extending QKD over long distances. Field trials have progressively expanded from inter-city links to larger-scale networks. Nevertheless, balancing cost–performance and security considerations will continue to challenge advanced research efforts. Based on the strategies addressing these obstacles, we highlight future directions that can support the efficient realization of global QKD infrastructures.

[H1] **Introduction**

In an information-driven society, concerns about information security are paramount, where

authorized users face potential adversaries. This ongoing conflict, driven by complementary concerns about protecting information versus the desire to intercept it, can be quantified by comparing the computational resources and information access capabilities of both authorized users and adversaries. Encryption remains the most common method for secure communication; however, the security of most cryptographic schemes relies on the limited computational power of adversaries, thus providing computational security rather than information-theoretical security. Quantum communication imposes natural limitations on an adversary's ability to access information by engaging quantum mechanical properties[1]. In quantum cryptography, quantum key distribution (QKD)[2] garners interest due to the intuitive role of securely shared keys in encryption. QKD enables the negotiation and sharing of private keys between distant users at information-theoretical security and is composable[3] with other cryptographic schemes. Thus, QKD provides a versatile option for encryption in communication schemes that require a pre-shared private key.

Classical networks, such as undersea fiber-optic cables, terrestrial fiber-optic networks, and satellite-based systems, are already in use worldwide, enabling seamless communication between users. Therefore, a global QKD network is in demand to protect the overall security of classical networks. Although not all communications may require quantum-secure encryption, it is crucial to ensure that the backbone of the network is covered. However, QKD faces questions regarding its practical value and reliability. The primary challenge comes from post-quantum cryptography (PQC)[4], which claims to be secure against existing quantum algorithms. While QKD maintains its unique advantage by offering information-theoretical security, PQC can still alleviate public concerns about the threat posed by quantum computers[5] to information security. Another concern is QKD's inherent vulnerability to denial-of-service (DoS) attacks. Unlike classical DoS attacks, those targeting QKD networks occur at the physical layer, which is easier to monitor[6]. However, these concerns have already negatively impacted on the reputation of QKD's reliability. Thus, the QKD community must reassure the public[7] before global adoption.

As QKD technology advances, its various components reach maturity at vastly different rates. For example, some aspects such as Bannett-Brassard 1984 (BB84)-like protocols[2] have moved beyond the scientific research and are being explored for commercial applications. In contrast, the envisioned backbone for all QKD applications, the quantum memory network[8], remains in its early stages. Consequently, predicting the optimal design of a QKD network is premature[9,10]. Nevertheless, it is possible to examine QKD research and anticipate future developments with greater clarity.

In this Review, we introduce the fundamentals of QKD implementation and discuss the main challenges confronting its applications. We further explore several approaches for achieving long-distance QKD and discuss the advantages and drawbacks of these methods through their applications. Chiefly, efforts aiming to extend the range of QKD are foundational for building a global quantum communication network. Finally, we outline the developments of both terrestrial and satellite-based QKD networks. We serve as both an introduction and an inspiration for fostering collaboration among

academia, government, and industry to build a global QKD network.

[H1] Realizing QKD Networks

The implementation of QKD first requires a protocol designed for the preparation, transmission, and measurement of quantum states, followed by post-processing to negotiate the key. Compared to classical communication, these procedures demand additional quantum devices and channels to handle QKD protocols.

[H2] QKD Protocols

QKD protocols are primarily categorized into two types: discrete-variable (DV) and continuous-variable (CV) protocols (Fig. 1). In DV-QKD, information is mapped, for example, onto single photons or weak coherent pulses[2] in a discrete manner. These photons are subsequently detected using single-photon detectors[11]. DV-QKD protocols utilize quantum systems that are described by finite-dimensional Hilbert spaces, including states of polarization[2], phase[11], or orbital angular momentum (OAM)[12]. Therefore, protocols such as differential-phase-shift[13], coherent-one-way[14] and Round-Robin differential-phase-shift[15] are also recognized as DV protocols. These distributed-phase-reference protocols are sometimes listed separately due to the unique challenges they present in security analysis[16,17].

Conversely, CV-QKD encodes information onto the field quadrature amplitudes of quantized electromagnetic fields, which are detected using homodyne[18] or heterodyne[19] detectors. The primary CV-QKD protocols employ coherent[20] or squeezed[21] Gaussian states encoded with Gaussian or discrete keys within infinite-dimensional Hilbert spaces. Additionally, protocols that utilize thermal states[22], discrete modulation[23] or unidimensional preparation[24] are also classified as CV protocols.
Though the goal of both DV and CV protocols is the distribution of secret keys, differences in modulation and measurement affect the device requirements and performance in specific scenarios. Gaining an understanding of the various protocols provides a comprehensive perspective for implementing QKD networks.

[H2] Quantum Devices for QKD

The implementation of QKD necessitates the use of specialized quantum devices, primarily consisting of a light source, modulators, and detectors. Many of these devices are similar to those used in classical optical communications (Fig. 1). For the light source, a single photon source is ideal for many DV-QKD protocols. Weak coherent pulses associated with the decoy state method[25,26] are more commonly employed as light source to simulate single photon sources due to their robustness and efficiency. For CV-QKD, homodyne or heterodyne detectors, where the signal interferes with a local oscillator, are required. For DV-QKD, the most indispensable devices are single photon detectors, such as single-photon avalanche diodes (SPADs)[27] and superconducting nanowire single-photon detectors (SNSPDs)[28]. Single photon detectors can precisely provide both the presence and timing of a single photon arriving at the detectors. Assisted by the optical design at the receiver, these detectors

effectively perform the positive operator valued measurements[29].

For near-infrared SPADs, the avalanche photodiode typically uses an indium gallium arsenide (InGaAs) layer for absorption and either an indium phosphide (InP) or indium aluminum arsenide (InAlAs) layer for multiplication[30]. SPADs work in Geiger-mode[31], where the absorption of a single photon can initiate the impact-ionization process. Therefore, the emerged macroscopic, self-sustaining avalanche current is detectable[31]. However, the electrical avalanche amplification structure is highly sensitive to environmental noise, and even noise from the avalanche process itself, resulting in a higher dark count rate and an increased probability of afterpulsing[32]. Thus, a quenching circuit is essential to suppress the avalanche and reset the SPAD to its initial bias condition. This process introduces additional dead time as a trade-off. Optimizing the design of the avalanche photodiode structure, such as increasing the multiplication region thickness[33], can reduce the dark count rate but further compromises photon detection efficiency (PDE).

The performance of SNSPD surpasses that of SPAD across most metrics. SNSPDs have a shorter reset time for returning to the superconducting state after detection and demonstrate superior PDE and dark count rate performance, particularly in the near-infrared spectrum. For example, the typical PDE of InGaAs SPAD is around 30%, whereas SNSPD can achieve a maximum PDE of up to 99.5% ref. [34]. Similarly, while an SPAD typically exhibits a dark count rate around several tens of thousands of Hertz, SNSPDs can reduce this to as low as 0.1 Hertz[35].

The operation of SNSPD is based on a mechanism where a supercurrent assists in the formation of non-superconducting regions, enhancing the PDE, time precision, and noise robustness. Typically, the nanowire is made of materials such as niobium nitride (NbN)[36], niobium titanium nitride (NbTiN)[34], tungsten silicide (WSi)[37], or molybdenum silicide (MoSi)[35], and is cooled to well below its superconducting transition temperature and biased with a constant current near its critical value. In this superconducting state, Cooper pairs—charge carriers formed through electron-phonon interactions—are stable under Bose-Einstein condensation[38]. Upon photon absorption, if the photon's energy surpasses the binding energy of a Cooper pair, it breaks into two quasiparticles. For example, a 1550 nm photon can break 125 Cooper pairs in a NbN superconductor[38]. The generation of hundreds of quasi-particles forms a non-superconducting 'hotspot.' Subsequently, increased current density and vortex-assisted mechanisms[39] cause the hotspot to expand, eventually encompassing the entire cross-section of the nanowire. This expansion leads to an instantaneous increase in resistance, which is then detected.

[H2] Quantum channel

Besides authenticated classical channels, quantum channels are required for sharing quantum resources between authorized users in the general settings of QKD protocols. Quantum channels establish a physical connection between QKD users, allowing quantum states to be transmitted at the lowest possible environmental perturbation. Optical fibers and free space links are the most commonly used quantum channels (Fig. 1). Single-mode fibers are the preferred choice, as telecommunications networks are already extensively built on single-mode fibers operating at telecommunication

wavelengths. Because single photons cannot be amplified like classical signals, the low-loss and stable transmission characteristics of telecom-band single-mode fibers make them ideal for quantum state transmission. Although issues such as birefringence, scattering[40], group-velocity dispersion, and polarization mode dispersion[41] still exist, even in underground dark fibers[42], their effects can be substantially mitigated by noise-reducing strategies[29]. As a result, a QKD field test over 500 km has been successfully achieved[43]. The establishment of a free-space quantum channel offers greater flexibility than fiber optics, especially when navigating challenging terrains or setting up temporary links. Additionally, free-space channels can cover much longer distances than fiber channels as the attenuation in free space is less than in fiber. For instance, the satellite-to-ground channel attenuation varied from 29 dB at 530 km to 44 dB at 1600 km in Micius experiment[44]. However, additional noise factors such as stray light and turbulence need to be addressed. Stray light can cause serious background noise, while turbulence can lead to space-time redistribution as well as beam spreading and wandering, causing a higher error rate of quantum states. Consequently, the use of spectral, spatial, and temporal filters, along with careful selection of operating times, spaces, wavelengths, and quantum basis, are essential considerations to avoid or compensate for noise[45,46]. For an unmanned aerial vehicle[47] or satellite QKD[48], developing a fast optical tracking system is also crucial for maintaining a stable and low-loss quantum channel[49]. Additionally, the quantum channel for terahertz QKD can be readily established using wireless technologies, albeit with a limited communication range of approximately a hundred meters[50]. In summary, optical fibers and free-space links remain the primary choices for QKD quantum channels, each suited to different deployment scenarios and, consequently, facing distinct practical challenges.

[H1] Practical challenges of QKD

Application challenges arise from the gap between practical performance and expected demands, as well as the substantial trade-offs required to gain the benefits. The performance of QKD is prized for its key rate and practical security, but additional costs stem from the specialized requirements of quantum devices and channels.

[H2] Key rate

QKD supports key agreements for encryption. Once the key has been negotiated, the system then operates as classical encryption, ensuring compatibility with conventional devices. Explicitly, information-theoretical security can be achieved using a one-time pad, where the key must be as long as the data sequence. However, the key generation rate of practical QKD systems is inherently limited by the response rate, presenting challenges for encrypting large volumes of classical data transmission. Therefore, understanding and overcoming the constraints on QKD capacity are paramount.

[H3] Channel attenuation

Channel loss occurs when the photons flying in the quantum channel have a probability of disappearing, rendering them undetectable. This phenomenon can be described as the quantum states

splitting into the environment. Despite the efforts of manufacturers to purify the glass-core fiber to minimize absorption, intrinsic inhomogeneities still cause Rayleigh scattering, leading to optical attenuation throughout the fiber. In particular, the low-loss fiber used in QKD experiments typically achieves attenuation as low as 0.16 dB km^{-1} ref. [51,52], which is slightly lower than the standard telecommunication fiber attenuation of 0.2 dB km^{-1}. In the absence of a quantum repeater, the probability of photon detection will decay with the accumulation of channel loss[53], limiting the operational distance of QKD networks.

For point-to-point QKD over a pure-loss channel with a transmittance of η, the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound[54] provides a tight limit on the secret key capacity. This bound demonstrates that the secret key rate per channel use is constrained to $-log_2(1-\eta)$, approximating a near linear scale of 1.44η at low transmittance (Fig. 2a). Hence, it is sometimes referred to as the linear bound. This bound is achievable in CV-QKD with the use of quantum memory. In practical scenarios operating without quantum memory, the secret key capacity of CV-QKD is reduced to 0.72η, which is lower than that typically achieved by DV-QKD. Specifically, the secret capacity of both BB84-like QKD with decoy states[25] and differential-phase-shift QKD with block-wise phase randomization[55] is proportional to η at low transmittance. Moreover, the reduced tolerance for channel loss in CV-QKD, combined with challenges in the post-processing procedure, leads to the more frequent application of DV-QKD in metropolitan QKD networks.

Consequently, developing new protocols[56] that can mitigate the limitations of secret key capacity imposed by channel loss, and constructing quantum channels with lower attenuation —such as free-space links and hollow-core fibers[57] —are critical for establishing a global QKD network.

[H3] QKD signaling rate

When the secret key capacity per channel use is fixed, the key rate of a QKD system is typically proportional to the relative frequency of channel uses. However, this repetition rate is limited by the speed of optical and electrical modulation and demodulation. Specifically, device bandwidth limitations can affect the accuracy of state preparation and measurement, while time jitter from the source, SNSPD, and time tagger can lead to crosstalk between adjacent signals, all contributing to an increase in quantum bit error rate. Implementations of differential-phase-shift QKD have reached speeds up to 10 GHz in 2007 ref. [58], as the issue of crosstalk is less severe in this context. Nonetheless, protocols like coherent-one-way QKD[14] have encountered challenges regarding security vulnerabilities under general attacks[59]. Owing to the deterministic phase relation of all pulses, the secret key capacity of coherent-one-way QKD has been proven to scale as $O(\eta^2)$ [16,60], indicating that such schemes are not suitable for long-distance deployments. For one-way BB84-like protocols, QKD systems have achieved repetition rates of up to 5 GHz for polarization encoding[61] and 2.5 GHz for time-bin and phase encoding[62].

To further increase the repetition rate, it would be crucial to enhance device performance[63], design ultrafast optical modulation schemes[64], or develop passive protocols[65]. However, the key rate increases only linearly with the repetition rate, which has already approached a bottleneck at the gigahertz level.

Moreover, further increasing the repetition rate introduces additional side-channel loopholes, such as correlations between pulses[66]. Consequently, increasing the repetition rate is not a promising focus for the QKD community.

[H3] Detector Saturation

Assuming low-loss channels and high repetition rates, the saturation of single-photon detectors in DV-QKD could still limit the key rate of the system[67]. This saturation arises due to the dead time, during which SPADs or SNSPDs become temporarily insensitive to incoming photons as they reset to their initial state for subsequent detection. To address this, multi-pixel SNSPDs have been developed[68] to maximize the key rate (Fig. 2b). When one pixel detects a photon and begins resetting, the remaining pixels are still active and ready to detect additional photons. The multi-pixel design not only shortens the dead time by reducing the length of each pixel, but also reduces time jitter[69]. This enhancement improves the saturation count rate of SNSPDs and subsequently increases the overall key rate to 110 Mbps[70],approaching the throughput achievable in 4G networks.

[H2] Cost

When deploying a large-scale QKD network, it is crucial to strike a compelling balance between benefits and costs. Like many new technologies, the implementation of QKD networks remains expensive, often costing hundreds of times more than deploying classical networks of a similar scale.

[H3] Channel Occupation

Establishing stable quantum links is fundamental for constructing QKD networks. However, extensive resources and close cooperation with governmental bodies are required. For instance, satellite links and other aerial vehicles are necessary, and even the ground stations are ideally situated on tall buildings or on plateau regions. For instance, a metropolitan entanglement-based free-space network[71] can be established using a tall building as the central node. Fortunately, the presence of dense classical networks provides potential fiber link resources for QKD network deployment, making it a cost-efficient option to share fibers with classical communication. However, the coexistence of quantum signals with classical optical communications demands effective isolation of the quantum channel from noise[72]. Using a dedicated frequency band[49], along with high-isolation wavelength division multiplexing[73] devices or optical filters[74], can help mitigate environmental disturbances. Even so, in-band noise caused primarily by Raman scattering[75] from high-power classical signals[76] must also be addressed[77] to ensure the efficient use of bandwidth resources.

However, certain devices commonly used in classical networks, such as reconfigurable optical add-drop multiplexers and optical communication repeaters[78], are not suitable for quantum signals. Instead, the quantum channel must bypass these devices to prevent the quantum signals from being disturbed. Furthermore, while classical optical communication can transmit data over hundreds of kilometers of fiber with the help of repeaters, quantum signals over such long distances become too weak relative to the background noise[74]. Consequently, a ready-to-use integration of a QKD network

into existing classical networks is not yet feasible. Designing the appropriate QKD network infrastructure[79] and coordinating with telecommunications companies is required before such integration can be realized.

[H3] Device Form-factor

For widespread applications of QKD networks, quantum devices are expected to achieve a similar level of miniaturization as those in classical networks. Dense integration of quantum devices can enhance functionality and enable the construction of scalable QKD systems. In fact, QKD systems require precise modulation of quantum states, and lithographic precision makes this achievable even in mass production. Moreover, integrated structures make components like Mach–Zehnder interferometers robust against environmental noise[80], reducing the need for feedback systems[29].

Much of the research on on-chip QKD is based on silicon and silica photonics[81] due to its mature manufacturing techniques. Modulation on silicon chips primarily relies on thermo-optic effects, whose slow response limits the choice of QKD protocols[82]. However, carrier depletion in silicon enables high-speed modulation for active QKD[70]. Additionally, developments in on-chip lithium niobate[83] provide an alternative by facilitating easier electro-optic modulation.

The main advantages of chip-based QKD systems lie in achieving monolithic hybrid integration (Fig. 2c). For QKD transmitters, it is crucial to integrate the light source directly onto the chip[84], making materials like InP[85] preferable for this purpose. For QKD receivers, integrating SNSPDs[86], SPADs[87], and homodyne detectors[88,89] onto the chip is essential. However, practical issues such as stability and optical loss in coupling communication fibers to chips must be carefully considered[90]. Solving these issues would enable the mass production of components for QKD networks and consequently reduce the cost of integration and worldwide commercial deployment.

[H3] Cooling requirements

Single-photon detectors operating in the telecommunication wavelength range require much lower temperatures than classical detectors to minimize noise. For example, SNSPDs achieve optimal performance only at temperatures much below half the critical temperature of their superconducting material —practically around 2–4 K for Nb(Ti)N-based SNSPDs[91]. This temperature necessitates multi-stage cooling systems (Fig. 2d), such as Gifford–McMahon[91] or Joule–Thomson cryocoolers[92], which have considerable size, weight, and power requirements when implemented at base stations within classical networks. Although there is ongoing research to develop SNSPDs from materials with higher critical temperatures[93], the fundamental operating principle of SNSPDs implies that the cost of cryogenic cooling systems cannot be entirely eliminated. Centralizing the SNSPD chips could reduce the number of cryogenic systems needed, crucially bringing down the cooling costs for the overall structure of QKD networks. Moreover, advances in cost-effective cryocoolers will play a crucial role in shaping the future infrastructure of QKD networks.

In contrast, SPADs can operate near or even at room temperature[94], although they generally suffer from lower detection efficiency and higher noise levels. A typical thermoelectric cooler provides

adequate cooling for SPADs, avoiding the need for cryogenic systems and offering an economical and flexible option for equipping QKD receivers[9]. Consequently, in advanced and well-funded research groups, SNSPDs are commonly employed for detecting photons in the telecommunication band. In more commercially oriented settings, however, SPADs remain the preferred choice. As global QKD transitions to commercial applications, reducing the cooling requirements may shift the cost–performance balance and ultimately reshape the motivation for building QKD networks.

[H2] Practical Security

QKD promises to guard against all types of attacks encountered in quantum mechanics and information theory, thereby providing information-theoretic security for shared keys. However, despite the rigorous derivations in security analysis, it generally assumes that all user devices are perfectly modeled—an assumption that rarely holds in practice. Such discrepancies could lead to unexpected information leakage beyond the bounds set by the security analysis, a phenomenon known as side-channels. These side-channels involve highly sensitive quantum devices designed to ensure rigorous security. Therefore, addressing these side-channel vulnerabilities is crucial for the security of QKD applications.

[H3] Attack on devices

A practical QKD system may be vulnerable to various quantum attacks due to device imperfections (Table 1). In response to the challenges posed by these quantum attacks, effective countermeasures have been proposed. Countermeasures can be broadly categorized into two main types: suitable monitoring modules and machine-learning detection modules. In monitoring modules, leveraging suitable monitoring devices to track the physical parameters of pulses, such as intensity, phase, and wavelength, guards against specific quantum attacks. However, these monitoring devices can introduce potential security vulnerabilities due to their inherent imperfections and increase the overall complexity of QKD systems. In detection modules, machine learning algorithms identify various patterns and features of quantum attacks to achieve universal attack detection in specific protocols. Though these machine-learning detection modules can handle most quantum attacks on CV-QKD protocols, they are unable to detect quantum attacks on other protocols. Therefore, it is essential to develop a universal countermeasure that can protect any practical QKD protocol from various quantum attacks. For a comprehensive overview of quantum attacks on QKD systems, readers can refer to the report ‘Implementation Attacks against QKD Systems’ commissioned by the German Federal Office for Information Security (BSI)[95].

Research on potential attack methods exploiting specific device loopholes has spurred the development of corresponding countermeasures. Although these collective efforts have clarified the issue of practical security, relying on additional devices to monitor existing ones remains a reactive

rather than a forward-looking solution.

[H3] Measurement-device-independent QKD

In one-way quantum communication, attacks on the transmitter's devices are relatively less concerning as they can be more easily monitored[96]. However, isolators are not suitable for the receiver, and the measurement of quantum states requires the receiver's devices to be highly efficient and sensitive. Consequently, many challenges in defending QKD systems against practical attacks are linked to their measurement devices. To address this issue, measurement-device-independent QKD (MDI-QKD) protocols[97], also known as side-channel-free QKD[98], were proposed. These protocols eliminate the need for specific assumptions about modeling of the measurement devices.

To elaborate a little further, in MDI-QKD protocols two authorized users each generate quantum states, while a third party positioned between them performs interference-based measurements (Fig. 3a). Although high-fidelity measurements are still required in MDI-QKD, they do not need to be trusted. The third party is treated similarly to the quantum channel, with security verified through protocol procedures. It is worth noting that typical MDI-QKD protocols require two-photon interference with pre-selected measurements, resulting in roughly the same secret key capacity as point-to-point QKD, which scales as $O(\eta)$. While MDI-QKD resolves security concerns related to measurement devices, it introduces additional untrusted nodes and necessitates precise synchronization to account for timing differences between the two channels. Moreover, practical setups with asymmetric node positions can decrease secret key capacity[99]. As a result, MDI-QKD has not been as widely applied as point-to-point QKD for network establishment, awaiting the development of new protocols that surpass the PLOB bound[56].

[H3] Device-independent QKD

Device-independent QKD (DI-QKD) protocols[100] step further by eliminating the need for any specific assumptions about the modeling of all quantum devices, aiming for the ideal level of security promised by QKD[101]. In a device-independent scenario, authorized users treat local quantum devices as black boxes, focusing solely on their classical inputs and outputs rather than on their internal operations. As a result, any potential flaws in the quantum devices due to intrinsic imperfections or malicious tampering can, in principle, be eliminated. Specifically, DI-QKD distributes the secure key through nonlocal correlation[100], with the parameter estimation resembling the process of verifying the violation of Bell inequality (Fig. 3b). However, a key challenge remains in addressing the detection loophole. In DI-QKD, only one of the detectors clicks, known as non-coincidence outcomes, must be accounted for rather than discarded during post-selection, similar to the requirements of the loophole-free Bell test[102]. This loophole makes photonic approaches[103] to DI-QKD challenging for long-distance applications, unless improved protocols[104] can relax the stringent detection efficiency requirements such as relying on a qubit amplifier[105] or the remote Bell test[104]. In contrast, DI-QKD based on the establishment of distributed entanglement, such as systems using rubidium atoms[106] and trapped ions[107], can close the detection loophole through single-shot readout, offering a promising solution for

DI-QKD networks.

However, DI-QKD still cannot conduct entirely loophole-free experiments. Unlike in a loophole-free Bell test, where the locality loophole requires measurements to be separated to exclude hidden-variable influences. This concern is not as critical in DI-QKD. The general settings of DI-QKD inherently close the locality loophole under the assumption that quantum theory is correct and that no unintended information, such as the input and output, leaks from the users' ends[106]. Nevertheless, certain assumptions about the devices such as the perfect isolation[107] still persist, leaving potential loopholes. As DI-QKD becomes widely applied in networks, these issues could still limit the implementation reliability, reducing their competitiveness against classical networks. Consequently, DI-QKD appears to be bottlenecked by the technologies required for establishing distributed entanglement, as well as by the challenge of addressing the final unresolved aspect of practical security. As a result, the community's efforts and interests are increasingly directed toward extending the scale of QKD networks.

[H1] Long-haul QKD

Long-haul QKD serves as the backbone for establishing connectivity in global quantum networks. Since the 1990s, researchers have made substantial progress in this area (Fig. 4). In 1993, the first secure QKD link over 10 km was demonstrated using BB84 ref.[108]. This was followed by the plug-and-play system in 2002, which extended the distance to 67 km[109]. The introduction of decoy-state methods[25,26] enabled distances beyond 100 km by 2007 ref. [110] and over 250 km by 2009 using ultra-low-loss fibers[111]. By 2016, MDI-QKD achieved a record fiber-based QKD distance of 404 km[112]. 2017 saw the first demonstrations of satellite-to-ground QKD[48] and intercontinental satellite-relayed networks[113]. In 2018, the twin-field QKD (TF-QKD) protocol was introduced, breaking the theoretical limit of point-to-point protocols[56]. Using ultra-low-loss fibers, TF-QKD reached 509 km in 2020 ref. [114] and surpassed 830 km in 2022 ref. [115]. In parallel, the mode-pairing QKD (MP-QKD) protocol was proposed in 2022 ref. [116,117]. In 2023, TF-QKD extended secure QKD transmission beyond 1000 km, setting a new benchmark for practical long-distance quantum communication[118]. Despite this progress, QKD must sustain high key rates at such distances before it can be implemented in global networks.

[H2] Trusted relay

Optical loss increases with distance in quantum communication the same as in classical systems. To extend distance, the most direct approach is to add relays[119]. While quantum repeaters offer a trust-free solution in principle[120], they remain costly[121] and impractical for near-term deployment. In contrast, trusted relays are often installed in physically secured suburban facilities, but substantial operational resources are required for maintaining real-time monitoring against eavesdropping.

The European project Secure Communication based on Quantum Cryptography[122] is an early example of using quantum relays to implement a quantum network. Subsequently, trusted relays have been used in many quantum networks (Fig. 5. How to deploy nodes as trusted relays in a multi-user quantum network to optimize the network's efficiency and the number of relays is also an important

issue. There are many models and algorithms regarding this aspect[123]. Another approach would be to eliminate trusted relays altogether. MDI-QKD[97] allows the use of untrusted measurement nodes, further reducing the need for trusted relays in quantum networks and thereby the security of quantum networks and mitigating the practical costs. The best approach may be to use both trusted and untrusted relays to maximize the efficiency of quantum networks in terms of cost and performance for the future development of a global quantum network[124].

[H2] Hybrid quantum-safe relay

PQC is widely considered as a compelling quantum-safe alternative to QKD. PQC can effectively mitigate security concerns associated with trusted relays in quantum networks, a concept referred to as secure relay[125] or hybrid quantum-safe cryptosystem[126]. Combining PQC with quantum communication can further enhance security, with each method mutually reinforcing the other.

To secure trusted relays across quantum networks, one intrinsic solution involves transmitting ciphertext using quantum secure direct communication[127,128]. In this method, only information pre-encrypted by PQC is encoded onto quantum states and transmitted through quantum networks. This guarantees that, even if any network relay is compromised, the security of all encrypted messages remains quantum-safe. Alternatively, PQC can be integrated with the post-processing procedure of QKD for quantum-safe key derivation[126]. Furthermore, PQC can play a vital role in public key generation and authentication processes[129], establishing a robust and reliable classical infrastructure to support quantum networks. PQC complements quantum communication by mitigating vulnerabilities of trusted relays, securing ciphertext transmission, and strengthening key management and authentication, thereby establishing a robust hybrid framework for quantum networks.

[H2] Overcoming the bounds of repeater-less systems

The PLOB bound was initially considered as the definitive bound for all repeater-less point-to-point QKD systems[53,54]. However, it was subsequently recognized as inapplicable to interference-based QKD, which operates beyond the conventional point-to-point framework. In 2018, the TF-QKD protocol[56] allowed for effective events from single-photon responses to be directly used for key generation. This protocol is based on the principle of single-photon interference, in contrast to typical MDI-QKD protocols that rely on two-photon interference. Consequently, the key generation rate overcomes the PLOB bound and is rather proportional to the square root of the transmission rate. In 2022, the MP-QKD protocol, developed[116] and concurrently proposed as asynchronous MDI-QKD[117], exceeded the PLOB bound for key generation. The MP-QKD introduces a measure-then-pair strategy based on MDI-QKD, enhancing the utilization rate of response events. These protocols also allow the key rate to be proportional to the square root of the transmittance.

To compare the two methods, TF-QKD protocol imposes extremely stringent requirements on the wavelength matching between the two communicating parties' lasers, typically necessitating a frequency difference of less than 1 Hz[56]. In contrast, conventional MDI-QKD and MP-QKD are considerably more tolerant, allowing a central wavelength mismatch of up to 125 MHz[29,130]. Moreover,

TF-QKD and MP-QKD have been validated in laboratory settings[131-133] and field fiber optic environments[43,134,135]. However, despite surpassing the repeater-less bound, these single-interference based protocols still do not meet the single-repeater bound of $-\log_2(1-\sqrt{\eta})$ for end-to-end QKD[136]. The trade-off between key rate and channel loss still exists. Consequently, exploring strategies[137] to surpass this new bound at the protocol level remains a crucial area for future research in global QKD.

[H2] Satellite QKD

It is anticipated that in the future, satellite-based quantum networks can better support global QKD. For instance, the European Quantum Communication Infrastructure (EuroQCI) project, involving all 27 EU Member States, will consist of a terrestrial segment based on fiber communication networks and a space segment utilizing satellites[138].

For a satellite-based quantum network, multiple satellites are required to complete seamless coverage of the system. Satellites can be typically divided into Low-Earth Orbit (LEO) satellites, Medium-Earth Orbit (MEO) satellites, and Geostationary-Earth Orbit (GEO) satellites. The simplest satellite-based QKD network consists of a MEO satellite and three LEO satellites[44]. LEO satellites have shorter orbital periods, allowing them to provide 24-hour service, but they cover a smaller area so that more of them are needed for seamless coverage. In contrast, GEO satellites have longer orbital periods, meaning that the effective time for QKD within a day is shorter, but they cover a larger area. The benefits and trade-offs of MEO lie between those of LEO and GEO, as its orbital altitude is intermediate between the two. Therefore, when building a satellite-based QKD network, both LEO, MEO and GEO satellites are needed to achieve efficient QKD.

Satellites use free-space attenuation. Unlike exponential loss in fibers, free-space attenuation depends on atmospheric thickness, creating a ~20 dB loss over 1000 km[44]. Satellites thus could enable global QKD across countries and continents[139]. In 2008, the feasibility of single-photon transmission was initially verified via satellite-to-ground links[140]. Subsequently, in 2013, the feasibility of QKD under high-speed motion using an aircraft platform was demonstrated[141]. Quantum communication on a high-altitude balloon platform was also achieved [142]. As of 2025, the largest project is the Micius Quantum Science Experimental Satellite[44]. Two ground stations connected by Micius, Xinglong and Nanshan, are 2600 km apart. This communication distance was previously the longest achieved in single-relay QKD but has now been extended to 12,900 km[10].

Finally, the size and weight of satellite systems are also critical factors for successful operation[113]. More integrated systems offer smaller form factors for QKD systems, and could be potential solutions for quantum satellite networks[143]. In summary, satellite-based quantum networks provide a crucial pathway to extend QKD beyond the limits of optical fibers, enabling global-scale secure communication. Leveraging complementary LEO, MEO, and GEO satellites together with integrated

satellite systems will be key to building global quantum networks.

[H2] Fiber-based Terrestrial QKD networks

As QKD evolves toward large-scale deployment, building multi-user, multi-node quantum networks become inevitable. Practical implementation must consider diverse communication distances, asymmetric demands, and inter-channel crosstalk. For terrestrial links, optical fibers are the preferred medium due to low loss, electromagnetic immunity, and deployment readiness, despite demonstrations using free space and even underwater channels[144,145], where commercial fibers generally meet quantum communication requirements. Depending on the transmission scale, fiber-based QKD networks are typically classified as metropolitan or intercity.

[H3] Metropolitan areas

In metropolitan area QKD quantum networks, the distance of optical fibers is usually only a few kilometers to tens of kilometers but usually requires many nodes. For example, the quantum network in Hefei has 46 nodes[146]. It is therefore necessary to design a reasonable topology to optimize the overall key generation efficiency. Meanwhile, various practical factors in node deployment must also be considered, such as the fact that some locations may not be geographically suitable for use as intermediate trusted relays. In metropolitan networks, MDI-QKD reduces system complexity by enabling detector sharing, while optimized protocol parameters compensate for channel asymmetry[99]. One of the most straightforward ways to address an asymmetric path is to apply attenuation compensation to the less attenuated segment, making the situation symmetrical. However, the parameters under asymmetric conditions have been optimized to achieve a higher coding rate without needing attenuation compensation, even surpassing the results obtained with added attenuation[147].

Optical switching and secure key management in practical metropolitan quantum networks are also crucial[148] for optimizing the end-to-end key rate of QKD network. The switching can be categorized into two types: matrix switching and fully connected switching. Matrix switching does not allow any two users to connect freely, whereas fully connected switching enables users connected to the optical switch to establish connections between two endpoints.

Overall, metropolitan quantum networks must balance topology design, protocol optimization, and switching strategies to maximize key generation efficiency. Addressing channel asymmetry and enabling flexible interconnections are crucial steps toward building practical large-scale urban QKD infrastructures.

[H3] Intercity areas

Like metropolitan quantum networks, the setup of trusted relays in intercity networks also has to consider distance, fiber environment, and cost to ensure their efficient operation. Intercity quantum networks typically span hundreds of kilometers, where the effects of photon attenuation, dispersion, and scattering in optical fibers dominate[43]. Several countries, including the United States, Europe,

China, and others, have already begun establishing intercity quantum networks (Fig. 5).

One challenge in establishing intercity quantum networks is that long-distance fibers also contain multiple splicing points, introducing reflection and inter-channel crosstalk[134,135]. Quantum information is typically transmitted alongside classical optical communication[76], either in different optical cables or even in different fibers within the same cable. This often requires accounting for the various interferences introduced by classical optical signals and employing methods to reduce them. Most protocols have key rates scaling with the square of transmittance, making even small improvements in loss crucial for enhancing overall performance. Moreover, some classical synchronization signals often need to be amplified over intercity distances using optical amplifiers[134], making it even more crucial to address the crosstalk between the synchronization signals and optical quantum signals. Quantum noise also greatly increases over large intercity distances, ultimately degrading signal-to-noise ratio and reducing the achievable secure key rate.

However, at intercity distances up to 200 km apart, the TF-QKD and MP-QKD protocols have demonstrated advantages regarding key rate and security. By exploiting single-photon interference and mode-pairing strategies, these protocols achieve a more favorable $\sqrt{\eta}$ scaling, surpass the PLOB bound, and offer improved tolerance to channel loss and noise. These features are crucial for extending QKD from metropolitan links to practical intercity backbones, where both distance and stability are critical. The diversity of implementation methods[149] for TF-QKD and the simplicity of MP-QKD experimental setups give these two protocols even an broader application appeal. Therefore, TF-QKD and MP-QKD protocols are likely to become important protocols for future intercity quantum networks.

In summary, intercity quantum networks face significant challenges from loss, noise, and classical crosstalk, making protocol and infrastructure optimization essential. TF-QKD and MP-QKD stand out as promising solutions, combining practical feasibility with enhanced key rates and security, and are therefore strong candidates for the backbone of future intercity quantum networks.

[H1] Outlook

To extend communication distances, the core challenge lies in capturing more of the encoded information carried by photons. Beyond the aforementioned approaches to increase the key rate, the use of quantum repeaters can enhance the key rate up to the N-repeater bound[136] of $-\log_2\left(1-\sqrt[N+1]{\eta}\right)$. Although still far from realization, the establishment of quantum repeater networks[8] could address major performance challenges, including key rate limitations and security loopholes. For example, long-distance entanglement can be established by combining short-distance entanglement generation with entanglement swapping[120], which also supports the implementation of DI-QKD. Regarding security, fully passive QKD protocols have also been proposed to eliminate side-channel vulnerabilities introduced by active modulation[65,150] beyond what is possible through MDI-QKD and DI-QKD. High-dimensional QKD[151] encodes quantum states in a Hilbert space with dimension d>2 to improve noise tolerance. However, though the information density per mode $\log_2(d)/d$ can be slightly

increased when d=3, it tends to decrease for larger d, as higher-dimensional systems typically require more detectors. The measure-then-pair strategy introduced in MP-QKD offers an alternative route to enhance information density through techniques such as wavelength-division multiplexing[152].

As a quantum counterpart to the internet[153], the global QKD network will consist of multiple layers, each tailored to specific application requirements. A potential layout for a future global QKD network considers factors such as transmission distance, user numbers, integration needs, and data transmission volume across various application scenarios (Fig. 6). The challenge lies in the difficulty of quantitatively evaluating the practical security for the entire setup.[154]. Despite their paramount importance, security issues in QKD projects tend to receive less attention from funders and contractors, and key rates and costs are often prioritized instead. However, it is important to note that, compared with classical cryptography such as PQC, the only unique advantage of QKD lies in its unconditional security, which comes at the expense of capacity and cost. The motivation for establishing a global QKD network would be weakened if the strict requirements on security were to be deprioritized.

Additionally, different vendors and protocols often adopt distinct implementations and encoding schemes. Standardized interfaces and comprehensive testing frameworks, such as those published by the International Organization for Standardization and the International Electrotechnical Commission[155], are essential for enabling multi-vendor deployment, facilitating cross-border QKD operations, and ultimately establishing a globally integrated, quantum-secure communication infrastructure.

If all of these challenges are addressed, Global QKD promises to establish a worldwide, information-theoretically secure connection among all authorized users, offering practical capacity and cost-effectiveness.

[H1] References:

1 Devetak, I. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory* 51, 44–55 (2005).

2 Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science* 560, 7–11 (2014). Introduces the first quantum key distribution protocol, laying the foundation for modern quantum cryptography.

3 Renner, R., Gisin, N. & Kraus, B. Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A* 72, 012332 (2005).

4 Bernstein, D. J. & Lange, T. Post-quantum cryptography. *Nature* 549, 188–194 (2017).

5 Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review* 41, 303–332 (1999) Demonstrates that quantum algorithms efficiently solve integer factorization and discrete logarithm problems, posing a threat to the security of classical cryptosystems..

6 Mehic, M. *et al.* Quantum key distribution: a networking perspective. *ACM Computing Surveys (CSUR)* **53**, 1–41 (2020).
7 Awschalom, D. D. *et al.* A Roadmap for Quantum Interconnects. Medium: ED; Size: 48 p. (United States, 2022).
8 Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: A vision for the road ahead. *Science* **362**, eaam9288 (2018). **Presents a comprehensive vision for the quantum internet, situating quantum key distribution in the context of global quantum networks.**
9 Pittaluga, M. *et al.* Long-distance coherent quantum communications in deployed telecom networks. *Nature* **640**, 911–917, doi:10.1038/s41586-025-08801-w (2025).
10 Li, Y. *et al.* Microsatellite-based real-time quantum key distribution. *Nature* **640**, 47–54, doi:10.1038/s41586-025-08739-z (2025).
11 Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Physical review letters* **68**, 3121 (1992).
12 Vallone, G. *et al.* Free-space quantum key distribution by rotation-invariant twisted photons. *Physical review letters* **113**, 060503 (2014).
13 Inoue, K., Waks, E. & Yamamoto, Y. Differential phase shift quantum key distribution. *Physical review letters* **89**, 037902 (2002).
14 Stucki, D., Brunner, N., Gisin, N., Scarani, V. & Zbinden, H. Fast and simple one-way quantum key distribution. *Applied Physics Letters* **87** (2005).
15 Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **509**, 475–478 (2014).
16 Moroder, T. *et al.* Security of distributed-phase-reference quantum key distribution. *Physical review letters* **109**, 260501 (2012).
17 Sandfuchs, M., Haberland, M., Vilasini, V. & Wolf, R. Security of differential phase shift QKD from relativistic principles. *Quantum* **9**, 1611 (2025).
18 Ralph, T. C. Continuous variable quantum cryptography. *Physical Review A* **61**, 010303, doi:10.1103/PhysRevA.61.010303 (1999).
19 Weedbrook, C. *et al.* Quantum cryptography without switching. *Physical review letters* **93**, 170504 (2004).
20 Grosshans, F. *et al.* Quantum key distribution using gaussian-modulated coherent states. *Nature* **421**, 238–241 (2003).
21 Hillery, M. Quantum cryptography with squeezed states. *Physical Review A* **61**, 022309 (2000).
22 Weedbrook, C., Pirandola, S., Lloyd, S. & Ralph, T. C. Quantum cryptography approaching the classical limit. *Physical review letters* **105**, 110501 (2010).
23 Silberhorn, C., Ralph, T. C., Lütkenhaus, N. & Leuchs, G. Continuous variable quantum cryptography: Beating the 3 dB loss limit. *Physical review letters* **89**, 167901 (2002).
24 Usenko, V. C. & Grosshans, F. Unidimensional continuous-variable quantum key distribution. *Physical Review A* **92**, 062337 (2015).
25 Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Physical review letters* **94**, 230504 (2005). **Introduces the decoy-state method, enabling feasible long-distance quantum key distribution.**
26 Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical review letters* **94**, 230503 (2005).
27 Albota, M. A. & Wong, F. N. Efficient single-photon counting at 1.55 μm by means of frequency upconversion. *Optics letters* **29**, 1449–1451 (2004).
28 Gol'Tsman, G. *et al.* Picosecond superconducting single-photon optical detector. *Applied physics letters* **79**, 705–707 (2001).

29 Zhang, H. *et al.* Noise-reducing quantum key distribution. *Reports on Progress in Physics* **88**, 016001, doi:10.1088/1361-6633/ad9505 (2025).

30 Itzler, M. A. *et al.* Advances in InGaAsP-based avalanche diode single photon detectors. *Journal of Modern Optics* **58**, 174–200 (2011).

31 Ceccarelli, F. *et al.* Recent advances and future perspectives of single-photon avalanche diodes for quantum photonics applications. *Advanced Quantum Technologies* **4**, 2000102 (2021).

32 Zappa, F., Lotito, A., Giudice, A. C., Cova, S. & Ghioni, M. Monolithic active-quenching and active-reset circuit for single-photon avalanche detectors. *IEEE Journal of Solid-State Circuits* **38**, 1298–1301 (2003).

33 Acerbi, F., Anti, M., Tosi, A. & Zappa, F. Design criteria for InGaAs/InP single-photon avalanche diode. *IEEE Photonics Journal* **5**, 6800209–6800209 (2013).

34 Chang, J. *et al.* Detecting telecom single photons with 99.5− 2.07+ 0.5% system detection efficiency and high time resolution. *APL Photonics* **6** (2021).

35 Caloz, M. *et al.* High-detection efficiency and low-timing jitter with amorphous superconducting nanowire single-photon detectors. *Applied Physics Letters* **112** (2018).

36 Hu, P. *et al.* Detecting single infrared photons toward optimal system detection efficiency. *Optics Express* **28**, 36884–36891 (2020).

37 Chiles, J. *et al.* New constraints on dark photon dark matter with superconducting nanowire detectors in an optical haloscope. *Physical Review Letters* **128**, 231802 (2022).

38 You, L. Superconducting nanowire single-photon detectors for quantum information. *Nanophotonics* **9**, 2673–2692 (2020).

39 Renema, J. *et al.* Experimental test of theories of the detection mechanism in a nanowire superconducting single photon detector. *Physical review letters* **112**, 117604 (2014).

40 Qi, R., Zhang, H., Gao, J., Yin, L. & Long, G.-L. Loophole-free plug-and-play quantum key distribution. *New Journal of Physics* **23**, 063058 (2021).

41 Zhang, X. *et al.* Polarization-encoded quantum key distribution with a room-temperature telecom single-photon emitter. *National Science Review* **12**, doi:10.1093/nsr/nwaf147 (2025).

42 Zhang, H. *et al.* Metropolitan quantum key distribution using a GaN-based room-temperature telecommunication single-photon source. *Physical Review Applied* **23**, 054022, doi:10.1103/PhysRevApplied.23.054022 (2025).

43 Chen, J.-P. *et al.* Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. *Nature Photonics* **15**, 570–575 (2021).

44 Lu, C.-Y., Cao, Y., Peng, C.-Z. & Pan, J.-W. Micius quantum experiments in space. *Reviews of Modern Physics* **94**, 035001 (2022).

45 Avesani, M. *et al.* Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. *npj Quantum Information* **7**, 93 (2021).

46 Scriminich, A. *et al.* Optimal design and performance evaluation of free-space quantum key distribution systems. *Quantum Science and Technology* **7**, 045029 (2022).

47 Tian, X.-H. *et al.* Experimental Demonstration of Drone-Based Quantum Key Distribution. *Physical Review Letters* **133**, 200801 (2024).

48 Liao, S.-K. *et al.* Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017). **Demonstrates the first successful satellite-to-ground quantum key distribution, paving the way for global-scale quantum network**.

49 Liao, S.-K. *et al.* Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nature Photonics* **11**, 509–513 (2017).

50 Kundu, N. K., Dash, S. P., Mckay, M. R. & Mallik, R. K. Channel estimation and secret key rate analysis of MIMO terahertz quantum key distribution. *IEEE Transactions on Communications* **70**, 3350–3363 (2022).

51 Chen, J.-P. *et al.* Quantum Key Distribution over 658 km Fiber with Distributed Vibration Sensing. *Physical Review Letters* **128**, 180502, doi:10.1103/PhysRevLett.128.180502 (2022).

52 Zhang, H. *et al.* Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states. *Light: Science & Applications* **11**, 83, doi:10.1038/s41377-022-00769-w (2022).

53 Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature Communications* **5**, 5235, doi:10.1038/ncomms6235 (2014).

54 Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nature communications* **8**, 15043 (2017). **Defines the tight fundamental rate–loss bound for repeaterless point-to-point QKD, now a benchmark for emerging protocols.**

55 Mizutani, A. & Tsurumaru, T. Tight scaling of key rate for differential-phase-shift quantum key distribution. *Physical Review Research* **6**, 043300, doi:10.1103/PhysRevResearch.6.043300 (2024).

56 Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018). **Proposes the twin-field quantum key distribution protocol, first to surpass the fundamental rate–loss bound, revolutionizing long-distance quantum key distribution research.**

57 Numkam Fokoua, E., Abokhamis Mousavi, S., Jasion, G. T., Richardson, D. J. & Poletti, F. Loss in hollow-core optical fibers: mechanisms, scaling rules, and limits. *Adv. Opt. Photon.* **15**, 1–85, doi:10.1364/AOP.470592 (2023).

58 Takesue, H. *et al.* Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. *Nature photonics* **1**, 343–348 (2007).

59 Rey-Domínguez, J., Navarrete, Á., van Loock, P. & Curty, M. Hacking coherent-one-way quantum key distribution with present-day technology. *Quantum Science and Technology* **9**, 035044 (2024).

60 González-Payo, J., Trényi, R., Wang, W. & Curty, M. Upper security bounds for coherent-one-way quantum key distribution. *Physical Review Letters* **125**, 260510 (2020).

61 Grünenfelder, F., Boaron, A., Rusca, D., Martin, A. & Zbinden, H. Performance and security of 5 GHz repetition rate polarization-based quantum key distribution. *Applied Physics Letters* **117** (2020).

62 Boaron, A. *et al.* Secure quantum key distribution over 421 km of optical fiber. *Physical review letters* **121**, 190502 (2018).

63 Korzh, B. *et al.* Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector. *Nature Photonics* **14**, 250–255 (2020).

64 Bouchard, F., England, D., Bustard, P. J., Heshami, K. & Sussman, B. Quantum communication with ultrafast time-bin qubits. *PRX Quantum* **3**, 010332 (2022).

65 Wang, W. *et al.* Fully passive quantum key distribution. *Physical Review Letters* **130**, 220801 (2023).

66 Zapatero, V., Navarrete, Á., Tamaki, K. & Curty, M. Security of quantum key distribution with intensity correlations. *Quantum* **5**, 602 (2021).

67 Yuan, Z. *et al.* 10-Mb/s quantum key distribution. *Journal of Lightwave Technology* **36**, 3427–3433 (2018).

68 Zhang, W. *et al.* A 16-pixel interleaved superconducting nanowire single-photon detector array with a maximum count rate exceeding 1.5 GHz. *IEEE Transactions on Applied Superconductivity* **29**, 1–4 (2019).

69 Grünenfelder, F. *et al.* Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems. *Nature Photonics* **17**, 422–426 (2023).

70 Li, W. *et al.* High-rate quantum key distribution exceeding 110 Mb s–1. *Nature Photonics* **17**, 416–421 (2023).

71 Kržič, A. *et al.* Towards metropolitan free-space quantum networks. *npj Quantum Information* **9**, 95 (2023).

72 Cavaliere, F., Prati, E., Poti, L., Muhammad, I. & Catuogno, T. Secure quantum communication technologies and systems: From labs to markets. *Quantum Reports* **2**, 80–106 (2020).
73 Dynes, J. *et al.* Cambridge quantum network. *npj Quantum Information* **5**, 101 (2019).
74 Dou, T. *et al.* Coexistence of 11 Tbps (110× 100 Gbps) classical optical communication and quantum key distribution based on single-mode fiber. *Optics Express* **32**, 28356–28369 (2024).
75 Kumar, R., Qin, H. & Alléaume, R. Coexistence of continuous variable QKD with intense DWDM classical channels. *New Journal of Physics* **17**, 043027 (2015).
76 Mao, Y. *et al.* Integrating quantum key distribution with classical communications in backbone fiber network. *Optics express* **26**, 6010–6020 (2018).
77 Wang, B.-X. *et al.* Long-distance transmission of quantum key distribution coexisting with classical optical communication over a weakly-coupled few-mode fiber. *Optics express* **28**, 12558–12565 (2020).
78 Simmons, J. M. *Optical Network Design and Planning*. (Springer International Publishing, 2014).
79 Cao, Y. *et al.* The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Communications Surveys & Tutorials* **24**, 839–894 (2022).
80 Bunandar, D. *et al.* Metropolitan quantum key distribution with silicon photonics. *Physical Review X* **8**, 021009 (2018).
81 Luo, W. *et al.* Recent progress in quantum photonic chips for quantum communication and internet. *Light: Science & Applications* **12**, 175 (2023).
82 Zhang, G.-W. *et al.* Polarization-insensitive interferometer based on a hybrid integrated planar light-wave circuit. *Photonics Research* **9**, 2176–2181 (2021).
83 Renaud, D. *et al.* Sub-1 Volt and high-bandwidth visible to near-infrared electro-optic modulators. *Nature Communications* **14**, 1496 (2023).
84 Paraïso, T. K. *et al.* A modulator-free quantum key distribution transmitter chip. *npj Quantum Information* **5**, 42 (2019).
85 Sibson, P. *et al.* Chip-based quantum key distribution. *Nature communications* **8**, 13984 (2017).
86 Najafi, F. *et al.* On-chip detection of non-classical light by scalable integration of single-photon detectors. *Nature communications* **6**, 5873 (2015).
87 Martinez, N. J. *et al.* Single photon detection in a waveguide-coupled Ge-on-Si lateral avalanche photodiode. *Optics express* **25**, 16130–16139 (2017).
88 Zhang, G. *et al.* An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nature Photonics* **13**, 839–842 (2019).
89 Bruynsteen, C., Vanhoecke, M., Bauwelinck, J. & Yin, X. Integrated balanced homodyne photonic–electronic detector for beyond 20 GHz shot-noise-limited measurements. *Optica* **8**, 1146–1152 (2021).
90 Dolphin, J. A. *et al.* A hybrid integrated quantum key distribution transceiver chip. *npj Quantum Information* **9**, 84, doi:10.1038/s41534-023-00751-3 (2023).
91 Ma, R. *et al.* Disorder enhanced relative intrinsic detection efficiency in NbTiN superconducting nanowire single photon detectors at high temperature. *Applied Physics Letters* **124**, 072601 (2024).
92 Gemmell, N. R. *et al.* A miniaturized 4 K platform for superconducting infrared photon counting detectors. *Superconductor Science and Technology* **30**, 11LT01 (2017).
93 Charaev, I. *et al.* Single-photon detection using large-scale high-temperature MgB2 sensors at 20 K. *Nature Communications* **15**, 3973 (2024).
94 Na, N. *et al.* Room temperature operation of germanium–silicon single-photon avalanche diode. *Nature* **627**, 295–300, doi:10.1038/s41586-024-07076-x (2024).
95 Marquardt, C. *et al. Implementation attacks against QKD systems*. (Federal Office for Information Security,

2023).
96 Lucamarini, M. *et al.* Practical security bounds against the trojan-horse attack in quantum key distribution. *Physical Review X* **5**, 031030 (2015).
97 Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Physical review letters* **108**, 130503 (2012).
98 Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Physical review letters* **108**, 130502 (2012).
99 Wang, W., Xu, F. & Lo, H.-K. Asymmetric protocols for scalable high-rate measurement-device-independent quantum key distribution networks. *Physical Review X* **9**, 041012 (2019).
100 Zapatero, V. *et al.* Advances in device-independent quantum key distribution. *npj quantum information* **9**, 10 (2023).
101 Arnon-Friedman, R., Dupuis, F., Fawzi, O., Renner, R. & Vidick, T. Practical device-independent quantum cryptography via entropy accumulation. *Nature communications* **9**, 459 (2018).
102 Hensen, B. *et al.* Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526**, 682–686 (2015).
103 Liu, W.-Z. *et al.* Toward a photonic demonstration of device-independent quantum key distribution. *Physical Review Letters* **129**, 050502 (2022).
104 Tan, E. Y.-Z. & Wolf, R. Entropy bounds for device-independent quantum key distribution with local Bell test. *Physical Review Letters* **133**, 120803 (2024).
105 Gisin, N., Pironio, S. & Sangouard, N. Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier. *Physical review letters* **105**, 070501 (2010).
106 Zhang, W. *et al.* A device-independent quantum key distribution system for distant users. *Nature* **607**, 687–691 (2022). **Demonstrates device-independent quantum key distribution with entangled rubidium atoms, first to close untrusted-device loopholes and resist general attacks.**
107 Nadlinger, D. P. *et al.* Experimental quantum key distribution certified by Bell's theorem. *Nature* **607**, 682–686 (2022). **Demonstrates device-independent quantum key distribution with entangled trapped ions, first to close untrusted-device loopholes and resist general attacks.**
108 Townsend, P. D., Rarity, J. & Tapster, P. Single photon interference in 10 km long optical fibre interferometer. *Electronics Letters* **7**, 634–635 (1993).
109 Stucki, D., Gisin, N., Guinnard, O., Ribordy, G. & Zbinden, H. Quantum key distribution over 67 km with a plug&play system. *New Journal of Physics* **4**, 41 (2002).
110 Peng, C.-Z. *et al.* Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Physical review letters* **98**, 010505 (2007).
111 Stucki, D. *et al.* High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New Journal of Physics* **11**, 075003 (2009).
112 Yin, H.-L. *et al.* Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical review letters* **117**, 190501 (2016).
113 Liao, S.-K. *et al.* Satellite-relayed intercontinental quantum network. *Physical review letters* **120**, 030501 (2018).
114 Chen, J.-P. *et al.* Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km. *Physical review letters* **124**, 070501 (2020).
115 Wang, S. *et al.* Twin-field quantum key distribution over 830-km fibre. *Nature photonics* **16**, 154–161 (2022).
116 Zeng, P., Zhou, H., Wu, W. & Ma, X. Mode-pairing quantum key distribution. *Nature Communications* **13**, 3903 (2022).
117 Xie, Y.-M. *et al.* Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon

interference. *PRX Quantum* **3**, 020315 (2022).

118 Liu, Y. *et al.* Experimental twin-field quantum key distribution over 1000 km fiber distance. *Physical Review Letters* **130**, 210801 (2023).

119 Cao, Y. *et al.* From single-protocol to large-scale multi-protocol quantum networks. *IEEE Network* **36**, 14–22 (2022).

120 Azuma, K. *et al.* Quantum repeaters: From quantum networks to the quantum internet. *Reviews of Modern Physics* **95**, 045006, doi:10.1103/RevModPhys.95.045006 (2023).

121 Liu, J.-L. *et al.* Creation of memory–memory entanglement in a metropolitan quantum network. *Nature* **629**, 579–585, doi:10.1038/s41586-024-07308-0 (2024).

122 Peev, M. *et al.* The SECOQC quantum key distribution network in Vienna. *New Journal of Physics* **11**, 075001 (2009).

123 Yang, C., Zhang, H. & Su, J. The QKD network: Model and routing scheme. *Journal of Modern Optics* **64**, 2350–2362 (2017).

124 Cao, Y. *et al.* Hybrid trusted/untrusted relay-based quantum key distribution over optical backbone networks. *IEEE Journal on Selected Areas in Communications* **39**, 2701–2718 (2021).

125 Long, G.-L. *et al.* An evolutionary pathway for the quantum internet relying on secure classical repeaters. *IEEE Network* **36**, 82–88 (2022).

126 Garms, L. *et al.* Experimental Integration of Quantum Key Distribution and Post-Quantum Cryptography in a Hybrid Quantum-Safe Cryptosystem. *Advanced Quantum Technologies* **7**, 2300304, doi:https://doi.org/10.1002/qute.202300304 (2024).

127 Long, G.-L. & Liu, X.-S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Physical Review A* **65**, 032302 (2002).

128 Wu, J., Long, G.-L. & Hayashi, M. Quantum secure direct communication with private dense coding using a general preshared quantum state. *Physical Review Applied* **17**, 064011 (2022).

129 Wang, M. & Long, G.-L. Lattice-based access authentication scheme for quantum communication networks. *Science China Information Sciences* **67**, 222501 (2024).

130 Zhu, H.-T. *et al.* Experimental mode-pairing measurement-device-independent quantum key distribution without global phase locking. *Physical Review Letters* **130**, 030801 (2023).

131 Zhang, L. *et al.* Experimental Mode-Pairing Quantum Key Distribution Surpassing the Repeaterless Bound. *Physical Review X* **15**, 021037, doi:10.1103/PhysRevX.15.021037 (2025).

132 Wang, S. *et al.* Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system. *Physical Review X* **9**, 021046 (2019).

133 Shao, S.-F. *et al.* High-Rate Measurement-Device-Independent Quantum Communication without Optical Reference Light. *Physical Review X* **15**, 021066, doi:10.1103/PhysRevX.15.021066 (2025).

134 Liu, H. *et al.* Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km. *Physical Review Letters* **126**, 250502 (2021).

135 Zhu, H.-T. *et al.* Field test of mode-pairing quantum key distribution. *Optica* **11**, 883–888 (2024).

136 Pirandola, S. End-to-end capacities of a quantum communication network. *Communications Physics* **2**, 51 (2019).

137 Zou, M. *et al.* Realization of an untrusted intermediate relay architecture using a quantum dot single-photon source. *Nature Physics*, doi:10.1038/s41567-025-03005-5 (2025).

138 Ribezzo, D. *et al.* Deploying an Inter-European Quantum Network. *Advanced Quantum Technologies* **6**, 2200061, doi:https://doi.org/10.1002/qute.202200061 (2023).

139 Lim, C. C.-W., Xu, F., Pan, J.-W. & Ekert, A. Security Analysis of Quantum Key Distribution with Small Block

Length and Its Application to Quantum Space Communications. *Physical Review Letters* **126**, 100501, doi:10.1103/PhysRevLett.126.100501 (2021).

140 Villoresi, P. *et al.* Experimental verification of the feasibility of a quantum channel between space and Earth. *New Journal of Physics* **10**, 033038 (2008).

141 Nauerth, S. *et al.* Air-to-ground quantum communication. *Nature Photonics* **7**, 382–386 (2013).

142 Wang, J.-Y. *et al.* Direct and full-scale experimental verifications towards ground–satellite quantum key distribution. *Nature Photonics* **7**, 387–393 (2013).

143 Chen, Y.-A. *et al.* An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 214–219 (2021). Reports the largest integrated space-to-ground QKD network, spanning 4,600 kilometres.

144 Cao, Y. *et al.* Long-distance free-space measurement-device-independent quantum key distribution. *Physical Review Letters* **125**, 260503 (2020).

145 Ji, L. *et al.* Towards quantum communications in free-space seawater. *Optics Express* **25**, 19795–19806 (2017).

146 Chen, T.-Y. *et al.* Implementation of a 46-node quantum metropolitan area network. *npj Quantum Information* **7**, 134 (2021).

147 Zhong, X., Wang, W., Qian, L. & Lo, H.-K. Proof-of-principle experimental demonstration of twin-field quantum key distribution over optical channels with asymmetric losses. *npj Quantum Information* **7**, 8 (2021).

148 Chen, T.-Y. *et al.* Metropolitan all-pass and inter-city quantum communication network. *Optics express* **18**, 27217–27225 (2010).

149 Chen, J.-P. *et al.* Twin-Field Quantum Key Distribution with Local Frequency Reference. *Physical Review Letters* **132**, 260802, doi:10.1103/PhysRevLett.132.260802 (2024).

150 Lu, F.-Y. *et al.* Experimental Demonstration of Fully Passive Quantum Key Distribution. *Physical Review Letters* **131**, 110802, doi:10.1103/PhysRevLett.131.110802 (2023).

151 Cerf, N. J., Bourennane, M., Karlsson, A. & Gisin, N. Security of Quantum Key Distribution Using d-Level Systems. *Physical Review Letters* **88**, 127902, doi:10.1103/PhysRevLett.88.127902 (2002).

152 Zhou, X.-Y. *et al.* Enhancing the performance of mode-pairing quantum key distribution by wavelength division multiplexing. *Optics Express* **32**, 18366–18378, doi:10.1364/OE.519591 (2024).

153 Kimble, H. J. The quantum internet. *Nature* **453**, 1023–1030, doi:10.1038/nature07127 (2008).

154 Makarov, V. *et al.* Preparing a commercial quantum key distribution system for certification against implementation loopholes. *Physical Review Applied* **22**, 044076 (2024).

155 Länger, T. & Lenhart, G. Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD. *New Journal of Physics* **11**, 055051 (2009).

156 Mao, Y. *et al.* Hidden-Markov-model-based calibration-attack recognition for continuous-variable quantum key distribution. *Physical Review A* **101**, 062320 (2020).

157 Qin, H., Kumar, R. & Alléaume, R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Physical Review A* **94**, 012325 (2016).

158 Huang, J.-Z. *et al.* Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Physical Review A* **87**, 062329 (2013).

159 Huang, A. *et al.* Laser-seeding attack in quantum key distribution. *Physical Review Applied* **12**, 064043 (2019).

160 Tang, Y.-L. *et al.* Source attack of decoy-state quantum key distribution using phase information. *Physical Review A* **88**, 022308 (2013).

161 Xu, F., Qi, B. & Lo, H.-K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics* **12**, 113026 (2010).

162 Qin, H., Kumar, R., Makarov, V. & Alléaume, R. Homodyne-detector-blinding attack in continuous-variable

quantum key distribution. *Physical Review A* **98**, 012312 (2018).
163 Yuan, Z., Dynes, J. F. & Shields, A. J. Avoiding the blinding attack in QKD. *Nature Photonics* **4**, 800–801 (2010).
164 Ma, X.-C., Sun, S.-H., Jiang, M.-S. & Liang, L.-M. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems. *Physical Review A* **88**, 022339 (2013).
165 Peng, Q. *et al.* Practical security of twin-field quantum key distribution with optical phase-locked loop under wavelength-switching attack. *npj Quantum Information* **11**, 7, doi:10.1038/s41534-025-00963-9 (2025).
166 Stucki, D. *et al.* Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New Journal of Physics* **13**, 123001 (2011).
167 Wang, S. *et al.* Field test of wavelength-saving quantum key distribution network. *Optics letters* **35**, 2454–2456 (2010).
168 Sasaki, M. *et al.* Field test of quantum key distribution in the Tokyo QKD Network. *Optics express* **19**, 10387–10409 (2011).

[H1] ACKNOWLEDGMENTS

This work is supported by ASTAR (M21K2c0116, M24M8b0004), Singapore National Research Foundation (NRF-CRP22-2019-0004, NRF2023-ITC004-001, NRF-CRP30-2023-0003, NRF-CRP31-0001, NRF-MSG-2023-0002), Singapore Ministry of Education Tier 2 Grant (MOE-T2EP50222-0018). We acknowledge the support of Dieter Schwarz Stiftung GmbH for the QUASAR project.

[H1] COMPETING INTERESTS

The authors declare no competing interests.

[H1] CONTRIBUTONS

H.Z. and H.Z. researched data for the article, All authors contributed substantially to discussion of the content, wrote the article. H.Z., H.Z., L.H. and W.G. reviewed and edited the manuscript before submission.

Peer review information

Nature Reviews Electrical Engineering thanks [Referee#1 name], [Referee#2 name] and the other, anonymous, reviewer(s) for their contribution to the peer review of this work.

Table 1. Typical quantum attacks against quantum key distribution (QKD)

Quantum attack	Target device*	Protocol	Countermeasures	References
Calibration attack	Local oscillator	Continuous variable (CV)	Hidden-Markov-model-based recognition	ref. [156]
Saturation attack	Homodyne detector	CV	Gaussian post-selection	ref. [157]
Wavelength attack	Beam splitter	CV	Incorporating a simple wavelength filter	ref. [158]
Laser-seeding attack	Source	Discrete variable (DV)	Incorporating an external isolator	ref. [159]
Source attack	Source	DV	Implementing phase randomization	ref. [160]
Phase-remapping attack	Phase modulator	DV	Enhancing timing control and implementing phase randomization	ref. [161]
Blinding attack	Homodyne detectorAvalanche photodiode	CV DV	Using a sensitive p-i-n photodiode	ref. [162,163]
Local oscillator - intensity attack	Local oscillator	CV	Monitoring the Local oscillator intensity	ref. [164]
Wavelength-switching attack	Acousto-optic modulator	DV	Well-calibrated modulator	ref. [165*]

* The specific devices under attack, as well as the corresponding countermeasure methods, differ depending on the attack schemes associated with each protocol.

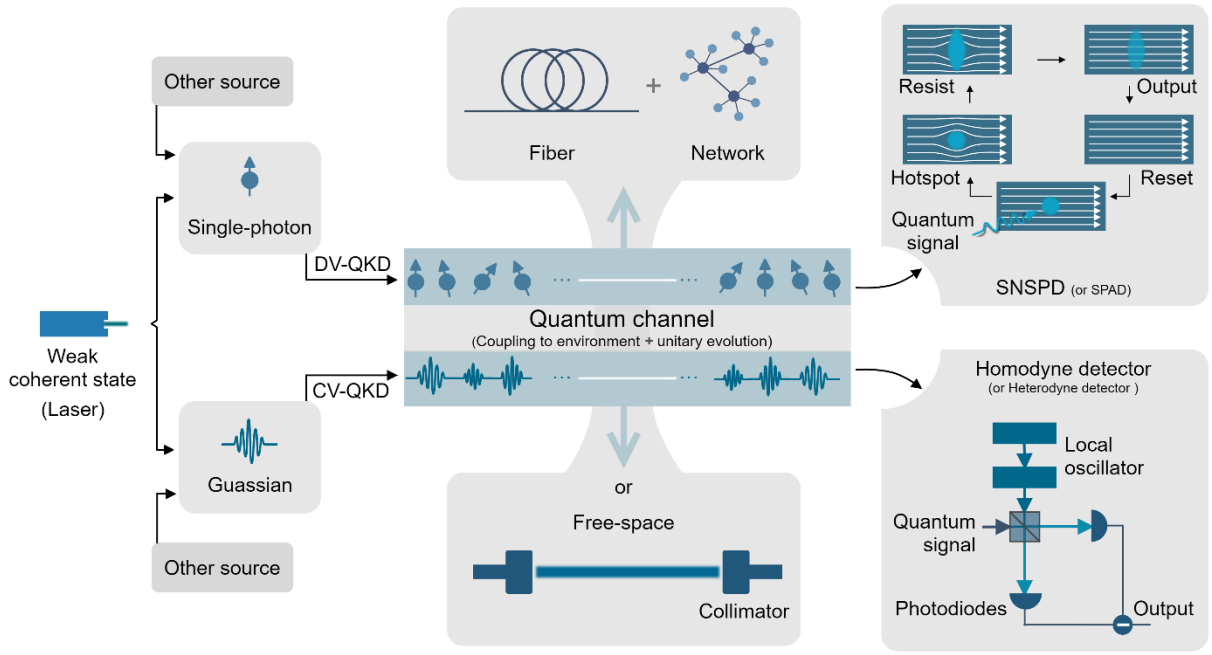

Figure 1 Schematic of quantum key distribution (QKD) systems employing discrete-variable (DV) and continuous-variable (CV) encoding. From an implementation perspective, DV and CV schemes are largely similar, as they can share the same sources and channels. The weak coherent state is used to simulate a single-photon source in DV-QKD, as its Poisson distribution primarily consists of vacuum and single-photon components. The quantum channel is commonly implemented via fiber or free-space links. DV-QKD typically employs superconducting nanowire single-photon detector (SNSPD) or single-photon avalanche diode (SPAD), whereas CV-QKD relies on homodyne or heterodyne detection.

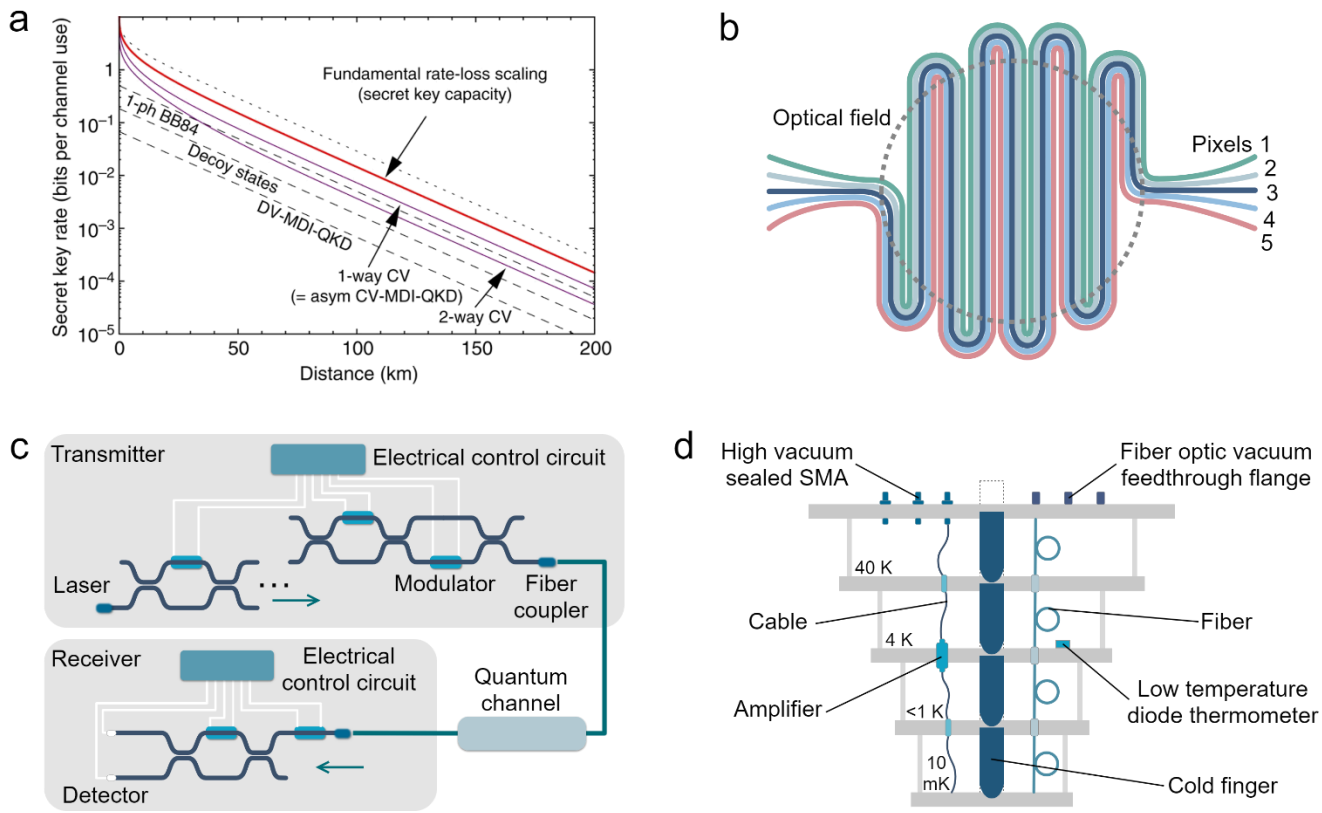

Figure 2 Fundamental limitations of quantum key distribution (QKD) schemes. (a) Simulation of ideal performances for different QKD schemes[54]. Reproduced with permission from REF. 54. (b) Schematic of SNSPD chip with multiple interleaved pixels. (c) Schematic of on-chip QKD systems. (d) Schematic of multi-stage cryogenic cooling system.

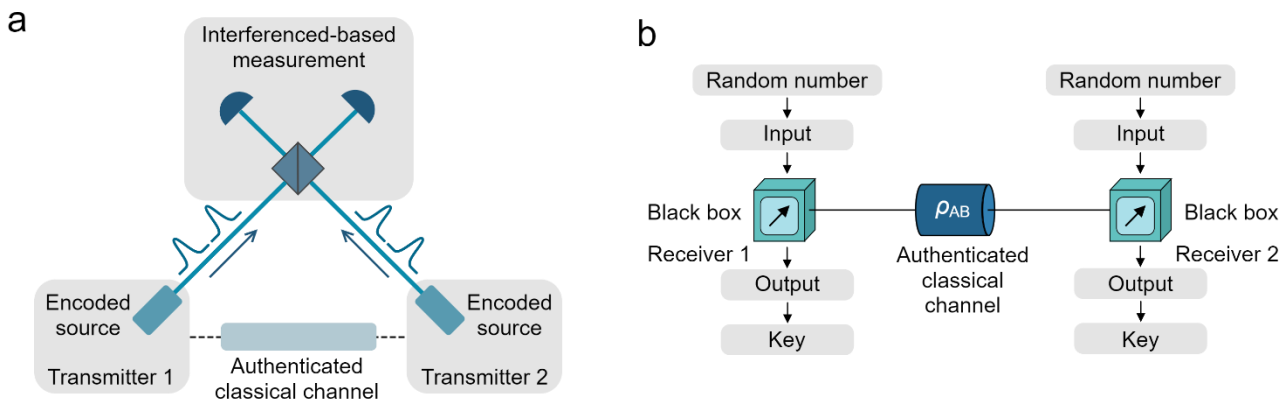

Figure 3 Advanced technologies in quantum key distribution (QKD) developed to address practical challenges. (a) Schematic of an interference-based QKD system. (b) Schematic of device-independent QKD protocol.

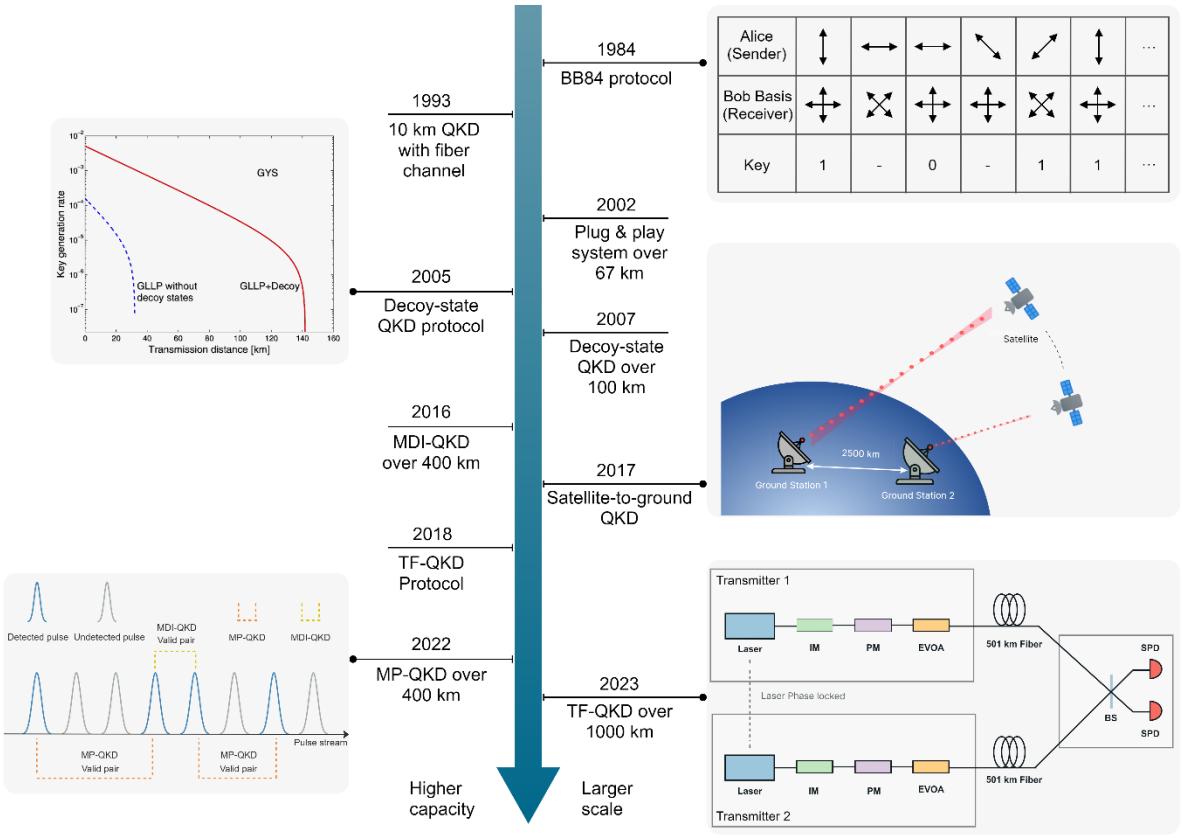

Figure 4 Timeline of Long-haul quantum key distribution (QKD) developments. 1984, Bannett-Brassard 1984 (BB84) protocol[11]; 1993, 10 km QKD with fiber channel[108]; 2002, plug-and-play system over 67 km[109]; 2005, decoy-state QKD protocol[25]; 2007, decoy-state QKD over 100 km[110]; 2016, measurement-device-independent (MDI)-QKD over 400 km[112]; 2017, satellite-to-ground QKD[48]; 2018, twin-field (TF)-QKD protocol[56]; 2022, mode-paring (MP)-QKD protocol[116]; and 2023, TF-QKD over 1000 km[118].

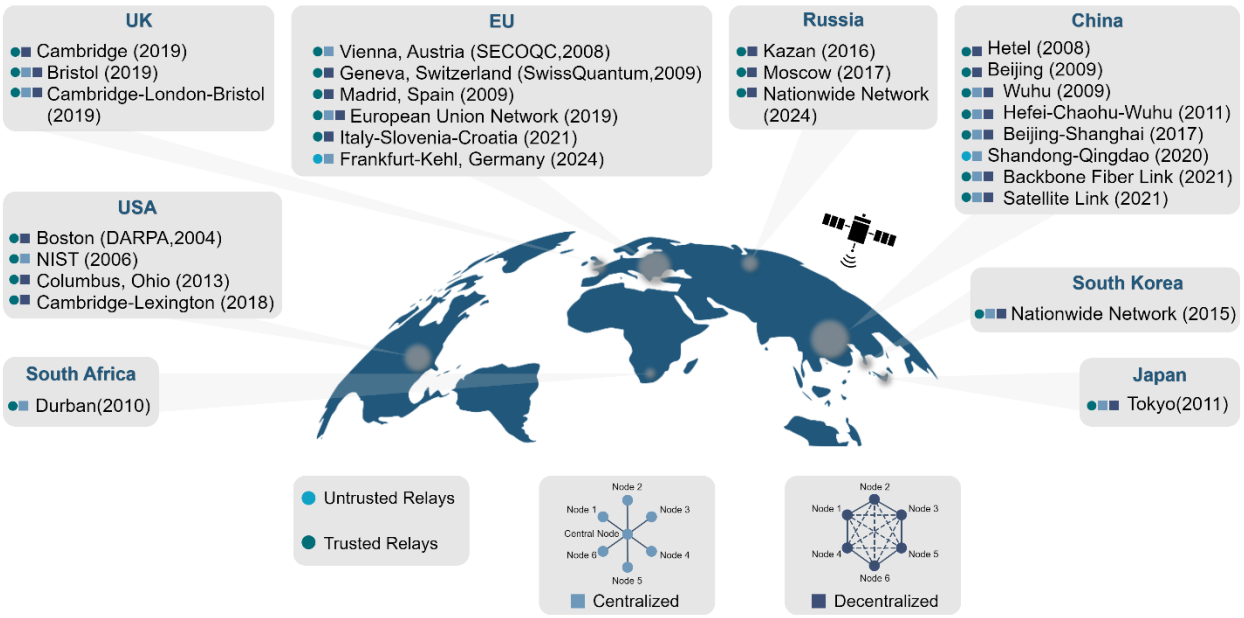

Figure 5 Main existing quantum key distribution (QKD) networks worldwide. Representative QKD networks have been deployed worldwide, including national and metropolitan implementations in Europe[9,138,166], the USA[72], China[143,148,167], Japan[168] and Others[79]. The architectures of existing QKD networks may vary in design, but they are generally classified according to two main distinctions: trusted versus untrusted relays, and centralized versus decentralized topologies.

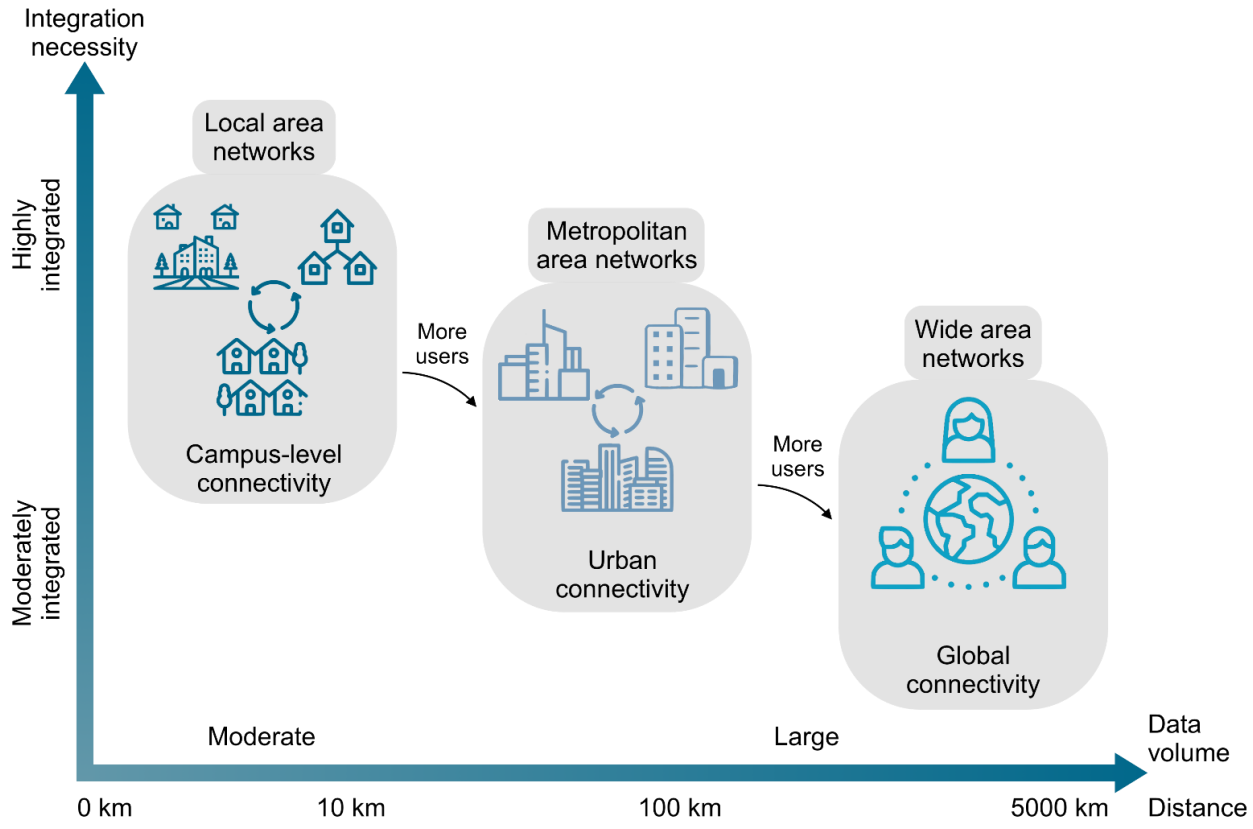

Figure 6 An envisioned layout for a global QKD network. Range definitions of local area networks (LAN), metropolitan area networks (MAN), and wide area networks (WAN) are approximated from classical networking. LANs generally require a higher level of user system integration to meet user demands, while the integration requirements decrease for MANs and WANs.

TOC: Information security remains a vital concern for communications technology, and Quantum Key Distribution (QKD) may offer the highest security theoretically possible. This Review discusses the performance limitations, high costs, and practical security concerns for QKD to scale to a global level.