Received: 21 December 2023 | Revised: 21 February 2024 | Accepted: 23 March 2024

IET Quantum Communication

DOI: 10.1049/qtc2.12094

REVIEW

Advances in artificial intelligence and machine learning for quantum communication applications

Mhlambululi Mafu

Department of Physics, Case Western Reserve University, Cleveland, Ohio, USA

Correspondence
Mhlambululi Mafu.
Email: mxm1625@case.edu

Abstract

Artificial intelligence (AI) and classical machine learning (ML) techniques have revolutionised numerous fields, including quantum communication. Quantum communication technologies rely heavily on quantum resources, which can be challenging to produce, control, and maintain effectively to ensure optimum performance. ML has recently been applied to quantum communication and networks to mitigate noise-induced errors and analyse quantum protocols. The authors systematically review state-of-the-art ML applications to advance theoretical and experimental central quantum communication protocols, specifically quantum key distribution, quantum teleportation, quantum secret sharing, and quantum networks. Specifically, the authors survey the progress on how ML and, more broadly, AI techniques have been applied to optimise various components of a quantum communication system. This has resulted in ultra-secure quantum communication protocols with optimised key generation rates as well as efficient and robust quantum networks. Integrating AI and ML techniques opens intriguing prospects for securing and facilitating efficient and reliable large-scale communication between multiple parties. Most significantly, large-scale communication networks have the potential to gradually develop the maturity of a future quantum internet.

KEYWORDS

learning (artificial intelligence), quantum communication, quantum cryptography, quantum information

1 | INTRODUCTION

Quantum communication is the art of transferring a quantum state from one place to another [1, 2]. Quantum states encode quantum information and allow one to perform tasks that afford secure and efficient communication surpassing the capabilities of classical information [3, 4]. Quantum communication harnesses the distinct characteristics of quantum mechanics, such as the phenomenon of quantum entanglement [5], when two objects can be instantaneously connected; superposition [6], a case in which a single object can be in two places at once; the uncertainty principle [7], which states that there is inherent uncertainty in measuring a variable of a particle, and the quantum no-cloning theorem [8], which prevents perfect copying of an arbitrary unknown quantum state to enable the secure and efficient transmission of information [3, 9]. Owing to these properties, any attempt by an eavesdropper to access information encoded in quantum states can be detected before confidential information is exchanged between the legitimate parties. Classical communication relies on bits to encode and transmit data, and its security is guaranteed by the computational hardness of specific mathematical problems, such as factorisation of large integers [10, 11]. The advances in quantum computing pose a significant threat to classical algorithms based on symmetric and asymmetric cryptography, which are only computationally secure [12]. To break public-key cryptography, one needs the ability to solve problems that are believed to be hard for classical and quantum computers. For instance, Shor's algorithm, a quantum computing algorithm can efficiently factor large numbers, breaking the security of the Rivest-Shamir-Adleman (RSA) encryption algorithm [13]. The RSA algorithm is widely used for secure data

transmission and digital signatures, and its susceptibility to Shor's algorithm potentially presents a critical challenge to cybersecurity.

Quantum communication promises information-theoretic or unconditional security because it relies on the laws of physics rather than the presumed computational hardness of certain problems [3, 9]. The secure exchange of sensitive information could be transmitted via a quantum network, such as quantum photonic chips [14, 15], optical fibre, or free-space channels [16, 17]. One of the main goals of quantum communication is connecting quantum computers to build a quantum network [18]. This could increase the total computing power, especially if only processors with a few qubits are available at each network node [19] and will enable the realisation of the envisaged quantum internet [20–22]. Nevertheless, the limitations faced by quantum information carriers, such as losses at large distances or quantum decoherence, a quantum network will also contain other elements, such as a quantum repeater or quantum switch to enable the transmission of quantum information over long distances without degradation [21, 23]. Most significantly, the primary paradigms of quantum communication are quantum key distribution (QKD) [16], quantum teleportation [24], quantum secret sharing (QSS) [25] and quantum networks [20]. Notably, quantum communication technologies such as QKD for point-to-point connection at short distances or by using trusted repeaters at large distances have gone beyond prototypes and begun being commercialised [26–28]. Furthermore, the International Organization for Standardisation has developed standards governing the security requirements, test, and evaluation methods for QKD [29, 30]. This versatility of quantum communication demonstrates its immense potential for transforming the modern world, ranging from enhancing security to revolutionising long-distance communication to paving the way for a quantum internet [21]. The quantum internet is expected to profoundly impact various technological frontiers and everyday life through providing quantum secure cloud-based services [22, 31, 32]. Clearly, in addition to its technological significance, quantum communication protocols and networks are expected to have far-reaching social, economic, political, and geostrategic implications [33, 34].

Meanwhile, advances in artificial intelligence (AI) and machine learning (ML) have revolutionised science and society [35]. Precisely, AI and ML enable machines to perform complex tasks autonomously, without human intervention [36, 37]. For instance, AI and ML promise unprecedented applications in data processing problems such as data prediction, data sorting, pattern recognition, and classification [36, 38–41]. These technologies have already begun transforming various sectors such as banking and finance [42, 43], business [44, 45], consumer [46, 47], education [48–51] and defence [52, 53]. Furthermore, AI and ML applications have become essential in communication, resulting in improved, efficient, and secure systems [54–60]. A suitable example is Rivest's 1991 discussion on the relationship between cryptography and ML, highlighting how both fields have developed ideas and techniques from each other resulting in improved security systems [61]. Recently, ML and more broadly, AI techniques have been successfully applied to various aspects of quantum communications, such as identifying fundamental quantum protocols [55], including quantum teleportation [62, 63], entanglement purification [64–67], quantum repeaters [68, 69] and estimating parameters of quantum devices [70–72]. AI and ML techniques have demonstrated outstanding performance in addressing noise, channel losses, and quantum state detection [55, 57]. Since quantum communication is highly susceptible to errors due to noise and decoherence caused by environmental factors and hardware imperfections [4, 73], AI and ML promises to significantly contribute to addressing classical and quantum error correction [74–78]. Specifically, ML algorithms allow the optimisation of quantum systems and possibilities to identify and correct errors more effectively [79–81]. This will improve the reliability and accuracy of quantum communication systems [42, 75, 82–85].

The field of AI and ML dates back to the 1950s when Alan Turing proposed developing intelligent machines and testing their intelligence [86] and at the Dartmouth Summer Research Project on Artificial Intelligence, a summer workshop widely credited as the founding event of AI as a field [87, 88]. On the other hand, quantum communication has existed since the 1980s when Bennett and Brassard proposed a quantum physics-based solution to the key distribution problem [9, 16]. While these fields have long existed, the application, development of AI and ML, and impact on quantum communication technologies are still relatively low, though it is proliferating [82, 89]. Consequently, we present a concise overview of recent developments regarding the main paradigms of quantum communication, including quantum networks, as well as a brief discussion of some of the main challenges. Specifically, we discuss how AI and ML algorithms have been integrated into various components of quantum communication systems in order to overcome implementation challenges. We advise the reader that due to the subjective nature of the selection process and the pace at which AI and ML applications and developments progress, some contributions will inevitably be missed. We do not conduct an extensive review of various quantum communication protocols. However, we provide a comprehensive list of literature on significant contributions to the field, covering the more detailed issues that we can only briefly cover in a review. After discussing the examples in our article, we hope the reader will appreciate and understand the significance of AI and ML techniques in quantum communication protocols and quantum networks.

2 | FUNDAMENTALS OF AI AND ML

AI refers to the development of computer systems with the capacity to solve advanced problems based on analytical models that generate predictions, rules, answers, recommendations, or similar outcomes [37, 90–92]. These systems are designed to analyse data, recognise patterns, and make decisions or predictions based on the information they gather [93, 94]. ML is a subset of AI that focuses on developing algorithms and models that enable computers to learn from and

make predictions or decisions without being explicitly programmed [94, 95]. The algorithms also adapt in response to new data and experiences to improve their efficacy over time [96]. With the capacity of systems to process vast amounts of data and make intelligent decisions, AI and ML have opened up new unprecedented possibilities and opportunities in various fields [97, 98], including physical sciences [40, 99, 100] and more specifically, quantum communications. The ML algorithms can be grouped into supervised and unsupervised learning [101]. The adjectives 'supervised or unsupervised' indicate whether there are labelled samples in the database [93, 96]. Moreover, reinforcement learning has emerged as a new ML category inspired by behavioural psychology and neuroscience [102]. Reinforcement learning concerns an agent's specific form of reward or utility connected to its environment via perception and action [103]. A subset of ML called deep learning (DL), allows a computational model composed of multiple layers of processing units to learn multiple levels of abstraction in given data [93, 104]. Most significantly, DL is excellent at discovering intricate structures in high-dimensional data and is therefore applicable to many domains of science [105] and business [106]. The relationship among the AI, ML, and DL techniques is shown in Figure 1.

The family of AI and ML algorithms can be categorised based on their similarity in functionality and structure. This has given rise to regression algorithms [107], instance-based algorithms [108], regularisation algorithms [109], decision tree (DT) algorithms [110], Bayesian algorithms [111], clustering algorithms [112, 113], artificial neural networks (ANNs) [114, 115], DL algorithms [98], long short-term memory (LSTM) algorithms [116], dimension reduction algorithms [117], and ensemble algorithms [118]. We discuss how the synergistic integration of these AI and ML techniques has enhanced quantum communication system capabilities, resulting in more secure, reliable, and efficient quantum information transmission.

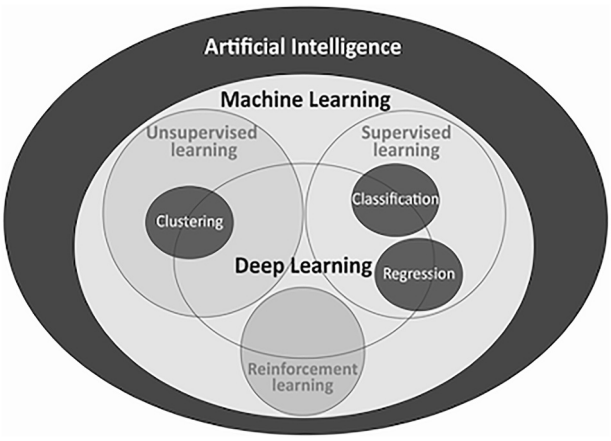

FIGURE 1 An overview of the relationship between AI, ML, and DL. A classification algorithm and a regression algorithm are examples of supervised learning, while a clustering algorithm is an example of unsupervised learning. Notably, DL is a subset of ML in which multilayered neural networks learn from data and examples include convolutional neural networks and recurrent neural networks. AI, artificial intelligence; DL, deep learning; ML, machine learning.

3 | APPLICATIONS OF AI AND ML TO QUANTUM COMMUNICATION

On the one hand, AI and ML have become ubiquitous and effective techniques for data processing and classification, and on the other hand, the ability to manipulate and control quantum states has resulted in a wide range of applications that enable the secure and efficient transmission of information through quantum systems. The increasing complexity of quantum systems and communication technologies necessitates powerful data processing and analysis tools [119]. One of the most important developments is integrating or co-existing quantum signal channels into classical telecommunication networks. While significant progress has been reported, various implementation challenges remain [120]. Most significantly, AI and ML have proven valuable tools for addressing these challenges in recent years. The reason for this is that AI and ML techniques thrive at learning highly complex input–output mappings, which enables optimisation of systems [121, 122], developing signalling and detection schemes for complex channels or channels without analytical or numerical models [123], and detecting ultra-sensitive signals [124, 125]. Due to the unprecedented progress in these fields, in the following subsections, we examine how AI and ML techniques have been applied to solve various theoretical and practical challenges in QKD, quantum teleportation, QSS, and quantum networks. To provide context, we offer a concise overview of the various quantum communication paradigms. This is followed by examining the current challenges and briefly discussing how recent advances in AI and ML have been used to address them, thus enhancing quantum communication applications.

3.1 | Quantum key distribution

QKD-the establishment of information-theoretically secure random key, which guarantees a level of security that is independent of any computational assumptions based on quantum mechanics [3, 11, 16, 126]. The information about a secure key is transmitted using qubits. The symmetric cryptographic systems such as the one-time pad utilise the securely generated secret keys for encryption and decryption of messages to ensure confidentiality and prevent eavesdropping [9, 127, 128]. The secret key enables secure communication and authentication between spatially separated legitimate parties, known as Alice and Bob. QKD protocols require a quantum channel, through which qubits containing information about the distributed key are exchanged, and a public channel, which is used to check whether communication through the quantum channel is distorted. An illustration of a general QKD protocol where Alice and Bob share an insecure quantum channel and an authenticated classical channel wishes to share a secret secure key in the presence of an adversarial eavesdropper, Eve is shown in Figure 2. While Eve can intercept a quantum channel and extract information by measuring the transmitted quantum states, she is prevented from doing so by the laws of quantum mechanics, since any measurement, in general,

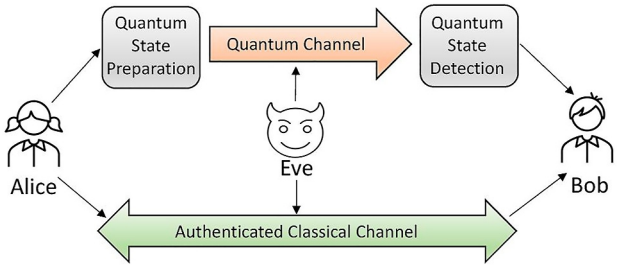

FIGURE 2 The schematic setting of a typical QKD protocol. The two legitimate parties, Alice and Bob are connected by a quantum channel, which an eavesdropper, Eve can tap without any restriction other than by quantum mechanics. In the authenticated public classical channel, Eve can only listen to the conversation but cannot modify the messages being sent between Alice and Bob. A shared secure random key that meets the desired properties is produced at the end of the protocol, or the protocol aborts. Reproduced from Ref. [129]. QKD, quantum key distribution.

modifies the state of the measured system [130]. Additionally, Eve is forbidden by the quantum non-cloning theorem [8] to make a perfect copy of the state Alice sends to Bob while keeping the original copy. Any action by the eavesdropper would lead to her detection and Alice and Bob can abort the protocol and discard the keys. The classical channel is authenticated such that the eavesdropper can only listen to communication about the basis Alice and Bob used to measure the quantum states but not the actual measurement results. Therefore, Eve cannot recover information about generated secret keys. As a result, combining a QKD protocol with a secure one-time pad encryption algorithm promises information-theoretic or unconditional security [11, 131].

Since Bennett and Brassard's (BB84) [16] and Ekert 1991 (E91) [126] now represent protocols using QKD, various QKD protocols and schemes have been developed to overcome the mismatch between the theoretical security of the communication model and the security of practical implementations [132–134]. These protocols belong to a class of discrete-variable (DV-QKD) protocols because the information is encoded in a discrete manner by using single photons to carry information, exploiting, for instance, different polarisation directions to realise the two states of a qubit [3, 9]. Another approach to QKD is the continuous-variable (CV-QKD), in which information is encoded in the properties of light that are continuous, for instance, the quadrature components of the electromagnetic field, yielding continuous values as measurement results [135] and the distributed-phase-reference protocols in which information is encoded in time and phase of weak coherent pulses [3, 17]. Owing to the demand for various practical implementation requirements has led to developments such as decoy-state QKD [136], device-independent QKD or measurement-device independent QKD (MDI-QKD) [137] as well as Twin-Field QKD (TF-QKD) [138] protocols. Detailed descriptions of these approaches, including proofs of their security, may be found in Refs. [3, 9, 17, 139]. As a result of these developments, there can be no doubt that QKD has emerged to be the most advanced practical quantum communication technology [129].

QKD has two significant characteristics: practical security and key-rate performance [140, 141]. These characteristics enable or limit QKD use in real-life applications [17, 132, 133, 142]. The key rates of DV-QKD protocols are evaluated using analytical methods since most of them are symmetric [9, 143–147]. However, symmetry assumptions usually fail for other classes of protocols because of the differences in encoding. This leads to new challenges in analysing the security of such protocols. As a result, numerical methods based on convex optimisations have been developed [148–151]. Typically, a QKD system consists of three components: a source, a channel, and a measurement device [3]. The source is relatively simple and can be well characterised [152, 153]. The security of the channel has been addressed in various QKD security proofs [145, 154]. Nevertheless, quantum information transmission over long distances is still a long way from becoming a reality, possibly until functional quantum repeaters are realised [155]. Quantum repeaters require quantum memories with memory times close to a second [156]. As a result, the certification of the physical hardware remains a critical challenge for quantum communication. While multi-hop quantum networks are capable of providing better rates at longer distances, they have limited achievable key rates [157].

Compared to DV-QKD, the class of CV-QKD protocols have gained interest because of their potential technology advantage such as offering an improved secret key rate and being much more compatible with the existing standard optical fibre communication system [17, 146, 158, 159]. The CV-QKD schemes depend heavily on coherent detection and digital signal processing techniques, which are closely related to classical coherent communication systems. Despite the significant differences between classical and quantum optical communication systems, the knowledge gained through classical coherent communication systems over the past few years can be applied to quantum optical communication systems, making CV-QKD implementations possible. However, due to imperfect devices and insufficient assumptions, a practical CV-QKD system may still be vulnerable to various quantum hacking attacks [160]. Most significantly, these challenges limit practical QKD security.

Considering the difficulty of calibrating the measurement device [161], an adversary could manipulate the measurement device by sending unexpected signals [162–164]. The MDI-QKD schemes have been developed to address detection loopholes in QKD systems [165], and TF-QKD protocols have been proposed for long-distance communication with QKD keys [166]. Although improved security can be achieved by selecting optimal QKD resources, this requires time-consuming algorithms, such as exhaustive traversal or local searches [167–169]. Theoretically, as aforementioned, CV-QKD protocols lack symmetry, and security proofs involving discrete modulation rely mainly on numerical methods [150, 170]. Although numerical methods offer tight security bounds for various QKD protocols [149], their high implementation requirements remain a challenge [170–172] as they require large amounts of computational resources and time. Furthermore, numerical methods require minimising a convex function over

all eavesdropping attacks related to the experimental data [173] and depend on numerous QKD parameters. Unfortunately, this may require a significant amount of time for the corresponding optimisation [150, 170]. Due to these challenges, it is imperative to develop techniques that are more useful than standard numerical modelling methods.

ML and AI techniques provide powerful tools for learning from unknown features or complex patterns [94]. They demonstrate significant potential in predicting optimisation parameters from noisy measurement data and address challenges in practical quantum communications [174]. Particularly, AI and ML models have been developed for optimising various system parameters, such as equipment parameters or measurement device parameters [175], physical parameters of signals [176], and optimising the raw secret key [177]. Fundamentally, the integration of AI and ML in quantum communication systems addresses both QKD characteristics (e.g. key rate performance and practical security) as well as system components (e.g. source, channel, and measurement devices). This has resulted in improved QKD schemes and long-distance transmissions. Parameter optimisation refers to the choice of intensities (i.e. signal states and decoy states) and probabilities of sending them, which is an essential step in attaining optimal performance [178], especially when one realistically considers statistical fluctuations due to finite-size key in practical communications [179, 180]. Most often, exhaustive search or local search is used to optimise parameters in point-to-point QKD systems. Although these methods are feasible for small-scale QKD networks in the future, they are not yet suitable for large-scale networks. Accordingly, in the following section, we examine how various AI and ML models have been integrated to enhance QKD performance.

In 2020, Ding et al. [181] used random forest (RF) instead of traditional search algorithms to directly predict optimal parameters based on any given system conditions for finite data for MDI-QKD and MDI-BB84 QKD protocols. An RF model is particularly useful for various ML tasks such as classification and regression. This is due to its high prediction accuracy, tolerance to outliers and noise, and low overfitting probability [93]. This method waives the simulation and iteration methods, which are inherent in traditional search techniques. The results of the RF model are shown in Figure 3.

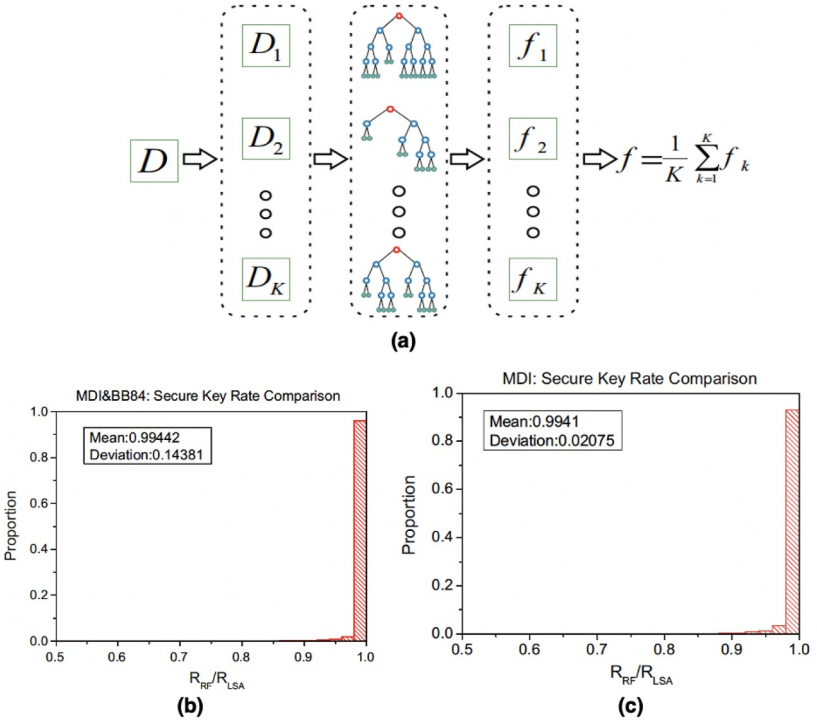

FIGURE 3 (a) An illustration of the RF model, where D denotes the original training set, $D_k (k = 1, \ldots, K)$ denotes the subset sampled with replacement from D, and f_k denotes a decision tree grown on D_k. (b) Comparison of secure key rate between RF and LSA for MDI QKD protocol. The average ratio is 0.9941 and the standard deviation is 0.0207. (c) Comparison of secure key rate between RF and LSA for MDI-BB84 QKD protocol. The average ratio is 0.9944 and the standard deviation is 0.1438. (d) Typical search space of input features: e, d, N and L for fibre loss $\alpha = 0.2$ dB/km, detector efficiency $\eta_d = 14.5\%$, and error correction efficiency $f_e = 1.16$. (e) Comparison of prediction accuracy when using the RF and NN model and a better generalisation is achieved in each situation. Reproduced from Ref. [181]. LSA, local search algorithm; MDI QKD, measurement-device independent quantum key distribution; NN, neural network; RF, random forest.

Table 1 Typical search space of input features

Parameter	e_d	d	N	L
Scope	$0.01 \sim 0.02$	$10^{-8} \sim 10^{-6}$	$10^{11} \sim 10^{13}$	$0 \sim 200$ km

(d)

Table 2 Prediction accuracy: $1 - |\vec{v}_{\text{pred}} - \vec{v}_{\text{opt}}|/\vec{v}_{\text{opt}}$

Parameter	μ	ν	P_μ	P_ν	$P_{X\|\mu}$	$P_{X\|\nu}$
RF	0.9984	0.9983	0.9954	0.9958	0.9918	0.9992
NN	0.9048	0.8869	0.9878	0.9712	0.9469	0.9828

(e)

Specifically, the RF model assumes the training set $D = \{X_i, Y_i\}_{i=1}^{n}$, where X_i are input features with responses Y_i. As part of the RF model, bootstrap aggregating or bagging is applied repeatedly (i.e. K times) to randomly n examples, with their replacement from the training set with an independent bootstrap sample, D_k. Trees are grown based on D_k, with each node selecting a random subset of features and the best split being determined from those features. After training, the predictors for a fresh sample X' can be obtained by averaging the predictions from all tress $f = \frac{1}{K}\sum_{k=1}^{K} f_k(X')$, where $f_k(X')$ is the prediction on X' of an individual tree. For the 3-intensity MDI-QKD protocol, Alice (Bob) should optimise the intensities of signal state and decoy state (μ, v), and the probability of intensities and bases (P_μ, P_v, $P_{X|\mu}$, $P_{X|v}$), where $P_\mu(P_{X|v})$ is the probability to choose signal (decoy) state and $P_{X|\mu}(P_{X|v})$ denotes the probability to choose the X basis conditional on signal (decoy) state. These parameters are grouped as vectors $\vec{v}$, which represent responses. Note that the key rate is influenced by the system's conditions $\vec{s}$, including the misalignment e_d, the dark count rate d, the detector efficiency η_d, the pulse number N, and the transmission distance L between Alice and Bob. The key rate is calculated using the equation $r = R\left(\vec{s}, \vec{v}\right)$. Optimal secure key rate is achieved by searching $\vec{v}_{opt}$ according to $\vec{v}_{opt}(s) = \text{argmax}_{\vec{v}\in V} R\left(\vec{s}, \vec{v}\right)$, where V is the search space of $\vec{v}$. Since $\vec{v}_{opt}$ is a function of the given system condition $\vec{s}$ it is challenging to simulate analytically. Particularly, using the RF model results in reduced time and hardware overhead compared to traditional search methods. Moreover, this model achieves a high prediction accuracy of over 99% of the optimal secure key rate. This holds significant promise for future QKD applications.

In MDI-QKD protocols, selecting parameters, such as the probability of selecting an X-basis or Z-basis, the signal state intensity and decoy state, as well as system calibration, becomes more challenging as the number of parties in the network increases. The most common method for optimising parameters at the moment is to use optimisation algorithms. Even though the method is accurate, it is time-consuming and consumes hardware resources. Rather than searching for optimised parameters, Lu et al. [182] present a novel back propagation neural network (BPNN) capable of predicting optimised parameters with fewer resources and at a higher speed. Moreover, it is notable that the BPNN addresses the challenge of system recalibration, which is experienced when working with large-scale MDI-QKD networks. The BPNN can be used to address system recalibration in real-time. This is achieved by requiring the use of some discarded data generated by the communication process rather than the addition of additional devices or a complete scan of the system.

On the other hand, Dong et al. [174] use the extreme gradient boosting (XGBoost), BPNN, and RF model to predict the TF-QKD optimisation parameters affecting the key rate and transmission distance. While a TF-QKD, overcomes the basic limits of QKD without repeaters, in practice, it still needs to optimise all parameters when a finite data size is considered. Using these ML models, predictive parameters significantly reduce optimisation time while maintaining high accuracy. Notably, XGBoost's performance is better than BPNN and RF in parameter prediction. This approach eliminates the need for simulation and iterations in the search method which requires real-time optimisation of the future QKD network.

Practical QKD implementations require efficient, real-time feedback control to maintain stability if there are disturbances from either the external environment or imperfect components within the system. The 'scanning-and-transmitting' programme is used to compensate for physical parameter variations of the devices, which can provide accurate compensation, but may require a considerable amount of time to stop and calibrate the processes, which may reduce the efficiency of key transmission. As a result, Liu et al. [183] proposed a practical phase-modulation in QKD that employs an ML model, specifically the LSTM network to predict physical parameters of devices in advance and actively perform real-time control on corresponding QKD devices. Figure 4 shows the schematic setup and results of the experimental study. This experiment runs the BB84 QKD system by applying either the traditional 'scanning-and-transmitting' programme or the proposed LSTM model. During transmission, the 3-intensity (μ = 0.5, v = 0.1, 0) decoy-state method is implemented and the corresponding quantum bit error rate (QBER) and counting rates for 2 days are recorded. The results are shown in Figure 4a–c. Notably, the 'duty ratio' of the traditional 'scanning-and-transmitting' programme and the proposed LSTM model-based system is 50% and 83%, respectively. As a demonstration that the proposed LSTM has the ability to predict continuously over an extended period, the proposed LSTM model-based QKD system was run for 10 days at a distance of 50 km, and the results are shown in Figure 4d. Specifically, the results demonstrate no trend of deterioration from start to finish, demonstrating the long-term reliability and stability of the proposed ML model. According to these authors, this ML model is a promising candidate for large-scale quantum communication networks.

The implementation and performance of CV-QKD are threatened by various attack strategies. To counter these attacks, various real-time monitoring modules are exploited to prevent different types of attacks. Due to the uncertainty associated with the estimation of excess noise, this strategy lacks a universal defence method, which prompted Mao et al. [184] to propose a defence strategy to address these disadvantages and resist the majority of known attacks on CV-QKD systems. By analysing several pulse characteristics that are affected by a variety of types of attacks, the authors deduce a feature vector that is used as input to an ANN model for analysis. As a result of the trained ANN model, attacks can be automatically identified and classified with a precision and recall rate exceeding 99%. By implementing most of the known attack strategies, the proposed scheme significantly increases system security. However, compared to a CV-QKD system that did not adopt any countermeasures against attacks, the proposed scheme slightly decreased the transmission distance and secret key rate.

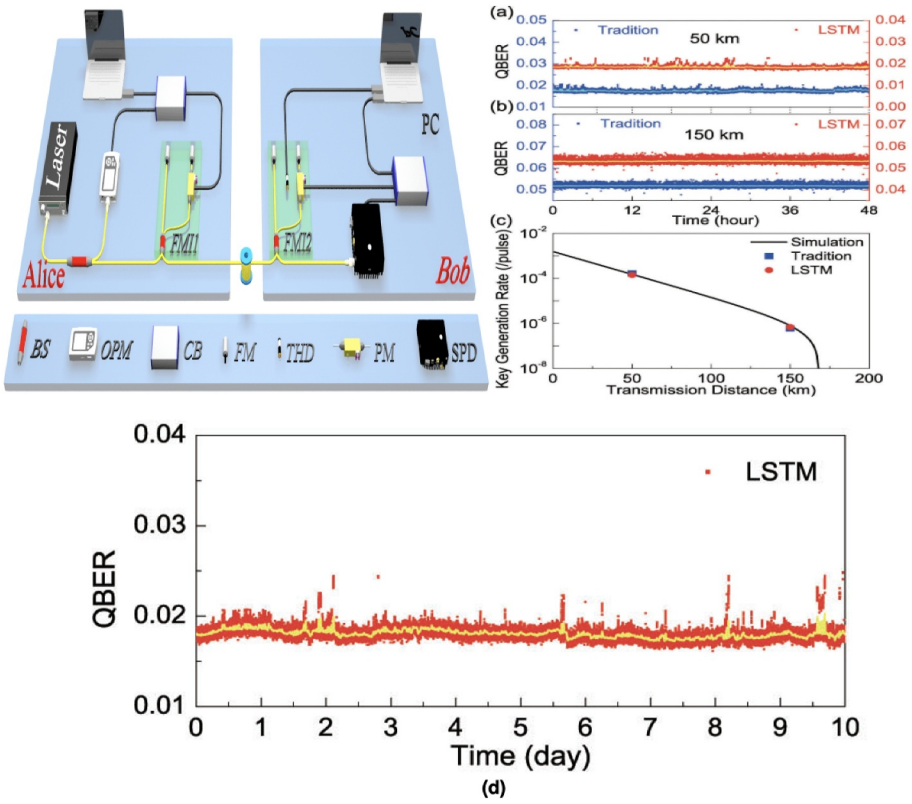

FIGURE 4 Schematic of the experimental setup. BS, beam splitter; CB, control board; FM, Faraday mirror; FMI, Faraday-Michelson Interferometer; OPM, optical power metreer; PM, phase modulator; SPD, single-photon detector; THD, temperature, and humidity detector. (a, b) Comparisons between applying the traditional 'scanning-and-transmitting' programme and using present LSTM model-based QKD systems with respect to time and average values at the transmission distance of 50 and 150 km. Notably, the QBER of the traditional method is linked to the left *Y*-axis, and of LSTM model is linked to the right *Y*-axis. (c) The key generation rate versus transmission distance. In each figure, the square points refer to the results of applying the traditional 'scanning-and-transmitting' programme, and the circle points correspond to using our new method. (d) Comparisons between applying traditional scanning-and-transmitting programme and using current LSTM-model-based QKD systems on QBER at the transmission distance of 100 km. Reproduced from Ref. [183]. LSTM, long short-term memory; QBER, quantum bit error rate; QKD, quantum key distribution.

Another important approach to QKD practical systems is underwater CV-QKD. However, the implementation of underwater QKD faces challenges such as such as equipment imperfections, channel disturbances, and eavesdroppers, which may cause invalid communication. As a result, Li et al. [56] investigate the risk ensemble learning (EL) approach caused by channel disturbance resulting in communication failure. To improve the security of the CV-QKD system with discrete modulation, the authors present an EL approach with a self-adaptive structure and predictability of communication failures. Based on the EL approach, the current communication status of the discrete-modulated CV-QKD (DM-CV-QKD) system can be predicted based on Bob's phase data, enabling adaptive judgement of the current communication status, and ensuring typical QKD communications. As opposed to the traditional ML process used for CV-QKD systems, this method does not require additional parameter detection equipment. This means the scheme is not susceptible to security vulnerabilities caused by parameter detection equipment. Moreover, the EL approach can reach 70%, which is higher than other learners, especially in logistic regression, support vector machines, and BPNNs. As a result, this ability to predict communication failures contributes to improved practical implementation feasibility of CV-QKD. Due to the vulnerability of CV-QKD systems to various quantum hacking attacks, Ding et al. proposed an ML-based attack detection scheme (MADS) as a universal defence strategy [160]. According to the results, the MADS can detect most quantum hacking attacks and revise overestimated secret key rates resulting from a CV-QKD system that does not employ a defence strategy to achieve a tighter security bound.

Towards addressing measurement device or detection challenges, using an ML-assisted MDI-QKD system, Zhang et al. [185] demonstrate how phase drift between two users can be predicted in advance and compensated actively in real-time, dramatically increasing key transmission efficiency. Specifically, they demonstrate the application of the LSTM model to the MDI-QKD system for calibrations of reference frames. This schematic setup and results are shown in Figure 5. By utilising this model, the QKD system can predict phase drift between two users in advance, and compensate for it in real-time. The MDI-QKD scheme generally achieves lower secret key rates than the BB84 QKD scheme, while achieving a balance and practicality with finite data size effects. As a means of

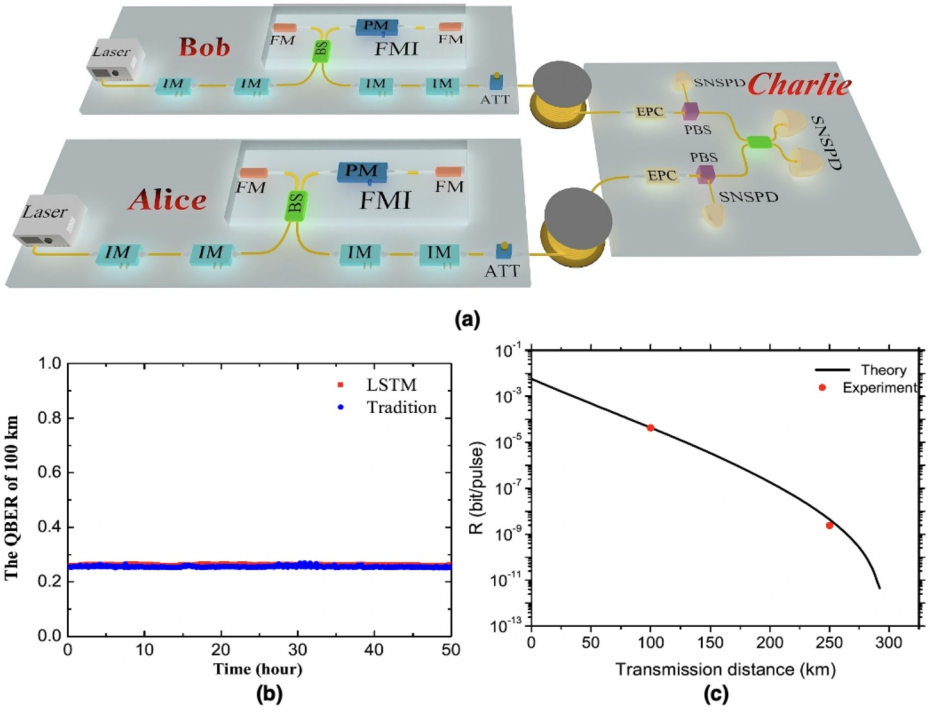

Table 1. Optimized parameters of sources with 100 km and 250 km fibers.

Parameters	μ	v	ω	P_μ	P_v	$P_{X\|\mu}$
100 km	0.6353	0.0476	0.3171	0.885	0.110	0.002
250 km	0.4492	0.0691	0.4817	0.495	0.436	0.027

Table 2. Crucial values in the key rate formula: estimated single photon yield ($Y_{11}^{Z,L}$) and phase error rate ($e_{11}^{X,U}$); measured values of QBER ($E_{\mu\mu}^{ZZ}$, $E_{\mu\mu}^{XX}$) and gain ($Q_{\mu\mu}^{ZZ}$, $Q_{\mu\mu}^{XX}$) when Alice and Bob both prepare the signal state in Z basis, X basis.

Distance	$Y_{11}^{Z,L}$	$e_{11}^{X,U}$	$Q_{\mu\mu}^{ZZ}$	$E_{\mu\mu}^{ZZ}$	$Q_{\mu\mu}^{XX}$	$E_{\mu\mu}^{XX}$
100 km	0.0015	0.1539	4.57×10^{-4}	0.002	9.16×10^{-4}	0.257
250 km	3.0182×10^{-6}	0.3118	5.597×10^{-7}	0.00236	1.085×10^{-6}	0.267

FIGURE 5 (a) Schematic setup of the MDI-QKD system. ATT, attenuator; BS, beam splitter; EPC, electronic polarization polarisation controller; FM, Faraday mirror; IM, intensity modulator; Laser, continuous-wave laser; PM, phase modulator; SNSPD, super-conducting nanowire single-photon detector. (b) Theoretical and experimental results of the key rate's dependence on the transmission distance. The system parameters are as follows: dark counting rate per pulse and overall efficiency of detection side are 4×10^{-8} and 60%; misalignment errors in Z and X bases are 0.15% and 1.5%, respectively. (c) Comparisons between applying traditional scanning-and-transmitting programme and using current LSTM-model-based QKD systems on QBER at the transmission distance of 100 km. Reproduced from Ref. [185]. LSTM, long short-term memory; MDI-QKD, measurement-device independent QKD; QBER, quantum bit error rate; QKD, quantum key distribution.

increasing the key rate, the authors demonstrate a variation of the LSTM model based on a simple three-intensity decoy-state MDI-QKD scheme with biased basis choice, in which the decoy pulses are only prepared in the X-basis. This protocol consists of signal pulses prepared either on a Z or X basis, which is distinct from the traditional three-intensity decoy state schemes [186]. However, similar to the approach demonstrated in Ref. [183], authorised parties randomly prepare phase-randomised weak coherent state pulses in three different intensities (μ, v, 0) with certain probability values that correspond to the intensity of the signal state, the decoy state, and the vacuum state. The experimental demonstration demonstrated improved secure key exchange for single-mode fibres over 100 and 250 km. By utilising this approach, MDI-QKD systems show a significant improvement in transmission efficiency over conventional scanning-and-transmitting systems. Furthermore, the method avoids potential vulnerabilities since no additional quantum resources are required. The programme optimisation can further improve the duty cycle and stability time to match the requirements of different systems. Furthermore, the proposed system maintains excellent stability over a long period, conclusively demonstrating its effectiveness. As a final point, this approach can serve as a valuable reference when it comes to the implementation of future large-scale quantum communications.

Notably, Ismail et al. demonstrated using the EL technique called RF to predict the strength of the atmospheric turbulence in the quantum channel in free space using the Strehl Ratio [187]. The authors estimate the Strehl ratio of the quantum channel with a mean absolute percentage error of 4.44%. The authors also perform predictions using linear and support vector regressors; however, the RF performs better. As part of the

process of characterising quantum channels, these values provide insight into the level of disturbances that must be overcome during key distribution. This allows one to accurately characterise quantum channels and assist in mitigating the challenges related to information losses in transmission channels. Hence, using ML to monitor free-space quantum channels will enable real-time monitoring of QKD systems. In 2022, Lollie et al. [188] demonstrated high-dimensional encryption in optical fibres using spatial modes of light and ANNs. A particular feature of this communication protocol is that it allows the recovery of messages and images with a high level of accuracy. This protocol provides a way to increase the quantum information capacity per photon while maintaining the fidelity of information transfer that is essential for quantum technologies utilising structured fields of light, particularly those whose propagation is challenged by free space. Moreover, in 2018, Ou et al. [189] developed a method to assist coexistence between quantum and classical communication channels. They predicted the quantum channel QKD quality in a dense wavelength-division multiplexing (DWDM) fibre network with multiple ML models. The authors demonstrate that the *K*-neighbours regression is the most accurate model to spectrally re-allocate the channels for stable performance. The feasibility of the ML application was confirmed by several field trials, which demonstrated robust key generation and distribution. Furthermore, Liu et al. [176] demonstrated the advantages of using a support vector regression model for optimising the performance and security of fibre QKD systems. This SVR-based approach provides optimal performance and practical security for the QKD system. As the system does not require additional resources and no real-time monitoring module, it supports automatic prediction of signal physical parameters over time and can be applied to any signal physical parameter that can be measured in a practical QKD system. It is noteworthy that Okey et al. [169] showed that the Tree-CNN algorithm is an efficient method for selecting the optimal QKD (i.e. BB84 for short distances and TF-QKD for long distances) for the implementation of large-scale communication systems in real-time. The proposed model is compared to other ML techniques based on convolutional neural networks (CNN). This study showed a 99.89% Area Under Curve during testing and 0.65 s time-cost performance, which outperformed the results obtained in related studies in predicting the best QKD protocol. The proposed scheme was further validated using different transmission distances and three QKD protocols to demonstrate that the predictions and actual results matched one another. The proposed model demonstrated a fast, reliable, and precise solution to the problem of selecting an appropriate QKD protocol based on performance and time. The authors suggest that long distances established using TF-QKD implementations may eliminate the need for quantum repeaters in certain instances. Particularly, other ML models have also been applied to fibre-based optical communication systems [101, 190] as well as nanoscale devices characterisation and parameter estimation, leading to improvements in quantum communication systems [125].

A NN is presented by Wang and Lo [178] in 2019 which predicts the optimal parameters based on the characteristics of devices and channels for four examples: MDI-QKD, BB84, and TF-QKD. According to the authors, the approach is general and does not depend on any particular protocol. With a fraction of the power consumption of local search, this technique is suitable for low-power devices and can achieve 2–3 orders of magnitude faster optimisation speed than local search. The programme can be run on either NN acceleration chips or on common CPUs with relatively low performance, depending on their preference. Besides this being extremely useful for free-space QKD applications that require low latency and low power budgets, it is useful for quantum internet-of-things (IoT). The IoTs allow even a small portable device connected to numerous users to optimise everything parameters in real-time. Furthermore, this simple demonstration suggests that similar methods may apply to other optimisation tasks commonly encountered in the design and control of practical QKD systems, including the determination of the optimal post-selection thresholds in free-space QKD and the tuning of polarisation controller motors to control misalignment. This could be useful for reference-free independent QKD schemes [191].

Moreover, in 2018, Li et al. [177] presented a distance-weighted *K*-nearest neighbours (DW-KNN) algorithm to a DM-CV-QKD to preprocess the raw key data before performing the reconciliation. This improves the accuracy of the raw key data and the performance of DM-CV-QKD. The proposed scheme could be employed to overcome several impairments induced by the channel, thereby lowering the demand for error correction codes on the signal-to-noise-ratio threshold of the quantum channel. Classical error correction techniques are used to detect and correct errors in the transmission of classical information [3, 9]. This technique plays a crucial role in improving the security and reliability of QKD systems. Niemiec demonstrates a key reconciliation technique that uses ANNs (TPM machines) to reconcile errors in quantum channels [78]. The authors argue that error correction using ANNs is robust to current attacks imposed by quantum computers. Furthermore, Long et al. [81] presents an overview of how ML has been applied to almost every stage of the QKD protocol, particularly CV-QKD. The study indicates that ML has been used in phase error estimation, excess noise estimation, state discrimination, parameter estimation and optimisation, key sifting, information reconciliation, and key rate estimation. To improve time and resource consumption in CV-QKD, Liu et al. [171] improve a NN model predicting key rates in nearly real-time by combining the model with Bayesian optimisation. The combined model automatically designs the best architecture of neural networks computing the key rates for DM-CV-QKD protocols in real-time. Precisely, two variants of CV-QKD protocols with quaternary modulation were studied using the model. The results indicate high reliability with a secure probability as high as 99.15%–99.59%, tight secure bounds, and high efficiency with a speed-up of approximately 10^7 than the numerical methods. A key benefit of the model is that it allows real-time automatic and efficient computation of QKD. This will address the growing demand for implementing QKD protocols on mobile platforms such as handheld QKD systems, drone-based QKD, or satellite-

ground QKD. The authors argue that using neural networks to optimal parameters in their work outperforms results in Refs [176, 178, 181, 182].

In 2020, Liao et al. [192] proposed a multi-label learning-based scheme for discretely-modulated CV-QKD (ML-CV-QKD). This scheme divides the quantum system into a trusted state learning process for training and estimating classifier, and an untrusted state prediction process for generating the final secret key. To better represent the characteristics of modulated coherent states, feature extraction was used. This study also investigates how the multi-label classification algorithm embedded in ML-CV-QKD can be used for the prediction of unknown signals. The results illustrate that the MLCA-embedded ML-CV-QKD is both feasible and effective at predicting unknown signals. The numerical simulations show that the proposed MLCA-embedded ML-CV-QKD outperforms existing CV-QKD protocols, specifically in terms of maximum transmission distance, and the performance of both transmission distance and secret key rate will continue to increase with the increase of modulation variance. Moreover, Zhou et al. [172] developed an NN that can be used to predict the information-theoretically secure key rates of homodyne detection DM-CV-QKD with high probabilities of up to 99.2% at distances of 0–100 km with <0.015 excess noise. According to the authors, their method achieves a speed that is six orders of magnitude higher than the numerical method in Ref. [149]. Since it takes a certain time for the QKD system to collect data, the predictability of the key rates by the NN meets all practical requirements. This technique can in principle be applied to any protocol with reliable numerical methods. Furthermore, there is also increasing interest in applying ML techniques to suppress noise [60, 171, 193]. For an extended discussion on enhancing various CV-QKD systems with ML, including detection methods and attack methods, we refer the reader to Refs. [78, 176, 177, 194]. These works demonstrate that by strategically combining quantum mechanics and advanced computational algorithms, various AI and ML techniques can be used to optimise key generation rates, reduce error rates, and increase the reliability and transmission distances of QKD systems. As QKD technology matures, standardisation efforts are underway to ensure its sustainability and reliability soon. Standardisation is critical to accommodate a variety of potential use cases and several plausible QKD protocols. Regarding the progress in standardisation and the practical challenges that prevent the widespread implementation of QKD in our future communication networks, we refer the reader to Refs. [29, 129]. The Table 1 provides a summary of the AI/ML solutions proposed for each QKD scheme. Moreover, it provides an overview of the main objectives or outcomes of each application.

3.2 | Quantum teleportation

Quantum teleportation remains one of the most significant protocols in quantum communication [5, 24, 195]. It enables the nonlocal transmission of an arbitrary unknown quantum state without transmitting the encoded particle itself [24, 196], despite the quantum no-cloning theorem [8]. This phenomenon is influenced by the fundamental principle of quantum entanglement and therefore cannot be simulated with classical channels [63, 197, 198]. This enables it to serve as a valuable resource for overcoming distance limitations in quantum communication and quantum networks, as well as the difficulty of establishing long-range interactions among qubits in quantum computation [199, 200]. An overview of the teleportation scheme based on the Bennett et al. [24], is illustrated in Figure 6. The quantum state teleportation scheme consists of an unknown quantum state being transmitted from the sender, Alice to the receiver, Bob. The two authorised participants are connected by a quantum channel and a classical channel. The quantum channel consists of an entangled pair shared between Alice and Bob:

$$|\psi^{-}\rangle_{23} = \frac{1}{\sqrt{2}}(|0\rangle_2|1\rangle_3 - |1\rangle_2|0\rangle_3), \tag{1}$$

where particles 2 and 3 are held by Alice and Bob, respectively. This shared entangled state is one of the four maximally entangled Bell states $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle)$ and $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle)$. Notably, Charlie provides the input particle 1 to be teleported to Bob in a general quantum state:

$$|\psi_A\rangle = \alpha|0\rangle_1 + \beta|1\rangle_1, \tag{2}$$

where the complex coefficients α and β satisfy $|\alpha|^2 + |\beta|^2 = 1$. Alice performs a Bell-state measurement (BSM) and randomly projects particles 1 and 2 each to one of the four Bell states with equal probability. Finally, Alice informs Bob of the BSM result through the classical channel, and Bob performs the corresponding Pauli or combinations of operators $\{I, X, Z, ZX\}$ on his particle according to the results to recover the unknown quantum state $|\psi_A\rangle$ of the particle of Charlie. Notably, the same scheme can serve for entanglement swapping when the qubit to be teleported is itself entangled with a fourth qubit held by another party.

Since the Bennett et al. proposal in 1993 [24], quantum teleportation has been demonstrated using various platforms and technologies, including single atoms [201, 202], BSM [203], photonic chips [14], time-bins [204, 205], atomic ensembles [206], solid-state quantum systems [207, 208], nuclear magnetic resonance [209], quantum optics [195, 196, 210–215], spins [199], photons [216], and superconducting qubits trapped ions [217, 218], which have become integral to numerous quantum computing architectures [200, 219], where it allows quantum information to be 'swapped' between different qubits. In awe of these developments, recent theoretical and practical advances in quantum teleportation focus on understanding its nonclassical nature and its potential applications. In terms of practical applications, outstanding teleportation distances of 100-km [220], 1200-km [221], and 1400-km [222] using free-space optical links as well as 100-km

TABLE 1 Summary of AI/ML applications in QKD schemes.

QKD protocol or device	AI/ML model	Main objective or outcome
MDI-QKD	BPNN	Predicted various optimised parameters using limited resources [182]
MDI-QKD	LSTM	Addressed measurement device or detection challenges and predicted in advance phases drifts between two users and compensates for it in real-time [185]
BB84 & MDI-QKD	LSTM	Predicted physical parameters in advance and actively performed real-time control of corresponding QKD devices [183]
MDI-QKD & MDI-BB84-QKD	RF	Predicted optimal parameters based on any given system conditions for finite data [181]
TF-QKD	XGBoost/BPNN/RF	Predicted the TF-QKD optimisation parameters influencing the key rate and transmission distance. Eliminated the need for simulation and iterations in the search method. Results of XGBoost outperform the BPNN and RF [174]
BB84 & TF-QKD	Tree-CNN	Accurately selected optimal QKD parameters [169]
MDI-QKD, BB84 QKD and TF-QKD	Neural network	Accurately and efficiently predicted the optimal parameters [178]
CV-QKD	LSTM	Enhanced the performance and stability of the protocol [185]
CV-QKD	BPNN	Adjusted the modulation variance to ensure an optimal system with a higher achievable key rate under varied atmospheric turbulence intensities [54]
CV-QKD	ANN	Detected quantum attacks in the communication system [184]
CV-QKD	Ensemble learning	Predicted channel failure due to disturbance in underwater communication systems [56]
CV-QKD	MADS	Detected most quantum hacking attacks and revised overestimated secret key rates [160]
CV-QKD	Support vector regression	Optimised the performance and the practical security of a fibre QKD system [176]
CV-QKD	ANN	Experimentally addressed a quantum attack defense strategy [184]
DM-CV-QKD	KNN	Improved the accuracy of the raw key data and secure distance of DM-CV-QKD systems [177]
DM-CV-QKD	Neural network + Bayesian optimisation	Computed key rates in real-time on a low power platform [171]
DM-CV-QKD	Neural network	Predicted information-theoretically secure key rates of homodyne detection DM-CV-QKD with a great probability (up to 99%) at a distance of 0–100 km and an excess noise of no more than 0.015 [172]
Quantum channel	RF	Predicted the atmospheric strength of quantum channels in free space [187]
Quantum channel	KNN regression	Predicted the quantum channel quality in a DWDM fibre network [189]
Optical fibre	ANN	Recovered messages and images with a high level of accuracy [188]
Key distillation	ANN	Corrected errors occurring during transmission [78]

Abbreviations: AI, artificial intelligence; ANN, artificial neural network; BPNN, back propagation neural network; CNN, convolutional neural network; CV-QKD, continuous-variable QKD; DM-CV-QKD, discrete-modulated CV-QKD; KNN, *K*-nearest neighbour; LSTM, long short-term memory; MADS, ML-based attack detection scheme; MDI-QKD, measurement-device independent QKD; ML, machine learning; QKD, quantum key distribution; RF, random forest; TF-QKD, twin-field QKD.

[214] and 143-km [223] via commercial optical fibre channels are observed. These performances signify a key step towards realising quantum communication at a global scale [22, 199, 220, 224–226] and establish a promising avenue towards a quantum internet [23, 213, 227, 228]. Thus, quantum teleportation over long distances is essential for realising global quantum communications as well as large-scale quantum networks. Over the years, several quantum teleportation models have been widely investigated theoretically and experimentally (see Refs [63, 199]), including quantum technology protocols and others that are conceptually valuable in the theoretical model. These include entanglement swapping [229–231], controlled quantum teleportation [232, 233], teleportation of a shared quantum secret [234, 235], quantum teleportation network [236], port-based teleportation [237, 238], quantum gate teleportation, and quantum computing [239, 240].

Most significantly, various ML techniques have been applied in detecting or classifying quantum entanglement, a valuable resource in quantum teleportation, in various settings. For instance, in 2018 Lu et al. [241] demonstrated a reliable classifier for classifying entangled and non-entangled states by

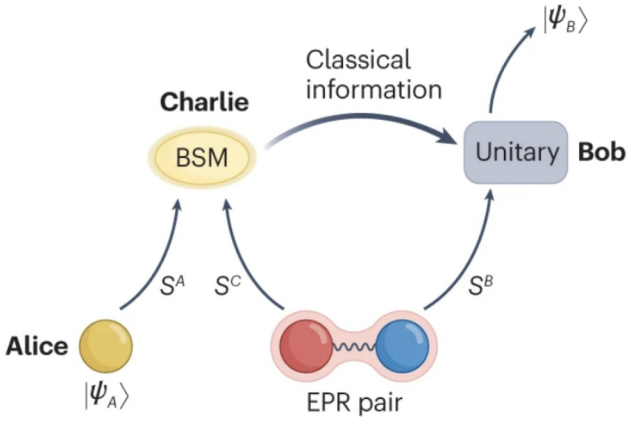

FIGURE 6 An illustration of a quantum state teleportation scheme. The scheme consists of previously shared entanglement, BSM, classical communication, and unitary operations. The red, yellow, and blue circles represent particles in the quantum teleportation protocol. The S^A, S^B, S^C represent the quantum channels for transmitting particles A, B and C. The states $|\psi_A\rangle$ and $|\psi_B\rangle$ represent the input quantum state and output quantum state, respectively. The EPR pair is a maximally entangled quantum state. Reproduced from Ref. [63]. BSM, Bell-state measurement; EPR, Einstein–Podolsky–Rosen.

employing supervised learning techniques. Specifically, the authors developed a reliable separability-entanglement classifier by combining supervised learning and the convex hull approximation method. This method outperforms conventional criteria for entanglement detection in generic cases in terms of speed and accuracy. Furthermore, the authors claim that the classifier can be extended to higher dimensions in the future and incorporated into experiments involving entanglement engineering. In 2021 Chen et al. [64] proposed a procedure for detecting quantum entanglement with an unsupervised ML method (complex-valued NN) for high-dimensional and multipartite quantum systems. A noteworthy feature of this NN is that it achieves a detection accuracy of 97.5%. This work is critical since quantum features, such as entanglement and coherence, are indispensable resources in various quantum information processing tasks, such as QKD, teleportation, and quantum computing [5]. Additionally, by harnessing ML algorithms to detect entanglement, recently in 2023, Asif et al. [242] use supervised ML methods to construct a classifier by employing the relationship between coherence and entanglement. In particular, this method encodes multiple Bell-type inequalities (as an entanglement witness) for the relative entropy of coherence into ANNs for detecting entangled and separable states in a quantum dataset. Notably, the classifier trained with the most straightforward NN distinguishes the quantum states with an accuracy of 78.18%, and the classifier's performance increased by increasing the number of neurons to result in a performance of 94.62%. As a result, this brief review illustrates the potential of using ML techniques to detect entanglement thereby enhancing quantum communication protocols, including teleportation.

Furthermore, another important but different aspect, Boerkamp (2023) demonstrates the utility of ML to calculate the minimum number of qubits required and how they should be coded to create a quantum wormhole with the Google Sycamore quantum processor [243]. Through quantum information passing through the system, the researchers sought insights into gravitational dynamics. Most significantly, these examples demonstrate that this field is advancing, and integrating AI and ML algorithms promises significant potential to optimise quantum state control and manipulation, which is critical in teleportation. Broadly, this could facilitate the discovery of novel teleportation techniques and enable long-distance and high-fidelity quantum communication.

The research on quantum teleportation has demonstrated significant progress, suggesting quantum teleportation of complex quantum states (i.e. multiple degrees of freedom [216], high-dimensional quantum states [244, 245]) with high fidelity under the premise of long distances [222] is possible in these systems in the near future. However, since quantum teleportation inherently depends on manipulating complex quantum states, some inherent challenges remain. These challenges are associated with the preparation of entanglement [199, 246, 247], Bell-state measurements [248], the randomness of the spontaneous parametric down-conversion [249] and inefficient nonlinear processes [250]. Most significantly, efforts such as implementing quantum teleportation via a deterministic photon source [251, 252], highly efficient on-chip nonlinearity [253], high-dimensional entanglement of trapped-ion [254], nitrogen-vacancy (NV) centres [255] and superconducting qubits [256] have been poised as promising solutions [63].

Due to some of these outstanding challenges, several ML algorithms have recently been proposed to enhance and optimise quantum teleportation protocols. A study conducted in 2019 by Wallnöfer et al. [55] develops the mathematical tools needed to perform reinforcement learning of central quantum communication protocols, specifically quantum teleportation, entanglement swapping, and entanglement purification. This was achieved by combining reinforcement learning techniques with projective simulations. Particularly, a projective simulation is a physically motivated framework for reinforcement learning and decision-making, based on deliberation in an episodic and compositional memory (ECM) [55]. An example of this is Figure 7, which illustrates the trial-and-error process of learning quantum communication protocols through reinforcement learning interactions between an agent and the environment. An agent is equipped with a universal gate set, and it specifies the desired task through a reward scheme. By trial and error, the agent manipulates quantum states to create quantum communication protocols. When the agent (the protocol) interacts with the protocol (the environment), the agent perceives the present state of the protocol (the environment) and selects one of its available options (actions). Thus, the previous protocol is revised and the interaction step is completed. A reward function specifies feedback given to agents during each interaction step. This is based on the specific quantum communication task (a–d) illustrated in Figure 7. Notably, a reinforcement learning agent interprets a reward and updates its memory accordingly. The agent plays a more critical role than mere parameter estimation since simple search

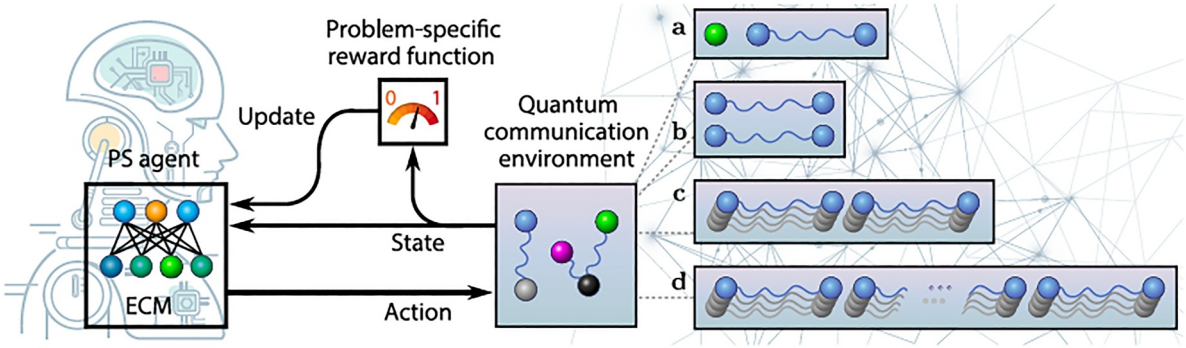

FIGURE 7 An illustration of a reinforcement-learning agent interacting with the environment. The agent performs actions that change the state of the environment, while the environment communicates information about its state to the agent. The reward function is customised for each environment. ECM, episodic and compositional memory; PS, projective simulation. The initial states for the different environments that we consider here are illustrated: (a) teleportation of an unknown state, (b) entanglement purification applied recurrently, (c) quantum repeater with entanglement purification and entanglement swapping, (d) scaling of quantum-repeater concepts to distribute long-distance entanglement. Reproduced from Ref. [55].

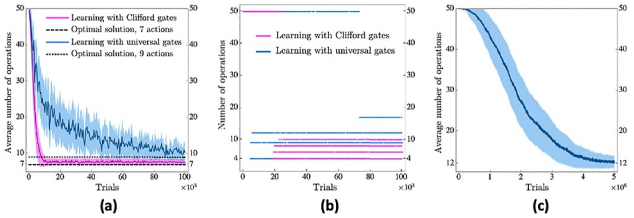

FIGURE 8 An illustration of a reinforcement learning algorithm in a teleportation protocol. (a) Learning curves of an ensemble of projective simulation agents: average number of actions performed to teleport unknown quantum states. (b) Two learning curves (magenta and blue) of two individual projective simulation agents. Four solutions of different lengths are found by agents. (c) Learning curve in the learning setting that is, the average number of actions performed to teleport an unknown quantum state. In (a and c), the curves represent an average of over 500 agents. The shaded areas show the mean squared deviation $\gamma/3$. This deviation appears not only because of the different individual histories of the agents but also because of the difference in the individual solution lengths shown in (b). Reproduced from Ref. [55].

methods would not be sufficient for problems of this size (i.e. the number of possible states in teleportation tasks). According to Figure 7, the ECM is based on a random walk process, which requires little computational effort and can be accelerated via quantum walk processes, which result in a quadratic speedup in deliberation time, making the projective simulation model conceptually appealing.

Particularly, the learning process is depicted in Figure 8, where the two particles 2 and 3 at the sender's station and receiver station, respectively, are described in Equations (1) and (2). Figure 8a, shows the learning curve, which is the number of operations the agent applies to reach a solution in each trial. The authors observe that the learning curve converges to some average number of operations in both cases though the mean square deviation does not go to zero. A learning curve, or the number of operations the agent uses in each trial, is shown in Figure 8a. According to the authors, the learning curves converge to the same average number of operations for both Clifford (magenta) and universal (blue) gates. As you can see from the individual learning curves of two agents in Figure 8, the mean squared deviation does not reach zero. A better explanation can be found in Figure 8b by examining the individual learning curves of two example agents: the agent does not arrive at a single solution to this problem setup, but rather four different solutions. As shown in Figure 8c, the learning curve has been averaged over 500 agents. However, a significant number of trials are needed for the agent to discover a solution due to the long action sequence. However, this illustrates that the agent can locate the quantum teleportation protocol without being provided with an initial entangled state. Thus, this study provides a demonstration of how reinforcement learning is a more effective means of achieving quantum communication than optimisation techniques, particularly quantum teleportation over long distances. A key benefit of this development is that it opens up the possibility of using ML techniques, such as reinforcement algorithms, to design and implement quantum networks, which do not have a wide range of existing protocols.

Owing to difficulties associated with executing high-dimensional Bell-state measurements, teleportation of high-dimensional quantum states remains challenging [199]. Zhang et al. [62] demonstrated experimentally in 2022 that unknown qutrits can be teleported by generating, transferring, and manipulating photons and training quantum encoders on silicon chips. The use of quantum autoencoders can facilitate the efficient compression of quantum data. Specifically, the authors employ unsupervised ML to train an autoencoder to train an encoder capable of teleporting a quantum state from a particular d to n-dimensions (i.e. compressing-teleporting-decompressing a quantum state) using integrated photonic chips for future scaling. Training the encoder involves minimising the likelihood of the trash mode being occupied while retaining all information regarding qubit modes. A lossless compression occurs when the trashed state is unoccupied, allowing the decoder to reconstruct the initial qutrit. Notably, ML algorithms update the encoder parameters to achieve

teleportation fidelity of 0.894. This work lays the foundation for integrating ML techniques to develop reliable and efficient quantum networks and quantum computations, which opens the way to the quantum internet. Satellite-based quantum communications can also assist in establishing the infrastructure for a global quantum network [22, 222]. While satellite quantum technologies have some significant potential, they face challenges such as atmospheric turbulence, diffraction, and regular refraction. These challenges cause drift or random wandering and broadening of the transmitted beam. This results in fluctuations in transmittance, which complicate the prediction process. Therefore, there is a need to combat the effects of loss and noise in the transmission link.

Towards addressing challenges in satellite-based quantum communication, Xu et al. [257] proposed an ML-assisted approach to continuous-variable quantum teleportation prediction over the satellite-ground link. The authors employ a *K*-nearest neighbour (KNN) algorithm and a DT algorithm to predict the squeezing parameter r and satellite altitude H, which can be derived from the traditional formula. The authors simulate the difference between the real value and the predicted value using different zenith angles, turbulent intensities, and fidelity of the continuous-variable quantum teleportation system at different wavelengths. The numerical simulations indicate that the KNN algorithm has a significant error in the prediction, while the DT algorithm has a reasonable agreement with the actual results when the parameters are adjusted accordingly. As a result of this approach, authors overcome the challenges posed by numerical analysis approaches, which show that predictions can be made within an acceptable error range under certain conditions. Additionally, their procedure addresses quantum channel losses and guides ML-based continuous-variable quantum teleportation in practice. Thus, integrating AI and ML algorithms with quantum teleportation will shape quantum information processing, especially quantum teleportation as shown in Table 2. Overall, these advances will lead to the development of a global quantum networked landscape in the future.

3.3 | Quantum secret sharing

Secret sharing is an essential cryptographic protocol for sharing highly confidential information with trusted and untrusted individuals. Secret sharing was independently introduced by Shamir [258] and Blakley in 1979 [259] as a solution to safeguard cryptographic keys. Generally, in a secret sharing scheme, the distributor divides a classical or quantum secret into multiple shares, and only the shareholders in the authorised set can retrieve the secret when a sufficient number of shares are combined. Therefore, the shareholders in the non-authorised set are unable to leak any information or recover the shared secret [260, 261]. Various secret sharing schemes have since been realised can be classified as secret splitting [262], threshold sharing schemes [258, 259], and verifiable secret sharing scheme [263]. These schemes are utilised in various cryptographic protocols [264], for instance secure multiparty computation (MPC) [265, 266], secure aggregations [267], multi-signature [268, 269], and attribute-based encryption [270, 271]. The security of these schemes is dependent on the computational complexity of large prime decomposition. As quantum computers and quantum algorithms develop, the security of these classical secret sharing schemes is severely compromised [13]. Accordingly, secret sharing has been extended into various quantum versions. The first QSS scheme was proposed by Hillery et al. using the Greenberger–Horne–Zeilinger (GHZ) state, in which one party can share credible classical information with other two or three parties in the presence of an eavesdropper [25]. This was followed by Cleve et al. proposal of a threshold QSS scheme using the quantum error correction code theory [260]. While various schemes are constantly being proposed, typically, QSS protocols are divided into three categories: when the shared information is an unknown quantum state, it is called quantum state sharing [25, 234], QSS when shares the classical information [272] and a QSS of both of them [273]. These schemes are based on quantum physical properties to share classical information, while some schemes are based on quantum mechanics

TABLE 2 Summary of AI/ML applications in quantum entanglement or teleportation schemes.

Quantum protocol or resource	AI/ML model	Main objective or outcome
Quantum entanglement	Supervised learning	Demonstrated a reliable separability-entanglement classifier [241]
Quantum entanglement	Complex-valued neural network	Detected a quantum entanglement in high-dimensional and multipartite quantum systems and achieves a detection accuracy of 97.5% [64]
Quantum entanglement	Supervised learning	Constructed a classifier by employing the relationship between coherence and entanglement [242]
Quantum teleportation	Reinforcement learning + projective simulation	Discovered various quantum communication protocols, including quantum teleportation, quantum distillation, and end-to-end bipartite entanglement distribution along a chain of quantum repeaters [55]
Quantum teleportation	Unsupervised learning	Trained an on-chip autoencoder to encode 3-D quantum state onto 2-D quantum teleportation, observing 3-D teleportation [62]
Quantum teleportation	KNN	Predicted the continuous-variable quantum teleportation squeezing parameter and the satellite altitude [257]

Abbreviations: AI, artificial intelligence; KNN, *K*-nearest neighbour; ML, machine learning.

principles to share the arbitrary quantum state of information [272]. These schemes have been followed by several proposals based on various quantum principles, such as single photons [274, 275], entangled states [276] and product states [277]. These schemes include general QSS [278], multiparty QSS [25, 273, 279], multiparty semi-QSS [280], multiparty to multiparty QSS [281, 282], threshold QSS [283, 284], access structure-based QSS [278, 285], circular QSS [286], and dynamic QSS [287, 288] protocols.

As shown in Figure 9, the QSS scheme uses the GHZ three-qubit states [289]. The 3-qubit entangled GHZ state can be described as follows:

$$|\psi\rangle_{\mathrm{GHZ}} = \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2|0\rangle_3 + |1\rangle_1|1\rangle_2|1\rangle_3), \tag{3}$$

where $|0\rangle$ and $|1\rangle$ are orthogonal states in an arbitrary Hilbert space. Each particle is labelled by one of the indices. As illustrated in Figure 9, each of the three photons in the GHZ state has its own mode. When the two beamsplitters located at Alice's, Bob's and Charly's have their modes combined, the probability of finding the three photons in the output ports depends on the settings α, β, γ of the phase shifters:

$$P_{i,j,k} = \frac{1}{8}(1 + ijk\cos(\alpha + \beta + \gamma)), \tag{4}$$

where $i, j, k = \pm 1$ denotes different output ports. Before each measurement, Alice, Bob, and Charly will select randomly one phase value from $(0, \pi/2)$. Once a sufficient number of runs have been completed, they identify cases where they all detected a photon. Afterwards, Alice, Bob and Charly announce the phases chosen and identify cases in which the sum adds up to either 0 or π. Based on the probability function depicted in Equation (4), a result of 1/4 is obtained for these cases. Using $l = \cos(\alpha + \beta + \gamma) = \pm 1$ and $P_{i,j,k} = 1/4$ yields i, j, k, $l = 1$. At this moment Alice, Bob and Charly each know two of the values i, j, k. When Bob and Charly come together and combine their knowledge, they can establish three of the four parameters. Additionally, they are able to determine the last one, which is also known to Alice. By identifying '−1' with the bit value '0' and '+1' with '1', the correlated sequences of parameter values can then be turned into a secret key.

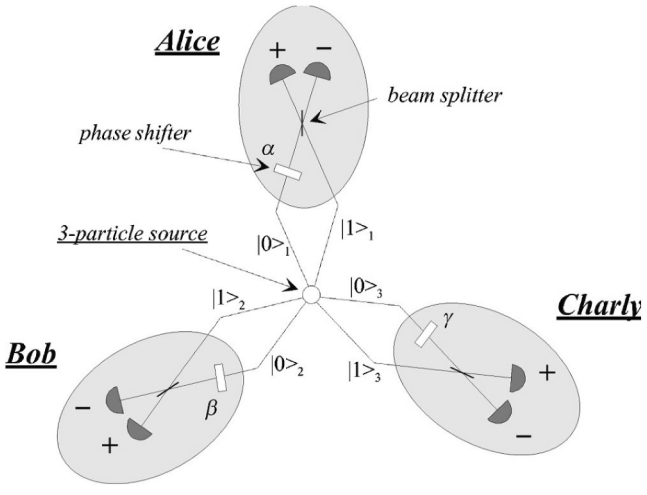

FIGURE 9 An illustration of a QSS scheme using the 3-qubit GHZ states. A real implementation would have the source as part of Alice setup, not that of a fourth party. Reproduced from Ref. [289]. GHZ, Greenberger–Horne–Zeilinger; QSS, quantum secret sharing.

While quantum entanglement constitutes a significant resource in QSS protocols, Guo et al. surprisingly demonstrated the implementation of a QSS protocol without entanglement, in which only product states are employed [290]. This protocol is more applicable when the number of parties sharing secrets is large. Notably, the authors demonstrate that this scheme has a theoretic efficiency that can be doubled to approach 100%. Due to the guarantee of quantum fundamental principles, QSS offers significantly enhanced security than the computationally complex classical secrets. While most of the proposed QSS schemes are designed based on two-dimensional quantum systems (i.e. qubits) with multi-qubit maximally entangled quantum state, QSS protocol design has recently been extended to higher-dimensional systems (i.e. qudits) [291–293] and orbital angular momentum [294]. This extension allows a higher degree of resource capacities and enhanced security, leading to improved practical implementations. QSS schemes have an important role to play in quantum communication, such as fibre network configuration [295] and quantum secure transport system [296]. Specifically, they have been utilised in a wide range of quantum cryptographic applications such as joint checking accounts containing quantum money [297], joint financial transaction and quantum digital signatures [298], share hard-to-create ancilla states [239], perform a distributed computation [297], missile launching codes [299], and electronic voting [17, 261, 300].

While QSS demonstrates promising potential, the schemes face several challenges that must be addressed to achieve practical implementation and widespread adoption. As quantum communication systems are vulnerable to interception, adversaries can exploit the vulnerability to intercept and gain unauthorised access to shared secrets [275, 277]. These schemes require precise manipulation and measurement of quantum states, which requires highly controlled and stable experimental setups [291, 294]. The shared secrets can be compromised by external noise, including decoherence and errors in quantum gates, environmental disturbances, and hardware imperfections. In addition to technical challenges and communication costs, practical implementation requires a high level of control and stability [284]. Furthermore, scalability and efficiency also pose challenges [274]. What is more, the complexity of the secret-sharing scheme typically increases exponentially with the number of parties involved. As a result, key management, communication overhead, and computational resources are challenging for secure sharing and reconstruction of secrets. These risks can be mitigated with fault-tolerant quantum computing architectures and robust error correction techniques. As a result, developing efficient algorithms and protocols for large-scale secret sharing is now an ongoing research area. A review of the integration of various ML has been presented, particularly

concerning multi-party computation protocols [301]. The authors demonstrate how these algorithms and secret sharing can be used to safeguard data privacy when multi-party computation is being performed.

ML models are typically trained on massive amounts of data collected from multiple sources [92, 93]. These data sources may contain sensitive data relating to finance, healthcare, personally identifiable information, and other confidential data. However, these models are not equipped with privacy-preserving features [302]. Rather, the models anonymise the data, which does not guarantee privacy [303]. This raises concerns since models must not expose sensitive information. For these reasons, various ML models incorporate secure MPC [304], homomorphic encryption [305], and differential privacy [306] as a means of protecting the privacy of collected data. Although this enhances security, performance, and accuracy still needs to be improved. Therefore, we are interested in an ML model that can achieve both full data privacy for security and efficiency for practicability. As a result, distributed ML approaches have been proposed, which allow clients to store their data locally but train collaboratively. This approach provides higher accuracy and improved performance, but security still needs to be improved. As a result, in 2020, Dong et al. [307] proposed a novel secure computation framework that integrates distributed ML, specifically linear regression, multilayer perceptron, and CNN with secret sharing to achieve reliable performance, accuracy and high-level security in semi-dishonest parties. This work demonstrates an efficient practical system that can be used to jointly learn an accurate model under semi-honest and server-only malicious adversary security, respectively. Notably, a client may not learn more information than what is contained in the trained model, and a parameter server may not learn sensitive information. As a result, integrating distributed ML with secret-sharing schemes ensures that the model achieves the best overall performance while still meeting security requirements.

Furthermore, in 2022, Wei et al. [308] presented a privacy-preserving K-means clustering algorithm that employs replicated secret sharing [309] with the honest majority in semi-honest models. The secret sharing-based privacy-preserving K-means clustering scheme is shown in Figure 10. Particularly, a privacy-preserving K-means clustering, which has full data privacy, allows the parties to cluster their combined datasets without revealing any other information except for the final centroid [310]. This means the information on intermediate centroids, cluster assignments, and cluster sizes should be protected in the protocol. Therefore, the clustering task is outsourced to three semi-honest computing servers. Specifically, the proposed protocol provides full privacy guarantees, which allows different computing parties to cluster the combined datasets without revealing any other information except the final centroids. As a result, the protocol is secure against a single corrupt server under a semi-honest model. The proposed secret sharing-based privacy-preserving K-means clustering scheme is illustrated in Figure 10. The scheme is implemented and analysed and the experimental results are shown in Table 3. Particularly, the authors use the 2D dataset arff and 4D dataset Iris to evaluate accuracy. Particularly, they compare the accuracy of ground truth, plaintext and privacy-preserving models for 2D dataset arff and obtain a value of 98.20%. The comparison of the experimental results of this dataset is visually illustrated in Figure 11. However, for the iris dataset, the privacy-preserving model reaches an accuracy of 92.67%. Therefore, the proposed scheme achieves both full data privacy for security and efficiency for practicability.

Experimental results demonstrate that the proposed protocol achieves the same level of accuracy as plaintext K-means clustering. By using the fast network, the privacy-preserving scheme can deal with datasets of millions of points in a reasonable amount of time. Comparatively, this scheme achieves about 16.5–25.2 times higher computation speeds and 63.8–68.0 times lower communication rates than the existing

Parameters:

- Number of clusters K; number of data points n; dimension d.
- Ideal $\mathcal{F}_{\mathsf{OS}}, \mathcal{F}_{\mathsf{SED}}, \mathcal{F}_{\mathsf{LT}}, \mathcal{F}_{\mathsf{Assign}}, \mathcal{F}_{\mathsf{Div}}$ primitives.

Secret Distribution:

1. The data owner generates the 3-out-of-3 additive shares of data points matrix $\mathbf{P} = (\mathbf{P}_1, \cdots, \mathbf{P}_n)$ with dimension $n \times d$.
2. The data owner sends the shares to three semi-honest computing parties/servers $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$.
3. Each party reshares the shares and obtains valid 2-out-of-3 replicated shares.

Initialization:

1. The data owner chooses K random points as the initialized centroids, forms $K \times d$ centroid matrix $\boldsymbol{\phi} = (\boldsymbol{\phi}_1, \cdots, \boldsymbol{\phi}_K)$.
2. The data owner shares $\boldsymbol{\phi}$ to three computing parties similar to secret distribution.

Lloyd's Steps:

For $t \in [T]$, the parties repeat the following steps until the stopping criterion.

1. For $i \in [n], k \in [K]$, the parties compute the shares of the Euclidean squared distance by invoking $[\![X_{ik}]\!] \leftarrow \mathcal{F}_{\mathsf{SED}}([\![\mathbf{P}_i]\!], [\![\boldsymbol{\phi}_k]\!])$. The parties form $n \times K$ matrix $\mathbf{X}$.
2. For $i \in [n]$, the parties assign point $\mathbf{P}_i$ to the closest cluster by invoking $[\![c_i]\!] \leftarrow \mathcal{F}_{\mathsf{Assign}}([\![\mathbf{X}_i]\!])$. The parties forms $K \times n$ matrix $[\![\mathbf{C}]\!]$ such that the i-th column of $\mathbf{C}$ is c_i.
3. The parties compute the share of matrix multiplication $[\![\mathbf{M}]\!] \leftarrow [\![\mathbf{C}]\!] \cdot [\![\mathbf{P}]\!]$ by using RSS vectorized multiplication technique. For $k \in [K]$, the parties jointly recalculate the sharing $[\![\boldsymbol{\varphi}_k]\!]$ of the new centroid as follows:
   (a) Compute the shares of the denominator $[\![D_k]\!] \leftarrow \sum_{i=1}^{n} [\![\mathbf{C}_{ki}]\!]$.
   (b) Compute the shares of the average of the points in each cluster by invoking $[\![\boldsymbol{\varphi}_k]\!] \leftarrow \mathcal{F}_{\mathsf{Div}}([\![\mathbf{M}_k]\!], [\![D_k]\!])$.
   (c) Compute the shares of Euclidean squared distance between $\boldsymbol{\varphi}_k$ and $\boldsymbol{\phi}_k$ by invoking $[\![e_k]\!] \leftarrow \mathcal{F}_{\mathsf{SED}}([\![\boldsymbol{\varphi}_k]\!], [\![\boldsymbol{\phi}_k]\!])$.
4. The parties update the cluster centroids as follows:
   (a) The parties locally compute the sharing of error $[\![e]\!] \leftarrow \sum_{i=1}^{K} [\![e_k]\!]$.
   (b) The parties invoke $[\![b]\!]^{\mathsf{B}} \leftarrow \mathcal{F}_{\mathsf{LT}}([\![e]\!], \varepsilon)$ and reveal b.
   (c) If $b = 1$, then stop criterion and reveal $\boldsymbol{\varphi}$. Otherwise, replace $[\![\boldsymbol{\phi}]\!]$ with $[\![\boldsymbol{\varphi}]\!]$.

FIGURE 10 An illustration of the proposed efficient three-party computation protocol for secret sharing-based K-means clustering algorithm. Based on the definition of full data privacy, the information about the intermediate centroids, cluster assignments, and cluster sizes should be protected. Thus, the only information that can be leaked is the range of D_k. Hence, the protocol provides full data privacy. Reproduced from Ref. [308].

TABLE 3 A description of datasets used in the experiments.

Dataset	n	K	d	Accuracy
Iris	150	3	4	92.67%
Arff	100	4	2	98.20%
Self-generated	{10, 000, 100, 000}	{2, 5}	{5, 10, 15, 20}	-

Note: Each dataset has n data points, K clusters, and d dimensions. The accuracy of different datasets is also evaluated if a ground truth model exists for the dataset. Reproduced from Ref. [308].

privacy-preserving schemes. Additionally to its high efficiency and practicality, the scheme is also suitable for large-scale clustering tasks. Overall, the privacy-preserving scheme guarantees full data privacy and is suitable for secure outsourcing of computations based on secret-sharing. The ability of ML to optimise resource allocation, enhance security, identify vulnerabilities, mitigate noise and imperfections, and uncover hidden correlations makes it a valuable tool for increasing the effectiveness and reliability of various QSS schemes. Even though this field is still undergoing development as summarised in Table 4, these few examples demonstrate the potential of integrating ML into secret-sharing schemes show the potential for improving QSS. Therefore, further research into incorporating AI and ML into QSS may ultimately result in more robust and secure methods for sharing secrets in the quantum world.

3.4 | Quantum networks

A quantum network is intended to facilitate secure communication between quantum computers or secure cloud quantum computing, as well as quantum-enhanced measurement networks, ultimately leading to a quantum internet, a global network capable of transmitting quantum data [20, 311]. Thus, quantum networks promise to enhance existing classical networks as well as execute protocols that would be impossible in a classical network. While significant progress has been made, challenges remain, including transmission losses, decoherence, and limitations imposed by the no-cloning theorem. As a result, to enable long-distance end-to-end communication of qubits, quantum networks rely on the following three primary components: end nodes, which serve as processors, quantum channels, which distribute information, and quantum repeaters, which generate separate entanglement pairs and transmit qubits from each pair to the respective nodes [20, 21]. Thus, in this section, we will discuss the integration of AI and ML algorithms to address the aforementioned challenges or limitations and improve the performance of these components, resulting in an overall improvement in quantum networks. An illustration of a typical quantum network is presented in Figure 12. Quantum network systems rely on existing network infrastructure for exchanging classical messages in order to run quantum protocols, as well as for controlling and managing the network [311]. Due to challenges in building long-distance communication, a chain of automated quantum repeaters is used in order to build links due to the limitations associated with sending secure messages over long distances. Regarding a comprehensive review of quantum networks, we refer the reader to Refs [21, 312–315].

Particularly, quantum repeaters are hybrid devices that can broadcast 'flying' qubits (photons) without measuring or cloning them, which is against the quantum no-cloning theorem. The operation of quantum repeaters is intrinsically based on the phenomenon of quantum teleportation, one of the most fascinating applications of entanglement. Typically, a quantum repeater comprises three elements: entanglement generation, entanglement connection, and entanglement purification. By connecting repeaters, entanglement can be

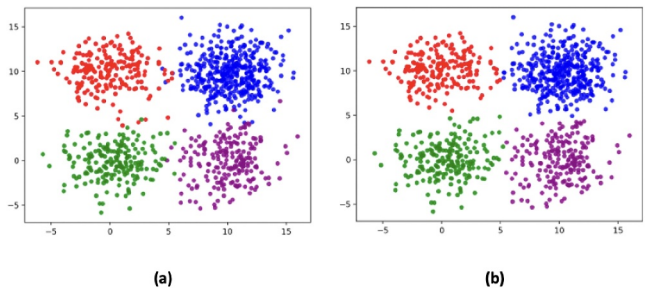

FIGURE 11 The comparison of accuracy for ground truth, plaintext and privacy-preserving for secret sharing-based *K*-means schemes using the 2D dataset arff. (a) a ground truth model and (b) a plaintext and privacy-preserving model. Notably, the privacy-preserving model achieves the same accuracy level as a plaintext model. The accuracy is 98.20% compared to the ground truth model. Reproduced from Ref. [308].

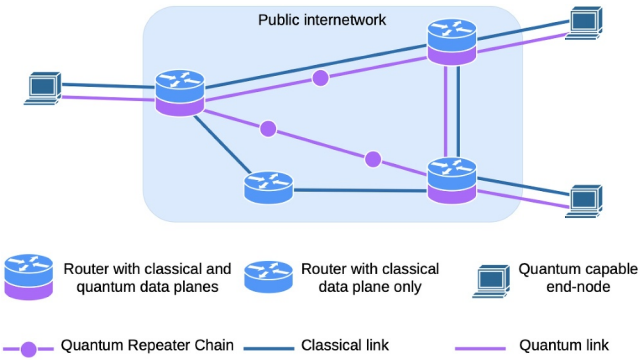

FIGURE 12 An illustration of a typical quantum network. The system consists of several components including a quantum repeater, classical links, and quantum links for establishing long-distance quantum communication or large-scale quantum networks. Reproduced from Ref. [311].

TABLE 4 Summary of AI/ML applications in secret sharing schemes.

Scheme	AI/ML model	Main objective or outcome
Secret sharing	Linear regression, MLP, and CNN	Improved the accuracy, reliability, security, and performance of privacy-preserving distributed ML based on secret sharing [307]
Secret sharing	*K*-means clustering	Enhanced the efficiency and practicality of a privacy-preserving secret-sharing-based secure three-party computation [308]

Abbreviations: AI, artificial intelligence; CNN, convolutional neural network; ML, machine learning; MLP, multilayer perceptron.

extended by a significant distance, providing a viable option for establishing long-distance quantum communication or large-scale quantum networks [214, 222].

An example of a long-distance end-end-QKD based on trusted quantum repeaters is shown in Figure 13. Typically, the sender and receiver are connected via a quantum channel and a public channel. The two intermediate nodes with trusted repeaters are placed between the source node and the destination node. Figure 13 illustrates how three secret keys are produced between the source node and intermediate node 1, intermediate node 1 and intermediate node 2, intermediate node 2, and the destination node. Most significantly, the produced three secret keys have the same key size. Essentially, the procedure consists of three steps: (1) Intermediate node 1 encrypts K_{s1} using K_{12} and obtains the ciphertext $K_{s1} \oplus K_{12}$. Then, the ciphertext $K_{s1} \oplus K_{12}$ is sent to intermediate node 2. (2) Using K_{12}, intermediate node 2 decrypts $K_{s1} \oplus K_{12}$ to obtain K_{s1}. Then, intermediate node 2 encrypts K_{s1} using K_{2d}, to obtain the ciphertext $K_{s1} \otimes K_{2d}$. The ciphertext $K_{s1} \otimes K_{2d}$ is sent to the destination node. (3) Using K_{2d}, the destination node decrypts the ciphertext $K_{s1} \otimes K_{2d}$ to obtain K_{s1}. As a result of the above three steps, K_{s1} can be shared between the source node and the destination node. Notably, for end-to-end QKD over long distances, several intermediate nodes with trusted repeaters can be placed between the source and destination nodes, where all of the intermediate nodes must be trustworthy because they will all know the real secret keys, for example, K_{s1}.

Although using trusted repeaters is a notable advance, there are still challenges in transmitting information over large distances due to turbulence and losses in the physical channels [17, 53]. The advancements in integrated photonics remain among the most stable, compact, and robust platforms for miniaturising massive photonic circuits [317, 318]. Due to the compatibility of integrated photonic chips with current integrated photonic telecommunication hardware, seamless integration is assured with classical communication channels and transceivers [319]. Through this integration, developments are underway to realise hybrid classical and quantum communications, with a current distance of more than 100 km achieved [320–322]. Notably, an integrated satellite-ground quantum communication network of over 4600 km has recently been reported [323]. The capability of satellite-ground QKD using optical photons shows tremendous potential for long-distance and intercontinental quantum communication [324]. The

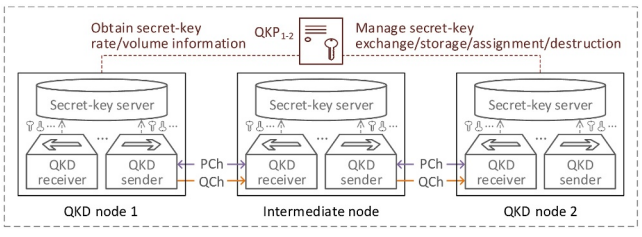

FIGURE 13 An illustration of a typical trusted quantum repeater. An example of QKP for managing secret keys in a pair-wise manner between QKD node 1 and QKD node 2. Reproduced from Ref. [316]. QKD, quantum key distribution; QKP, quantum key pool.

reason for this is that optical photons have low quantum information transmission losses and negligible quantum decoherence in space. This represents a significant development that shows the possibility of building quantum networks across continents.

Due to quantum properties such as quantum entanglement, quantum uncertainty, and quantum no-cloning theorem, quantum networks can provide ultra-secure information exchanged over multiple technologies across numerous channels [20, 21, 247]. With advances in quantum computing technologies, quantum networks can now complement classical networks in processing and delivering information securely since not all information transmitted must be encoded in photons, for example, quantum teleportation [23, 31, 53]. Thus, combining classical and quantum networks to create a quantum internet will result in capabilities that are unparallelled by either technology alone [20]. For instance, the quantum internet will provide new encryption services, enhance sensor network sensitivity, and connect distant quantum computers to facilitate computation, share quantum data, and expand the class of complex problems that can be solved [311, 325].

Due to photon limitations, such as losses at more considerable distances, quantum networks contain vital device elements, including quantum nodes [326], quantum repeaters or quantum switches [155, 156], quantum memories, and quantum channels [327, 328]. The purpose of these devices is to unlock the full potential of quantum networks. As a result, despite their potential, unfortunately, some of these devices are not capable of being successfully deployed with current technology. This presents an opportunity for AI and ML to fill the gap. Quantum networks have the following applications: quantum-secure communications [2, 3, 16, 126, 139], secure identification [329], blind quantum computing [330, 331], network clock synchronisation [332], distributed quantum computing [333, 334], and entanglement sensor network [335]. Notably, despite challenges and limitations, significant progress has been made in developing quantum networks for sending quantum information over reasonable distances, and they are now available for use in QKD with trusted nodes [21].

While quantum networks hold significant potential for secure communication and quantum computing, the development and deployment of quantum information in a large-scale network face several significant challenges. These challenges include: maintaining quantum entanglement, maintaining quantum coherence, scaling and interoperability, distance and connectivity, security, and integration with classical communication infrastructure [21, 227, 311]. Moreover, there are concerns regarding the nature of the hardware platform and its precise implementation requirements. As part of these challenges, scientists and researchers are actively addressing the issue of storing and manipulating qubits by integrating quantum error correction, quantum repeaters, quantum memories, and quantum routers into quantum networks [53, 156, 313, 326, 336]. Among these efforts is a recent attempt to determine whether a quantum network of nodes connected by quantum links has reached a particular development stage. This is done by evaluating the robustness of noisy quantum

networks [337] and quantum network benchmarking. By using this process, it is possible to benchmark the quality of a quantum network and measure its fidelity [338, 339]. Due to the inherent complexity of manipulating quantum systems and their vulnerability to noise, some challenges remain [340]. For instance, a quantum repeater requires a quantum memory, a device that stores conjugate quantum variables. However, no reliable and practical quantum memory is currently available [53]. As an intermediate step, trusted repeaters over long distances [166, 340–342], MDI-QKD networks [53], and TF-QKD protocols [138] are being implemented, and distances of up to 830-km reported [343]. These advances constitute significant steps towards the development of the quantum internet.

Scalable quantum networks require various optimisation models for efficiently assigning quantum information and repeaters in quantum networks. Various efforts have been made to integrate AI and ML into quantum networks leading to improved noise mitigation, network self-configuration, resource allocation efficiency, reliable error correction, self-optimisation, increased performance and security [129, 344–346]. This has resulted in increased performance and security, particularly concerning QKD-secured optical networks. For instance, Ou et al. [189] demonstrated how ML-aided software-defined networking relying on optimal resource allocation was constructed for investigating the coexistence of hybrid quantum and classical channels in a QKD-integrated optical network. The authors present various supervised ML methods to estimate channel QKD performance (noise, SKR, and quantum bit error rate) when Ch-Cs in various quantities, spectrum allocations, launch power, and channel spacing are present in the C-band. As compared to various models such as RF, least-squares method, lasso regression, and ridge regression, the KNN was the most accurate model. Most significantly, this work demonstrates the possibility of QKD integration with conventional DWDM fibre networks, which is crucial for the commercialisation and implementation of quantum networks.

AI and ML techniques have been proposed for predicting optimal channel allocation and quantum parameter values in near real-time, enabling reallocation of quantum channels while ensuring excellent performance through the efficient evaluation of parameter values [347–350]. Furthermore, various low-complexity, but near-optimal wavelength assignment methods have been employed to increase the achievable secret key rate in hybrid quantum-classical networks [228, 351, 352]. Particularly, due to their non-reusable nature, secret key resources in QKD networks are essentially finite and valuable, making their assignment unique. Thus, the expansive cost and challenges inherent in deploying QKD networks, multi-tenancy has become an attractive solution to improve cost efficiency for future QKD networks, particularly for organisations with high-security demands [316]. Essentially, a multi-tenant QKD network is composed of multiple QKD tenants who can share the same QKD network infrastructure in order to obtain their keys for securing their data transfers. Specifically, the generated secret keys can be allocated to multiple tenants over a QKD network infrastructure. Considering that tenant requests arrive on a dynamic basis, obtaining secret keys from the QKD network infrastructure becomes a challenge when simultaneously adapting to the complicated network conditions of the QKD network. As a result, there is an urgent need to develop an effective online multi-tenant secret-key assignment (MTKA) process that can accommodate multiple tenant requests in QKD networks. According to Cao et al. [353], reinforcement learning algorithms can efficiently allocate several network resources, including secret keys, to achieve a MTKA algorithm for QKD networks. According to the results, reinforcement learning based on the MTKA algorithm significantly outperforms benchmark heuristics (e.g. random, fit, best fit) regarding tenant-request blocking probability and secret-key resource utilisation. The reinforcement learning algorithm based on the MTKA algorithm effectively reduces the likelihood of tenant requests being blocked by more than half when compared to the benchmark heuristics. Furthermore, a recent study by Sharma et al. [120] illustrates how reinforcement learning algorithms can be utilised to address the routing and resource assignment challenge in quantum signal channels for QKD optical networks. The authors present a Deep reinforcement learning (DRL)-based routing and resource assignment approach that relies upon proximal policy optimisation in which the optimal route is selected and network resources are efficiently utilised to satisfy quantum signal channel resource requirements for QKD lightpath requests in QKD optical networks. A major finding of the study is that the DRL-based routine and resource assignment scheme outperforms the deep-Q network method, as well as first-fit and random-fit baseline schemes in terms of both blocking probability and resource utilisation.

Quantum memories constitute an integral component of quantum repeaters, which enables long-distance quantum communication and photonic quantum computation protocols beyond that permissible by passive transmission [354]. A universal optical quantum memory can store unknown input states of light and release them on demand with high efficiency and without additional noise [355, 356]. A critical threshold of 50% total storage and recall efficiency may be required depending on the application; however, coherence time will be restricted to tens of microseconds [356]. Over the years, various mechanisms for implementing optical quantum memory have been explored and developed. These include electronic induced transparency [357], Raman schemes [358], as well as atomic frequency combs [359]. However, among other schemes, the gradient echo memory has demonstrated the greatest recall frequency with longer coherence times [356, 360]. Several ML methods have been applied, resulting in significant improvements in optical depth. Accordingly, to enhance these schemes, Leung et al. [361], the integration of ML and compatible single photons improves gradient echo memory performance and may facilitate quantum computation by using it as quantum gates. Due to the analytical complexity of the system, it is generally difficult to optimise a cold atomic ensemble to achieve increased optical depth and lower temperatures. A large optical depth should result in higher memory

efficiencies with stronger atom-light interactions. Particularly, the authors employ reinforcement learning to optimise atom trapping and develop high-extinction filtering methods to isolate single photons from bright pump light. As a result, the cold atomic ensemble is optimised for higher optical depth and lower temperature, which improves the efficiency and coherence times of gradient echo memories.

Moreover, Buchler et al. [362] use an ANN to optimise a laser-cooled atomic ensemble of rubidium 87 atoms to achieve the 'stopped and stationary light' optical quantum memory with an efficiency of about 87% with a decay time of 1 ms with a cold-atom memory. An ML algorithm is used to expedite the trial-and-error approach when maximising the on-axis optical depth of the magneto–optic trap. Despite various efforts to develop efficient quantum networks, quantum memories still have limited coherence times. Although various efforts have been made to develop efficient quantum networks, quantum memories still have a limited coherence time. Khatri suggests that this challenge can be addressed by developing optimal entanglement distribution protocols that take into account the limitations of current and near-term hardware [363]. This includes quantum memories with limited coherence times. The author investigates quantum network protocols for entanglement distribution using decision processes theory. To find the optimal protocol the author leverages dynamic programming or reinforcement learning algorithms. Notably, the author optimises entanglement times on quantum channels across paths in order to establish entanglement states between two end nodes prior to the decay of the channel. The findings of this research pave the way for a systematic investigation of the limitations of near-term quantum networks as well as their physical realisation requirements.

Yun-Hong et al. developed a method to predict the key rate for satellite-to-ground quantum communication channels via ML and stellar image recognition in quantum networks [364]. This work demonstrates a stellar image recognition accuracy rate of approximately 88% and recommends whether to accept or abort the protocol based on the predicted key rate. Specifically, if satellite-to-ground QKD is accepted, the average rate of sifted key at an elevation angle of 39.5° is 8.8 kbit/s, which is adequate for satellite-to-ground QKD tasks involving multiple ground stations. Considering the finite nature of QKD resources, the present work improves the prediction and experimental verification of satellite-to-ground quantum communication networks. A deep NN technique was presented in 2022 by Le et al. that took account of the current network state to schedule the network's demands, which were then routed by a qubit-preserved short-path algorithm [328]. One of the critical challenges of next-generation network systems is routing in quantum networks. The results indicate that in a qubit-limited grid network, the deep reinforcement routing scheme maintains an average fulfiling rate of 80% and approximately 60% of routed requests under extreme conditions. According to the authors, deep reinforcement routing schemes have polynomial complexity and computational time based on quantum network sizes. Recently, Reiß et al. [69] illustrates how DRL can be used to search for optimal solutions for the memory storage time limits, typically known as memory cutoff. This technique allows one to explore general cut-off strategies that dynamically adjust to quantum repeater states. A recent paper by Robertson et al. [365] demonstrates how a genetic algorithm may be used to optimise the write control for Gaussian signal pulses of an optical memory. This work shows that it is possible to reduce pulse energy by 30% without compromising efficiency. The results of this study are consistent with those of Shinbrough et al. in Ref. [366] and support the development of optical quantum memories with high efficiency. A significant aspect of quantum networks is their evolution towards practical maturity, which makes standardisation efforts increasingly crucial. Among these efforts are the standardisation of AI and ML-enabled QKD networks [129, 367]. The standardisation efforts are intended to address the requirements, architectures, functional capabilities, and application programming interfaces needed to implement converged future networks. Accordingly, Table 5 summarises the progress in applying AI/ML algorithms in quantum network schemes.

4 | DISCUSSION AND CONCLUSION

Quantum communication is arguably one of the most successful fields that have evolved from quantum theory. Advances in research and development have resulted in the commercialisation of several quantum communication technologies that have transformed a variety of industries. Additionally, standards and certification processes have been developed to address regulatory considerations, interoperability, performance, and security requirements. This facilitates the integration of quantum systems into existing industries. A certification framework fosters the adoption and acceptance of quantum communication products and services by ensuring quality and reliability. Quantum communication relies on manipulating quantum states in order to ensure reliable and efficient transmission of quantum information. Although significant progress has been made in this area, a number of fundamental challenges still need to be addressed in order to accomplish this goal. Towards addressing these challenges, this work has examined several key milestones demonstrating how AI and ML algorithms have been integrated to optimise various components or implementation parameters to enhance quantum communication protocols and quantum networks, leading to large-scale deployment and ultimately shaping both fields. Moreover, this has the potential to open up new avenues for improving customer experience, optimising network operations, and increasing the efficiency of a network.

The discussion on QKD demonstrates examples of how AI and ML algorithms have been utilised to predict physical parameters, improve the accuracy of raw key data, predict quantum channel quality or failure due to a disturbance as well as recover messages and images with a high level of accuracy. These intelligent techniques adjust communication parameters in real-time and improve the overall key generation and management, security, and efficiency of the protocol. Furthermore, AI and ML methods have been used to detect and mitigate various types of attacks, thereby ensuring the integrity of

TABLE 5 Summary of AI/ML applications in quantum network schemes.

Quantum network or device	AI/ML model	Main objective or outcome
QKD + DWDM fibre network	KNN	To investigate and optimise the coexistence of hybrid quantum-classical channels in a QKD-integrated optical network [189]
Hybrid quantum-classical networks	Reinforcement learning	To increase the number of achievable secret keys for securing data transfers in a multi-tenant QKD network architecture [316, 353]
Optical networks	DRL	Optimise routing and resource assignment problem in the quantum signal channel of QKD-secured optical network [120]
Quantum memory	ANN	To optimise a laser-cooled atomic ensemble to achieve 'stopped and stationary light' optical quantum memory with an efficiency of about 87% [362]
Quantum memory	Reinforcement learning	To develop the mathematical tools needed to perform reinforcement learning of entanglement distribution protocols in general quantum networks [363]
Quantum network	ML	To accurately and quickly predict the key rate for satellite-to-ground quantum communication channels via ML and stellar image recognition in quantum network [220]
Quantum repeaters	DRL	To search for optimal solutions to memory storage time limits [69]

Abbreviations: AI, artificial intelligence; ANN, artificial neural network; DRL, deep reinforcement learning; DWDM, dense wavelength-division multiplexing; KNN, *K*-nearest neighbour; ML, machine learning; QKD, quantum key distribution.

quantum communications. Most significantly, this has also resulted in enhanced security, improved efficiency, and ensured the confidentiality and integrity of information.

We discuss implementations demonstrating the use of AI and ML to mitigate noise and decoherence, leading to enhanced performance of quantum teleportation schemes. Various works have shown that AI and ML techniques can improve several quantum error correction codes, making quantum teleportation systems more fault-tolerant and reliable. In particular, AI and ML algorithms have been used to identify central quantum protocols as well as detect and classify quantum entanglement. This could reduce the risk of eavesdropping and maintain confidentiality while enabling secure data transmission. Leveraging various AI and ML techniques leads to improved efficiency, reliability, and security of quantum teleportation protocols. This could enable longer and more secure quantum communication.

Several authors discuss how ML algorithms can be used to enhance data transmission rates and optimise the allocation of network resources based on the specific resource requirements of different communication tasks. The results demonstrate a significant improvement in resource utilisation and a reduction in the overall cost of quantum communication systems. Notably, noise mitigation is imperative for all quantum communication protocols and networks since they affect scalability. It has been demonstrated that ML algorithms can be trained to adjust QSS parameters dynamically based on real-time feedback and mitigate noise. This has led to improved performance, reliability, security, and defence capabilities of QSS schemes against emerging threats. AI and ML algorithms can predict and compensate for signal degradation or noise by analysing quantum channels. This will enhance the efficiency and practicality of various privacy-preserving secret-sharing-based schemes. Towards the future, AI and ML have a significant potential to optimise various quantum communication channels used in secret sharing protocols.

Considering the challenges in achieving long-distance transmission, we have explored how AI and ML have been applied in quantum communication networks. AI and ML algorithms have been used to optimise the existence of hybrid quantum-classical channels, optimise routing and resource allocation, optimise solutions to memory storage time limits, and improve scalability. As quantum communication networks evolve, AI and ML will be crucial to unlocking their potential. Besides this significant progress, some limitations must be overcome in order to harness the full potential of integrating AI and ML in quantum communication. For instance, a key aspect of AI and ML is the need for vast amounts of data to train models. However, the quantum communication field often deals with sensitive data, such as encryption keys, that require stringent security measures. Balancing the need for data with the desire for privacy poses a significant challenge. Furthermore, quantum communication schemes, including quantum networks are inherently susceptible to noise, disrupting the transmission of information. Developing algorithms that can efficiently handle and mitigate quantum noise is crucial for the successful integration of AI and ML in quantum communication. Moreover, integrating AI and ML algorithms with quantum communication requires optimising them for quantum hardware. This optimisation process can be challenging due to the limited computational power currently available in quantum computers.

As a future direction, it is critical to continue to expand efforts to improve the performance of quantum devices while overcoming their limitations. Moreover, improving the predictability of quantum systems will help AI and ML algorithms make more accurate predictions and perform efficient quantum computations. Another key aspect is developing algorithms to efficiently process and interpret quantum data. These algorithms need to be robust, scalable, and capable of handling the complex nature of quantum information. While there are still challenges and limitations

in quantum communication, with continued advancements in AI and ML, this field is poised for significant progress in the future. This review sets the stage for delivering the envisaged secure quantum internet.

AUTHOR CONTRIBUTIONS

The author confirms being the sole contributor to this work and has approved it for publication.

CONFLICT OF INTEREST STATEMENT

The author declares that they have no competing interests.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article.

CONSENT TO PARTICIPATE

Not applicable.

CONSENT FOR PUBLICATION

Not applicable.

ORCID

Mhlambululi Mafu https://orcid.org/0009-0000-6879-9531

REFERENCES

1. DiVincenzo, D.P.: The physical implementation of quantum computation. Fortschr. Phys. Prog. Phys. 48(9–11), 771–783 (2000). https://doi.org/10.1002/1521-3978(200009)48:9/11<771::aid-prop771>3.0.co;2-e
2. Gisin, N., Thew, R.: Quantum communication. Nat. Photonics 1(3), 165–171 (2007). https://doi.org/10.1038/nphoton.2007.22
3. Gisin, N., et al.: Quantum cryptography. Rev. Mod. Phys. 74(1), 145–195 (2002). https://doi.org/10.1103/revmodphys.74.145
4. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge: Cambridge University Press (2010)
5. Horodecki, R., et al.: Quantum entanglement. Rev. Mod. Phys. 81(2), 865–942 (2009). https://doi.org/10.1103/revmodphys.81.865
6. Bouwmeester, D., Zeilinger, A.: The physics of quantum information: basic concepts. In: The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation, pp. 1–14. Springer (2000)
7. Busch, P., Heinonen, T., Lahti, P.: Heisenberg's uncertainty principle. Phys. Rep. 452(6), 155–176 (2007). https://doi.org/10.1016/j.physrep.2007.05.006
8. Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. Nature 299(5886), 802–803 (1982). https://doi.org/10.1038/299802a0
9. Scarani, V., et al.: The security of practical quantum key distribution. Rev. Mod. Phys. 81(3), 1301–1350 (2009). https://doi.org/10.1103/revmodphys.81.1301
10. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21(2), 120–126 (1978). https://doi.org/10.1145/359340.359342
11. Renner, R., Wolf, R.: Quantum advantage in cryptography. AIAA J. 61(5), 1895–1910 (2023). https://doi.org/10.2514/1.j062267
12. Chen, L., Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R.A., Smith-Tone, D.: Report on Post-Quantum Cryptography, vol. 12. US Department of Commerce, National Institute of Standards and Technology … (2016). https://doi.org/10.6028/nist.ir.8105
13. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134. IEEE (1994)
14. Metcalf, B.J., et al.: Quantum teleportation on a photonic chip. Nat. Photonics 8(10), 770–774 (2014). https://doi.org/10.1038/nphoton.2014.217
15. Luo, W., et al.: Recent progress in quantum photonic chips for quantum communication and internet. Light Sci. Appl. 12(1), 175 (2023). https://doi.org/10.1038/s41377-023-01173-8
16. Bennett, C., Brassard, G.I.: In: Proceedings of the IEEE International Conference on Computers Systems and Signal Processing Bangalore India, pp. 175 (1984)
17. Pirandola, S., et al.: Advances in quantum cryptography. Adv. Opt. Photon. 12(4), 1012–1236 (2020). https://doi.org/10.1364/aop.361502
18. Ladd, T.D., et al.: Quantum computers. Nature 464(7285), 45–53 (2010). https://doi.org/10.1038/nature08812
19. Pompili, M., et al.: Realization of a multinode quantum network of remote solid-state qubits. Science 372(6539), 259–264 (2021). https://doi.org/10.1126/science.abg1919
20. Kimble, H.J.: The quantum internet. Nature 453(7198), 1023–1030 (2008). https://doi.org/10.1038/nature07127
21. Wehner, S., Elkouss, D., Hanson, R.: Quantum internet: a vision for the road ahead. Science 362(6412), eaam9288 (2018). https://doi.org/10.1126/science.aam9288
22. Sidhu, J.S., et al.: Advances in space quantum communications. IET Quantum Commun. 2(4), 182–217 (2021). https://doi.org/10.1049/qtc2.12015
23. Pirandola, S., Braunstein, S.L.: Physics: unite to build a quantum internet. Nature 532(7598), 169–171 (2016). https://doi.org/10.1038/532169a
24. Bennett, C.H., et al.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. 70(13), 1895–1899 (1993). https://doi.org/10.1103/physrevlett.70.1895
25. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. 59(3), 1829–1834 (1999). https://doi.org/10.1103/physreva.59.1829
26. Mohseni, M., et al.: Commercialize quantum technologies in five years. Nature 543(7644), 171–174 (2017). https://doi.org/10.1038/543171a
27. Gibney, E.: The quantum gold rush. Nature 574(7776), 22–24 (2019). https://doi.org/10.1038/d41586-019-02935-4
28. Bayerstadler, A., et al.: Industry quantum computing applications. EPJ Quantum Technol. 8(1), 25 (2021). https://doi.org/10.1140/epjqt/s40507-021-00114-x
29. van Deventer, O., et al.: Towards European standards for quantum technologies. EPJ Quantum Technol. 9(1), 33 (2022). https://doi.org/10.1140/epjqt/s40507-022-00150-1
30. T. I. O. for Standardization: ISO/IEC 23837-1:2023 information security security requirements, test and evaluation methods for quantum key distribution (2023)
31. Singh, A., et al.: Quantum internet—applications, functionalities, enabling technologies, challenges, and research directions. IEEE Commun. Surv. Tutorials 23(4), 2218–2247 (2021). https://doi.org/10.1109/comst.2021.3109944
32. Ramakrishnan, R.K., et al.: The quantum internet: a hardware review. J. Indian Inst. Sci. 103(2), 1–21 (2022). https://doi.org/10.1007/s41745-022-00336-7
33. Rohde, P.P.: The Quantum Internet: The Second Quantum Revolution. Cambridge University Press (2021)
34. Mafu, M., Senekane, M.: Quantum technology for development framework as a tool for science diplomacy. Front. Res. Metr. Anal. 8 (2023). https://doi.org/10.3389/frma.2023.1279376
35. Xu, Y., et al.: Artificial intelligence: a powerful paradigm for scientific research. Innovation 2(4), 100179 (2021). https://doi.org/10.1016/j.xinn.2021.100179
36. Shalev-Shwartz, S., Ben-David, S.: Understanding Machine Learning: From Theory to Algorithms. Cambridge University Press (2014)
37. Davenport, T.H., Ronanki, R.: Artificial intelligence for the real world. Harv. Bus. Rev. 96(1), 108–116 (2018)
38. Harrington, P.: Machine Learning in Action. Simon and Schuster (2012)
39. Lloyd, S.: Quantum machine learning for data classification. Physics 14, 79 (2021). https://doi.org/10.1103/physics.14.79

40. Schuld, M., Petruccione, F.: Machine Learning with Quantum Computers. Springer (2021)
41. Dean, J.: Big Data, Data Mining, and Machine Learning: Value Creation for Business Leaders and Practitioners. John Wiley & Sons (2014)
42. Wang, M.: CAS center for excellence in quantum information and quantum physics: exploring frontiers of quantum physics and quantum technology. Natl. Sci. Rev. 4(1), 144–152 (2017). https://doi.org/10.1093/nsr/nwx025
43. Hasan, S.R., et al.: Quantum communication systems: vision, protocols, applications, and challenges. IEEE Access 11, 15855–15877 (2023). https://doi.org/10.1109/access.2023.3244395
44. Bin, Y., Changwei, H., Xizheng, Y.: Research on business support system of quantum communication. Inf. Commun. Technol. Policy 45(9), 72 (2019)
45. Khan, F.S., La Torre, D.: Quantum information technology and innovation: a brief history, current state and future perspectives for business and management. Technol. Anal. Strat. Manag. 33(11), 1281–1289 (2021). https://doi.org/10.1080/09537325.2021.1991576
46. Humble, T.: Consumer applications of quantum computing: a promising approach for secure computation, trusted data storage, and efficient applications. IEEE Consum. Electron. Mag. 7(6), 8–14 (2018). https://doi.org/10.1109/mce.2017.2755298
47. Sotelo, R.: Quantum in consumer technology. IEEE Consum. Electron. Mag. 12(5), 4–7 (2023). https://doi.org/10.1109/mce.2023.3249402
48. Fox, M.F., Zwickl, B.M., Lewandowski, H.: Preparing for the quantum revolution: what is the role of higher education? Phys. Rev. Phys. Educ. Res. 16(2), 020131 (2020). https://doi.org/10.1103/physrevphyseducres.16.020131
49. Aiello, C.D., et al.: Achieving a quantum smart workforce. Quantum Sci. Technol. 6(3), 030501 (2021). https://doi.org/10.1088/2058-9565/abfa64
50. Dzurak, A.S., et al.: Development of an undergraduate quantum engineering degree. IEEE Trans. Quantum Eng. 3, 1–10 (2022). https://doi.org/10.1109/tqe.2022.3157338
51. Kaur, M., Venegas-Gomez, A.: Defining the quantum workforce landscape: a review of global quantum education initiatives. Opt. Eng. 61(8), 081806 (2022). https://doi.org/10.1117/1.oe.61.8.081806
52. Ahmed, S.A., Mohsin, M., Ali, S.M.Z.: Survey and technological analysis of laser and its defense applications. Defence Technol. 17(2), 583–592 (2021). https://doi.org/10.1016/j.dt.2020.02.012
53. Krelina, M.: Quantum technology for military applications. EPJ Quantum Technol. 8(1), 24 (2021). https://doi.org/10.1140/epjqt/s40507-021-00113-y
54. Su, Y., Guo, Y., Huang, D.: Parameter optimization based BPNN of atmosphere continuous-variable quantum key distribution. Entropy 21(9), 908 (2019). https://doi.org/10.3390/e21090908
55. Wallnöfer, J., et al.: Machine learning for long-distance quantum communication. PRX Quantum 1(1), 010301 (2020). https://doi.org/10.1103/prxquantum.1.010301
56. Li, Z., et al.: Ensemble learning for failure prediction of underwater continuous variable quantum key distribution with discrete modulations. Phys. Lett. 419, 127694 (2021). https://doi.org/10.1016/j.physleta.2021.127694
57. Houssein, E.H., et al.: Machine learning in the quantum realm: the state-of-the-art, challenges, and future vision. Expert Syst. Appl. 194, 116512 (2022). https://doi.org/10.1016/j.eswa.2022.116512
58. Venketeswaran, A., et al.: Recent advances in machine learning for fiber optic sensor applications. Adv. Intell. Syst. 4(1), 2100067 (2022). https://doi.org/10.1002/aisy.202100067
59. Krenn, M., et al.: Artificial intelligence and machine learning for quantum technologies. Phys. Rev. 107(1), 010101 (2023). https://doi.org/10.1103/physreva.107.010101
60. Jin, D., et al.: Key-sifting algorithms for continuous-variable quantum key distribution. Phys. Rev. 104(1), 012616 (2021). https://doi.org/10.1103/physreva.104.012616
61. Rivest, R.L.: Cryptography and machine learning. In: International Conference on the Theory and Application of Cryptology, pp. 427–439. Springer (1991)
62. Zhang, H., et al.: Resource-efficient high-dimensional subspace teleportation with a quantum autoencoder. Sci. Adv. 8(40), eabn9783 (2022). https://doi.org/10.1126/sciadv.abn9783
63. Hu, X.-M., et al.: Progress in quantum teleportation. Nat. Rev. Phys. 5(6), 1–15 (2023). https://doi.org/10.1038/s42254-023-00588-x
64. Chen, Y., et al.: Detecting quantum entanglement with unsupervised learning. Quantum Sci. Technol. 7(1), 015005 (2021). https://doi.org/10.1088/2058-9565/ac310f
65. Liu, Y., et al.: Entanglement-based feature extraction by tensor network machine learning. Front. Appl. Math. Stat. 7, 716044 (2021). https://doi.org/10.3389/fams.2021.716044
66. Bai, S.-C., Tang, Y.-C., Ran, S.-J.: Unsupervised recognition of informative features via tensor network machine learning and quantum entanglement variations. Chin. Phys. Lett. 39(10), 100701 (2022). https://doi.org/10.1088/0256-307x/39/10/100701
67. Pawłowski, J., Krawczyk, M.: Quantification of entanglement with siamese convolutional neural networks. *arXiv preprint arXiv:2210.07410* (2022)
68. Sheng, Y.-B., Zhou, L.: Distributed secure quantum machine learning. Sci. Bull. 62(14), 1025–1029 (2017). https://doi.org/10.1016/j.scib.2017.06.007
69. Reiß, S.D., van Loock, P.: Deep reinforcement learning for key distribution based on quantum repeaters. Phys. Rev. 108(1), 012406 (2023). https://doi.org/10.1103/physreva.108.012406
70. Marquardt, F.: Machine learning and quantum devices. SciPost Phys. Lecture Notes, 029 (2021). https://doi.org/10.21468/scipostphyslectnotes.29
71. Dawid, A., et al.: Modern applications of machine learning in quantum sciences. *arXiv preprint arXiv:2204.04198* (2022)
72. Pezzè, L., et al.: Machine learning for optical quantum metrology. Adv. Photon. 5(2), 020501 (2023). https://doi.org/10.1117/1.ap.5.2.020501
73. Suter, D., Álvarez, G.A.: Colloquium: protecting quantum information against environmental noise. Rev. Mod. Phys. 88(4), 041001 (2016). https://doi.org/10.1103/revmodphys.88.041001
74. Carrasquilla, J.: Machine learning for quantum matter. Adv. Phys. X 5(1), 1797528 (2020). https://doi.org/10.1080/23746149.2020.1797528
75. Gebhart, V., et al.: Learning quantum systems. Nat. Rev. Phys. 5(3), 141–156 (2023). https://doi.org/10.1038/s42254-022-00552-1
76. Zhu, Y., Yu, K.: Artificial intelligence (AI) for quantum and quantum for AI. Opt. Quantum Electron. 55(8), 697 (2023). https://doi.org/10.1007/s11082-023-04914-6
77. Fontanesi, G., et al.: Artificial intelligence for satellite communication and non-terrestrial networks: a survey. *arXiv preprint arXiv: 2304.13008* (2023)
78. Niemiec, M.: Error correction in quantum cryptography based on artificial neural networks. Quantum Inf. Process. 18(6), 174 (2019). https://doi.org/10.1007/s11128-019-2296-4
79. Lohani, S., Glasser, R.T.: Turbulence correction with artificial neural networks. Opt. Lett. 43(11), 2611–2614 (2018). https://doi.org/10.1364/ol.43.002611
80. You, C., et al.: Identification of light sources using machine learning. Appl. Phys. Rev. 7(2) (2020). https://doi.org/10.1063/1.5133846
81. Long, N.K., Malaney, R., Grant, K.J.: A survey of machine learning assisted continuous-variable quantum key distribution. Information 14(10), 553 (2023). https://doi.org/10.3390/info14100553
82. Dunjko, V., Briegel, H.J.: Machine learning & artificial intelligence in the quantum domain: a review of recent progress. Rep. Prog. Phys. 81(7), 074001 (2018). https://doi.org/10.1088/1361-6633/aab406
83. Mabena, C.M., Roux, F.S.: Quantum channel correction with twisted light using compressive sensing. Phys. Rev. 101(1), 013807 (2020). https://doi.org/10.1103/physreva.101.013807
84. Kundu, N.K., McKay, M.R., Mallik, R.K.: Machine-learning-based parameter estimation of Gaussian quantum states. IEEE Trans. Quantum Eng. 3, 1–13 (2021). https://doi.org/10.1109/tqe.2021.3137559
85. Cimini, V., et al.: Deep reinforcement learning for quantum multiparameter estimation. Adv. Photon. 5(1), 016005 (2023). https://doi.org/10.1117/1.ap.5.1.016005
86. Turing, A.M.: Computing Machinery and Intelligence. Springer (2009)

87. Solomonoff, R.J.: The time scale of artificial intelligence: reflections on social effects. Hum. Syst. Manag. 5(2), 149–153 (1985). https://doi.org/10.3233/hsm-1985-5207
88. Moor, J.: The Dartmouth college artificial intelligence conference: the next fifty years. AI Mag. 27(4), 87 (2006)
89. Rosch-Grace, D., Straub, J.: Analysis of the likelihood of quantum computing proliferation. Technol. Soc. 68, 101880 (2022). https://doi.org/10.1016/j.techsoc.2022.101880
90. Weiss, G.: Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence. MIT Press (1999)
91. Janiesch, C., Zschech, P., Heinrich, K.: Machine learning and deep learning. Electron. Mark. 31(3), 685–695 (2021). https://doi.org/10.1007/s12525-021-00475-2
92. Russell, S.J.: Artificial Intelligence a Modern Approach. Pearson Education, Inc. (2010)
93. Bishop, C.M., Nasrabadi, N.M.: Pattern Recognition and Machine Learning, vol. 4. Springer (2006). https://doi.org/10.1007/978-0-387-45528-0
94. Mehta, P., et al.: A high-bias, low-variance introduction to machine learning for physicists. Phys. Rep. 810, 1–124 (2019). https://doi.org/10.1016/j.physrep.2019.03.001
95. El Naqa, I., Murphy, M.J.: What Is Machine Learning? Springer (2015)
96. Muller, A.C., Guido, S.: Introduction to Machine Learning with Python. O'Reilly (2017)
97. Lake, B.M., et al.: Building machines that learn and think like people. Behav. Brain Sci. 40, e253 (2017). https://doi.org/10.1017/s0140525x16001837
98. Goodfellow, I., Bengio, Y., Courville, A.: Deep Learning. MIT Press (2016)
99. Das Sarma, S., Deng, D.-L., Duan, L.-M.: Machine learning meets quantum physics. Phys. Today 72(3), 48–54 (2019). https://doi.org/10.1063/pt.3.4164
100. Carleo, G., et al.: Machine learning and the physical sciences. Rev. Mod. Phys. 91(4), 045002 (2019). https://doi.org/10.1103/revmodphys.91.045002
101. Jiang, C., et al.: Machine learning paradigms for next-generation wireless networks. IEEE Wireless Commun. 24(2), 98–105 (2016). https://doi.org/10.1109/mwc.2016.1500356wc
102. Merrick, K.E., Maher, M.L.: Motivated Reinforcement Learning: Curious Characters for Multiuser Games. Springer Science & Business Media (2009)
103. Kaelbling, L.P., Littman, M.L., Moore, A.W.: Reinforcement learning: a survey. J. Artif. Intell. Res. 4, 237–285 (1996). https://doi.org/10.1613/jair.301
104. LeCun, Y., Bengio, Y., Hinton, G.: Deep learning. Nature 521(7553), 436–444 (2015). https://doi.org/10.1038/nature14539
105. Ma, W., et al.: Deep learning for the design of photonic structures. Nat. Photonics 15(2), 77–90 (2021). https://doi.org/10.1038/s41566-020-0685-y
106. Kraus, M., Feuerriegel, S., Oztekin, A.: Deep learning in business analytics and operations research: models, applications and managerial implications. Eur. J. Oper. Res. 281(3), 628–641 (2020). https://doi.org/10.1016/j.ejor.2019.09.018
107. Cleveland, W.S., Devlin, S.J., Grosse, E.: Regression by local fitting: methods, properties, and computational algorithms. J. Econom. 37(1), 87–114 (1988). https://doi.org/10.1016/0304-4076(88)90077-2
108. Aha, D.W., Kibler, D., Albert, M.K.: Instance-based learning algorithms. Mach. Learn. 6(1), 37–66 (1991). https://doi.org/10.1007/bf00153759
109. Bauer, F., Pereverzev, S., Rosasco, L.: On regularization algorithms in learning theory. J. Complex 23(1), 52–72 (2007). https://doi.org/10.1016/j.jco.2006.07.001
110. Kotsiantis, S.B.: Decision trees: a recent overview. Artif. Intell. Rev. 39(4), 261–283 (2013). https://doi.org/10.1007/s10462-011-9272-4
111. Snoek, J., Larochelle, H., Adams, R.P.: Practical Bayesian optimization of machine learning algorithms. Adv. Neural Inf. Process. Syst. 25 (2012)
112. Xu, R., Wunsch, D.: Survey of clustering algorithms. IEEE Trans. Neural Netw. 16(3), 645–678 (2005). https://doi.org/10.1109/tnn.2005.845141
113. Xu, D., Tian, Y.: A comprehensive survey of clustering algorithms. Ann. Data Sci. 2, 165–193 (2015). https://doi.org/10.1007/s40745-015-0040-1
114. Hassoun, M.H.: Fundamentals of Artificial Neural Networks. MIT Press (1995)
115. Jain, A.K., Mao, J., Mohiuddin, K.M.: Artificial neural networks: a tutorial. Computer 29(3), 31–44 (1996). https://doi.org/10.1109/2.485891
116. Gers, F.A., Schmidhuber, J., Cummins, F.: Learning to forget: continual prediction with LSTM. Neural Comput. 12(10), 2451–2471 (2000). https://doi.org/10.1162/089976600300015015
117. Raymer, M.L., et al.: Dimensionality reduction using genetic algorithms. IEEE Trans. Evol. Comput. 4(2), 164–171 (2000). https://doi.org/10.1109/4235.850656
118. Dietterich, T.G.: Ensemble methods in machine learning. In: International Workshop on Multiple Classifier Systems, pp. 1–15. Springer (2000)
119. Zibar, D., et al.: Advancing classical and quantum communication systems with machine learning. In: Optical Fiber Communication Conference, pp. W1K–1. Optica Publishing Group (2020)
120. Sharma, P., et al.: Deep reinforcement learning-based routing and resource assignment in quantum key distribution-secured optical networks. IET Quantum Commun. 4(3), 136–145 (2023). https://doi.org/10.1049/qtc2.12063
121. Khan, F.N., et al.: An optical communication's perspective on machine learning and its applications. J. Lightwave Technol. 37(2), 493–516 (2019). https://doi.org/10.1109/jlt.2019.2897313
122. Saif, W.S., et al.: Machine learning techniques for optical performance monitoring and modulation format identification: a survey. IEEE Commun. Surv. Tutorials 22(4), 2839–2882 (2020). https://doi.org/10.1109/comst.2020.3018494
123. Karanov, B., et al.: End-to-end deep learning of optical fiber communications. J. Lightwave Technol. 36(20), 4843–4855 (2018). https://doi.org/10.1109/jlt.2018.2865109
124. Kleis, S., Schaeffer, C.G.: Improving the secret key rate of coherent quantum key distribution with Bayesian inference. J. Lightwave Technol. 37(3), 722–728 (2018). https://doi.org/10.1109/jlt.2018.2877823
125. Zibar, D., et al.: Machine learning techniques in optical communication. J. Lightwave Technol. 34(6), 1442–1452 (2015). https://doi.org/10.1109/ecoc.2015.7341896
126. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. 67(6), 661–663 (1991). https://doi.org/10.1103/physrevlett.67.661
127. Mafu, M., Senekane, M.: Security of quantum key distribution protocols. In: Advanced Technologies of Quantum Key Distribution. IntechOpen (2018)
128. Karabo, K., et al.: A novel quantum key distribution resistant against large-pulse attacks. IET Quantum Commun. (2024). https://doi.org/10.1049/qtc2.12089
129. Liu, R., et al.: Towards the industrialisation of quantum key distribution in communication networks: a short survey. IET Quantum Commun. 3(3), 151–163 (2022). https://doi.org/10.1049/qtc2.12044
130. Busch, P., Lahti, P.J., Mittelstaedt, P.: The Quantum Theory of Measurement. Springer (1996)
131. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. 28(4), 656–715 (1949). https://doi.org/10.1002/j.1538-7305.1949.tb00928.x
132. Scarani, V., Kurtsiefer, C.: The black paper of quantum cryptography: real implementation problems. Theor. Comput. Sci. 560, 27–32 (2014). https://doi.org/10.1016/j.tcs.2014.09.015
133. Diamanti, E., et al.: Practical challenges in quantum key distribution. npj Quantum Inf. 2(1), 1–12 (2016). https://doi.org/10.1038/npjqi.2016.25
134. Brassard, G., et al.: Limitations on practical quantum cryptography. Phys. Rev. Lett. 85(6), 1330–1333 (2000). https://doi.org/10.1103/physrevlett.85.1330
135. Grosshans, F., Grangier, P.: Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. 88(5), 057902 (2002). https://doi.org/10.1103/physrevlett.88.057902

136. Lo, H.-K., Ma, X., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. 94(23), 230504 (2005). https://doi.org/10.1142/9789812701633_0013
137. Mayers, D., Yao, A.: Quantum cryptography with imperfect apparatus. In: Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280), pp. 503–509. IEEE (1998)
138. Lucamarini, M., et al.: Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature 557(7705), 400–403 (2018). https://doi.org/10.1038/s41586-018-0066-6
139. Portmann, C., Renner, R.: Security in quantum cryptography. Rev. Mod. Phys. 94(2), 025008 (2022). https://doi.org/10.1103/revmodphys.94.025008
140. Ekert, A., Renner, R.: The ultimate physical limits of privacy. Nature 507(7493), 443–447 (2014). https://doi.org/10.1038/nature13132
141. Sekga, C., Mafu, M., Senekane, M.: High-dimensional quantum key distribution implemented with biphotons. Sci. Rep. 13(1), 1229 (2023). https://doi.org/10.1038/s41598-023-28382-w
142. Sekga, C., Mafu, M.: Tripartite quantum key distribution implemented with imperfect sources. Optics 3(3), 191–208 (2022). https://doi.org/10.3390/opt3030019
143. Garapo, K., Mafu, M., Petruccione, F.: Intercept-resend attack on six-state quantum key distribution over collective-rotation noise channels. Chin. Phys. B 25(7), 070303 (2016). https://doi.org/10.1088/1674-1056/25/7/070303
144. Mafu, M., Garapo, K., Petruccione, F.: Finite-key-size security of the Phoenix-Barnett-Chefles 2000 quantum-key-distribution protocol. Phys. Rev. 90(3), 032308 (2014). https://doi.org/10.1103/physreva.90.032308
145. Lütkenhaus, N.: Security against individual attacks for realistic quantum key distribution. Phys. Rev. 61(5), 052304 (2000). https://doi.org/10.1103/physreva.61.052304
146. Matsuura, T., et al.: Finite-size security of continuous-variable quantum key distribution with digital signal processing. Nat. Commun. 12(1), 252 (2021). https://doi.org/10.1038/s41467-020-19916-1
147. Sekga, C., Mafu, M.: Security of quantum-key-distribution protocol by using the post-selection technique. Phys. Open 7, 100075 (2021). https://doi.org/10.1016/j.physo.2021.100075
148. Coles, P.J., Metodiev, E.M., Lütkenhaus, N.: Numerical approach for unstructured quantum key distribution. Nat. Commun. 7(1), 11712 (2016). https://doi.org/10.1038/ncomms11712
149. Winick, A., Lütkenhaus, N., Coles, P.J.: Reliable numerical key rates for quantum key distribution. Quantum 2, 77 (2018). https://doi.org/10.22331/q-2018-07-26-77
150. Lin, J., Lütkenhaus, N.: Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution. Phys. Rev. Appl. 14(6), 064030 (2020). https://doi.org/10.1103/physrevapplied.14.064030
151. Tan, E.Y.-Z., et al.: Computing secure key rates for quantum cryptography with untrusted devices. npj Quantum Inf. 7(1), 158 (2021). https://doi.org/10.1038/s41534-021-00494-z
152. Gottesman, D., et al.: Security of quantum key distribution with imperfect devices. In: International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings, pp. 136. IEEE (2004)
153. Sekga, C., Mafu, M.: Reference frame independent twin field quantum key distribution with source flaws. J. Phys. Commun. 5(4), 045008 (2021). https://doi.org/10.1088/2399-6528/abf472
154. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. 85(2), 441–444 (2000). https://doi.org/10.1103/physrevlett.85.441
155. Briegel, H.-J., et al.: Quantum repeaters: the role of imperfect local operations in quantum communication. Phys. Rev. Lett. 81(26), 5932–5935 (1998). https://doi.org/10.1103/physrevlett.81.5932
156. Sangouard, N., et al.: Quantum repeaters based on atomic ensembles and linear optics. Rev. Mod. Phys. 83(1), 33–80 (2011). https://doi.org/10.1103/revmodphys.83.33
157. Pirandola, S.: End-to-end capacities of a quantum communication network. Commun. Phys. 2(1), 51 (2019). https://doi.org/10.1038/s42005-019-0147-3
158. Denys, A., Brown, P., Leverrier, A.: Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. Quantum 5, 540 (2021). https://doi.org/10.22331/q-2021-09-13-540
159. Lupo, C., Ouyang, Y.: Quantum key distribution with nonideal heterodyne detection: composable security of discrete-modulation continuous-variable protocols. PRX Quantum 3(1), 010341 (2022). https://doi.org/10.1103/prxquantum.3.010341
160. Ding, C., et al.: Machine-learning-based detection for quantum hacking attacks on continuous-variable quantum-key-distribution systems. Phys. Rev. 107(6), 062422 (2023). https://doi.org/10.1103/physreva.107.062422
161. Jain, N., et al.: Device calibration impacts security of quantum key distribution. Phys. Rev. Lett. 107(11), 110501 (2011). https://doi.org/10.1103/physrevlett.107.110501
162. Makarov, V., Anisimov, A., Skaar, J.: Effects of detector efficiency mismatch on security of quantum cryptosystems. Phys. Rev. 74(2), 022313 (2006). https://doi.org/10.1103/physreva.74.022313
163. Fung, C.-H.F., et al.: Security proof of quantum key distribution with detection efficiency mismatch. *arXiv preprint arXiv:0802.3788* (2008)
164. Zhang, Y., et al.: Security proof of practical quantum key distribution with detection-efficiency mismatch. Phys. Rev. Res. 3(1), 013076 (2021). https://doi.org/10.1103/physrevresearch.3.013076
165. Lo, H.-K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. 108(13), 130503 (2012). https://doi.org/10.1103/physrevlett.108.130503
166. Langenfeld, S., et al.: Quantum repeater node demonstrating unconditionally secure key distribution. Phys. Rev. Lett. 126(23), 230506 (2021). https://doi.org/10.1103/physrevlett.126.230506
167. Ren, Z.-A., et al.: Implementation of machine learning in quantum key distributions. IEEE Commun. Lett. 25(3), 940–944 (2020). https://doi.org/10.1109/lcomm.2020.3040212
168. Tang, G.-Z., Li, C.-Y., Wang, M.: Polarization discriminated time-bin phase-encoding measurement-device-independent quantum key distribution. Quantum Eng. 3(4), e79 (2021). https://doi.org/10.1002/que2.79
169. Okey, O.D., et al.: Quantum key distribution protocol selector based on machine learning for next-generation networks. Sustainability 14(23), 15901 (2022). https://doi.org/10.3390/su142315901
170. Hu, H., et al.: Robust interior point method for quantum key distribution rate computation. Quantum 6, 792 (2022). https://doi.org/10.22331/q-2022-09-08-792
171. Liu, Z.-P., et al.: Automated machine learning for secure key rate in discrete-modulated continuous-variable quantum key distribution. Opt. Express 30(9), 15024–15036 (2022). https://doi.org/10.1364/oe.455762
172. Zhou, M.-G., et al.: Neural network-based prediction of the secret-key rate of quantum key distribution. Sci. Rep. 12(1), 8879 (2022). https://doi.org/10.1038/s41598-022-12647-x
173. George, I., Lin, J., Lütkenhaus, N.: Numerical calculations of the finite key rate for general quantum key distribution protocols. Phys. Rev. Res. 3(1), 013274 (2021). https://doi.org/10.1103/physrevresearch.3.013274
174. Dong, Q., et al.: Optimization parameter prediction-based XGBoost of TF-QKD. Quantum Inf. Process. 21(7), 233 (2022). https://doi.org/10.1007/s11128-022-03579-6
175. Liu, W., et al.: Monitoring of continuous-variable quantum key distribution system in real environment. Opt Express 25(16), 19429–19443 (2017). https://doi.org/10.1364/oe.25.019429
176. Liu, W., et al.: Integrating machine learning to achieve an automatic parameter prediction for practical continuous-variable quantum key distribution. Phys. Rev. 97(2), 022316 (2018). https://doi.org/10.1103/physreva.97.022316
177. Li, J., et al.: Discrete-modulated continuous-variable quantum key distribution with a machine-learning-based detector. Opt. Eng. 57(6), 066109 (2018). https://doi.org/10.1117/1.oe.57.6.066109
178. Wang, W., Lo, H.-K.: Machine learning for optimal parameter prediction in quantum key distribution. Phys. Rev. 100(6), 062334 (2019). https://doi.org/10.1103/physreva.100.062334
179. Scarani, V., Renner, R.: Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-

way postprocessing. Phys. Rev. Lett. 100(20), 200501 (2008). https://doi.org/10.1103/physrevlett.100.200501
180. Mafu, M., Garapo, K., Petruccione, F.: Finite-size key in the Bennett 1992 quantum-key-distribution protocol for Rényi entropies. Phys. Rev. A 88(6), 062306 (2013). https://doi.org/10.1103/physreva.88.062306
181. Ding, H.-J., et al.: Predicting optimal parameters with random forest for quantum key distribution. Quantum Inf. Process. 19(2), 1–8 (2020). https://doi.org/10.1007/s11128-019-2548-3
182. Lu, F.-Y., et al.: Parameter optimization and real-time calibration of a measurement-device-independent quantum key distribution network based on a back propagation artificial neural network. JOSA B 36(3), B92–B98 (2019). https://doi.org/10.1364/josab.36.000b92
183. Liu, J.-Y., et al.: Practical phase-modulation stabilization in quantum key distribution via machine learning. Phys. Rev. Appl. 12(1), 014059 (2019). https://doi.org/10.1103/physrevapplied.12.014059
184. Mao, Y., et al.: Detecting quantum attacks: a machine learning based defense strategy for practical continuous-variable quantum key distribution. New J. Phys. 22(8), 083073 (2020). https://doi.org/10.1088/1367-2630/aba8d4
185. Zhang, S., et al.: Machine learning-assisted measurement device-independent quantum key distribution on reference frame calibration. Entropy 23(10), 1242 (2021). https://doi.org/10.3390/e23101242
186. Xu, F., Xu, H., Lo, H.-K.: Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. Phys. Rev. 89(5), 052333 (2014). https://doi.org/10.1103/physreva.89.052333
187. Ismail, Y., Sinayskiy, I., Petruccione, F.: Integrating machine learning techniques in quantum communication to characterize the quantum channel. JOSA B 36(3), B116–B121 (2019). https://doi.org/10.1364/josab.36.00b116
188. Lollie, M.L., et al.: High-dimensional encryption in optical fibers using spatial modes of light and machine learning. Mach. Learn. Sci. Technol. 3(3), 035006 (2022). https://doi.org/10.1088/2632-2153/ac7f1b
189. Ou, Y., et al.: Field-trial of machine learning-assisted quantum key distribution (QKD) networking with SDN. In: 2018 European Conference on Optical Communication (ECOC), pp. 1–3. IEEE (2018)
190. Khan, F.N., Lu, C., Lau, A.P.T.: Machine learning methods for optical communication systems. In: Signal Processing in Photonic Communications, pp. SpW2F–3. Optica Publishing Group (2017)
191. Sekga, C., Mafu, M.: Three-party reference frame independent quantum key distribution protocol. Chin. Phys. B 30(12), 120301 (2021). https://doi.org/10.1088/1674-1056/abff1f
192. Liao, Q., et al.: Multi-label learning for improving discretely-modulated continuous-variable quantum key distribution. New J. Phys. 22(8), 083086 (2020). https://doi.org/10.1088/1367-2630/abab3c
193. Zhu, Y., et al.: Passive continuous variable quantum key distribution through the oceanic turbulence. Entropy 25(2), 307 (2023). https://doi.org/10.3390/e25020307
194. Huang, D., Liu, S., Zhang, L.: Secure continuous-variable quantum key distribution with machine learning. In: Photonics, vol. 8(11), p. 511. MDPI (2021). https://doi.org/10.3390/photonics8110511
195. Bouwmeester, D., et al.: Experimental quantum teleportation. Nature 390(6660), 575–579 (1997). https://doi.org/10.1038/37539
196. Braunstein, S.L., Kimble, H.J.: Teleportation of continuous quantum variables. Phys. Rev. Lett. 80(4), 869–872 (1998). https://doi.org/10.1103/physrevlett.80.869
197. Bell, J.S.: On the problem of hidden variables in quantum mechanics. Rev. Mod. Phys. 38(3), 447–452 (1966). https://doi.org/10.1103/revmodphys.38.447
198. Reid, M., et al.: Colloquium: the Einstein-Podolsky-Rosen paradox: from concepts to applications. Rev. Mod. Phys. 81(4), 1727–1751 (2009). https://doi.org/10.1103/revmodphys.81.1727
199. Pirandola, S., et al.: Advances in quantum teleportation. Nat. Photonics 9(10), 641–652 (2015). https://doi.org/10.1038/nphoton.2015.154
200. Bruzewicz, C.D., et al.: Trapped-ion quantum computing: progress and challenges. Appl. Phys. Rev. 6(2) (2019). https://doi.org/10.1063/1.5088164
201. Nölleke, C., et al.: Efficient teleportation between remote single-atom quantum memories. Phys. Rev. Lett. 110(14), 140403 (2013). https://doi.org/10.1103/physrevlett.110.140403
202. Flamini, F., Spagnolo, N., Sciarrino, F.: Photonic quantum information processing: a review. Rep. Prog. Phys. 82(1), 016001 (2018). https://doi.org/10.1088/1361-6633/aad5b2
203. Kim, Y.-H., Kulik, S.P., Shih, Y.: Quantum teleportation of a polarization state with a complete Bell state measurement. Phys. Rev. Lett. 86(7), 1370–1373 (2001). https://doi.org/10.1103/physrevlett.86.1370
204. Marcikic, I., et al.: Long-distance teleportation of qubits at telecommunication wavelengths. Nature 421(6922), 509–513 (2003). https://doi.org/10.1038/nature01376
205. Landry, O., et al.: Quantum teleportation over the Swisscom telecommunication network. JOSA B 24(2), 398–403 (2007). https://doi.org/10.1364/josab.24.000398
206. Bao, X.-H., et al.: Quantum teleportation between remote atomic-ensemble quantum memories. Proc. Natl. Acad. Sci. USA 109(50), 20347–20351 (2012). https://doi.org/10.1073/pnas.1207329109
207. Reindl, M., et al.: All-photonic quantum teleportation using on-demand solid-state quantum emitters. Sci. Adv. 4(12), eaau1255 (2018). https://doi.org/10.1126/sciadv.aau1255
208. Gao, W., et al.: Quantum teleportation from a propagating photon to a solid-state spin qubit. Nat. Commun. 4(1), 2744 (2013). https://doi.org/10.1038/ncomms3744
209. Nielsen, M.A., Knill, E., Laflamme, R.: Complete quantum teleportation using nuclear magnetic resonance. Nature 396(6706), 52–55 (1998). https://doi.org/10.1038/23891
210. Huo, M., et al.: Deterministic quantum teleportation through fiber channels. Sci. Adv. 4(10), eaas9401 (2018). https://doi.org/10.1126/sciadv.aas9401
211. Furusawa, A., et al.: Unconditional quantum teleportation. Science 282(5389), 706–709 (1998). https://doi.org/10.1126/science.282.5389.706
212. Ursin, R., et al.: Quantum teleportation across the Danube. Nature 430(7002), 849 (2004). https://doi.org/10.1038/430849a
213. Valivarthi, R., et al.: Teleportation systems toward a quantum internet. PRX Quantum 1(2), 020317 (2020). https://doi.org/10.1103/prxquantum.1.020317
214. Takesue, H., et al.: Quantum teleportation over 100 km of fiber using highly efficient superconducting nanowire single-photon detectors. Optica 2(10), 832–835 (2015). https://doi.org/10.1364/optica.2.000832
215. Zhao, H., et al.: Real time deterministic quantum teleportation over 10 km of single optical fiber channel. Opt. Express 30(3), 3770–3782 (2022). https://doi.org/10.1364/oe.447603
216. Wang, X.-L., et al.: Quantum teleportation of multiple degrees of freedom of a single photon. Nature 518(7540), 516–519 (2015). https://doi.org/10.1038/nature14246
217. Riebe, M., et al.: Deterministic quantum teleportation with atoms. Nature 429(6993), 734–737 (2004). https://doi.org/10.1038/nature02570
218. Barrett, M., et al.: Deterministic quantum teleportation of atomic qubits. Nature 429(6993), 737–739 (2004). https://doi.org/10.1038/nature02608
219. Häffner, H., Roos, C.F., Blatt, R.: Quantum computing with trapped ions. Phys. Rep. 469(4), 155–203 (2008). https://doi.org/10.1016/j.physrep.2008.09.003
220. Yin, J., et al.: Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. Nature 488(7410), 185–188 (2012). https://doi.org/10.1038/nature11332
221. Li, B., et al.: Quantum state transfer over 1200 km assisted by prior distributed entanglement. Phys. Rev. Lett. 128(17), 170501 (2022). https://doi.org/10.1103/physrevlett.128.170501
222. Ren, J.-G., et al.: Ground-to-satellite quantum teleportation. Nature 549(7670), 70–73 (2017). https://doi.org/10.1038/nature23675
223. Ma, X.-S., et al.: Quantum teleportation over 143 kilometres using active feed-forward. Nature 489(7415), 269–273 (2012). https://doi.org/10.1038/nature11472

224. Bennett, C.H., et al.: Purification of noisy entanglement and faithful teleportation via noisy channels. Phys. Rev. Lett. 76(5), 722–725 (1996). https://doi.org/10.1103/physrevlett.76.722
225. Xia, X.-X., et al.: Long distance quantum teleportation. Quantum Sci. Technol. 3(1), 014012 (2017). https://doi.org/10.1088/2058-9565/aa9baf
226. Simon, C.: Towards a global quantum network. Nat. Photonics 11(11), 678–680 (2017). https://doi.org/10.1038/s41566-017-0032-0
227. Cacciapuoti, A.S., et al.: When entanglement meets classical communications: quantum teleportation for the quantum internet. IEEE Trans. Commun. 68(6), 3808–3833 (2020). https://doi.org/10.1109/tcomm.2020.2978071
228. Cao, Y., et al.: The evolution of quantum key distribution networks: on the road to the Qinternet. IEEE Commun. Surv. Tutorials 24(2), 839–894 (2022). https://doi.org/10.1109/comst.2022.3144219
229. Zukowski, M., et al.: "Event-ready-detectors" Bell experiment via entanglement swapping. Phys. Rev. Lett. 71(26), 4287–4290 (1993). https://doi.org/10.1103/physrevlett.71.4287
230. Pirandola, S., et al.: Macroscopic entanglement by entanglement swapping. Phys. Rev. Lett. 97(15), 150403 (2006). https://doi.org/10.1103/physrevlett.97.150403
231. Takeda, S., et al.: Entanglement swapping between discrete and continuous variables. Phys. Rev. Lett. 114(10), 100501 (2015). https://doi.org/10.1103/physrevlett.114.100501
232. Wang, T.-J., Yang, G.-Q., Wang, C.: Control power of high-dimensional controlled teleportation. Phys. Rev. 101(1), 012323 (2020). https://doi.org/10.1103/physreva.101.012323
233. Barasiński, A., Černoch, A., Lemr, K.: Demonstration of controlled quantum teleportation for discrete variables on linear optical devices. Phys. Rev. Lett. 122(17), 170501 (2019). https://doi.org/10.1103/physrevlett.122.170501
234. Lance, A.M., et al.: Tripartite quantum state sharing. Phys. Rev. Lett. 92(17), 177903 (2004). https://doi.org/10.1103/physrevlett.92.177903
235. Bužek, V., Hillery, M.: Quantum copying: beyond the no-cloning theorem. Phys. Rev. 54(3), 1844–1852 (1996). https://doi.org/10.1103/physreva.54.1844
236. Yonezawa, H., Aoki, T., Furusawa, A.: Demonstration of a quantum teleportation network for continuous variables. Nature 431(7007), 430–433 (2004). https://doi.org/10.1038/nature02858
237. Ishizaka, S., Hiroshima, T.: Asymptotic teleportation scheme as a universal programmable quantum processor. Phys. Rev. Lett. 101(24), 240501 (2008). https://doi.org/10.1103/physrevlett.101.240501
238. Ishizaka, S., Hiroshima, T.: Quantum teleportation scheme by selecting one of multiple output ports. Phys. Rev. 79(4), 042306 (2009). https://doi.org/10.1103/physreva.79.042306
239. Gottesman, D., Chuang, I.L.: Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. Nature 402(6760), 390–393 (1999). https://doi.org/10.1038/46503
240. Aliferis, P., Leung, D.W.: Computation by measurements: a unifying picture. Phys. Rev. 70(6), 062314 (2004). https://doi.org/10.1103/physreva.70.062314
241. Lu, S., et al.: Separability-entanglement classifier via machine learning. Phys. Rev. 98(1), 012315 (2018). https://doi.org/10.1103/physreva.98.012315
242. Asif, N., et al.: Entanglement detection with artificial neural networks. Sci. Rep. 13(1), 1562 (2023). https://doi.org/10.1038/s41598-023-28745-3
243. Boerkamp, M.: Quantum computer creates wormhole analogue. Phys. World 36(1), 6 (2023). https://doi.org/10.1088/2058-7058/36/01/06
244. Luo, Y.-H., et al.: Quantum teleportation in high dimensions. Phys. Rev. Lett. 123(7), 070505 (2019). https://doi.org/10.1103/physrevlett.123.070505
245. Hu, X.-M., et al.: Experimental high-dimensional quantum teleportation. Phys. Rev. Lett. 125(23), 230501 (2020). https://doi.org/10.1103/physrevlett.125.230501
246. Erhard, M., Krenn, M., Zeilinger, A.: Advances in high-dimensional quantum entanglement. Nat. Rev. Phys. 2(7), 365–381 (2020). https://doi.org/10.1038/s42254-020-0193-5
247. McCutcheon, W., et al.: Experimental verification of multipartite entanglement in quantum networks. Nat. Commun. 7(1), 13251 (2016). https://doi.org/10.1038/ncomms13251
248. Calsamiglia, J.: Generalized measurements by linear elements. Phys. Rev. 65(3), 030301 (2002). https://doi.org/10.1103/physreva.65.030301
249. Zhong, H.-S., et al.: 12-photon entanglement and scalable scattershot boson sampling with optimal entangled-photon pairs from parametric down-conversion. Phys. Rev. Lett. 121(25), 250505 (2018). https://doi.org/10.1103/physrevlett.121.250505
250. Qiu, X., et al.: Optical vortex copier and regenerator in the Fourier domain. Photon. Res. 6(6), 641–646 (2018). https://doi.org/10.1364/prj.6.000641
251. Kaneda, F., Kwiat, P.G.: High-efficiency single-photon generation via large-scale active time multiplexing. Sci. Adv. 5(10), eaaw8586 (2019). https://doi.org/10.1126/sciadv.aaw8586
252. Schimpf, C., et al.: Quantum dots as potential sources of strongly entangled photons: perspectives and challenges for applications in quantum networks. Appl. Phys. Lett. 118(10) (2021). https://doi.org/10.1063/5.0038729
253. Lu, J., et al.: Ultralow-threshold thin-film lithium niobate optical parametric oscillator. Optica 8(4), 539–544 (2021). https://doi.org/10.1364/optica.418984
254. Ringbauer, M., et al.: A universal qudit quantum processor with trapped ions. Nat. Phys. 18(9), 1053–1057 (2022). https://doi.org/10.1038/s41567-022-01658-0
255. Fu, Y., et al.: Experimental investigation of quantum correlations in a two-qutrit spin system. Phys. Rev. Lett. 129(10), 100501 (2022). https://doi.org/10.1103/physrevlett.129.100501
256. Goss, N., et al.: High-fidelity qutrit entangling gates for superconducting circuits. Nat. Commun. 13(1), 7481 (2022). https://doi.org/10.1038/s41467-022-34851-z
257. Xu, J., et al.: Machine learning assisted prediction for free-space continuous variable quantum teleportation. IEEE Photon. J. 14(4), 1–7 (2022). https://doi.org/10.1109/jphot.2022.3186391
258. Shamir, A.: How to share a secret. Commun. ACM 22(11), 612–613 (1979). https://doi.org/10.1145/359168.359176
259. Blakley, G.R.: Safeguarding cryptographic keys. In: Managing Requirements Knowledge, International Workshop on, pp. 313. IEEE Computer Society (1979)
260. Cleve, R., Gottesman, D., Lo, H.-K.: How to share a quantum secret. Phys. Rev. Lett. 83(3), 648–651 (1999). https://doi.org/10.1103/physrevlett.83.648
261. Sekga, C., Mafu, M.: Quantum state sharing of an arbitrary m-particle state using Einstein–Podolsky–Rosen pairs and application in quantum voting. Mod. Phys. Lett. 36(21), 2150151 (2021). https://doi.org/10.1142/s0217732321501510
262. Al Ebri, N., Baek, J., Yeun, C.Y.: Study on secret sharing schemes (SSS) and their applications. In: 2011 International Conference for Internet Technology and Secured Transactions, pp. 40–45. IEEE (2011)
263. Chor, B., et al.: Verifiable secret sharing and achieving simultaneity in the presence of faults. In: 26th Annual Symposium on Foundations of Computer Science (SFCS 1985), pp. 383–395. IEEE (1985)
264. Beimel, A.: Secret-sharing schemes: a survey. In: International Conference on Coding and Cryptology, pp. 11–46. Springer (2011)
265. Cramer, R., Damgård, I., Maurer, U.: General secure multi-party computation from any linear secret-sharing scheme. In: International Conference on the Theory and Applications of Cryptographic Techniques, pp. 316–334. Springer (2000)
266. Cramer, R., Damgård, I.B.: Secure Multiparty Computation. Cambridge University Press (2015)
267. Goyal, R., Vaikuntanathan, V.: Locally verifiable signature and key aggregation. In: Annual International Cryptology Conference, pp. 761–791. Springer (2022)

268. Bellare, M., Neven, G.: Identity-based multi-signatures from RSA. In: Cryptographers' Track at the RSA Conference, pp. 145–162. Springer (2007)
269. Boldyreva, A., et al.: Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing. In: Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 276–285 (2007)
270. Goyal, V., et al.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 89–98 (2006)
271. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: 2007 IEEE Symposium on Security and Privacy (SP'07), pp. 321–334. IEEE (2007)
272. Gottesman, D.: Theory of quantum secret sharing. Phys. Rev. 61(4), 042311 (2000). https://doi.org/10.1103/physreva.61.042311
273. Zhang, Z.-J., Li, Y., Man, Z.-X.: Multiparty quantum secret sharing. Phys. Rev. 71(4), 044301 (2005). https://doi.org/10.1103/physreva.71.044301
274. Tavakoli, A., et al.: Secret sharing with a single d-level quantum system. Phys. Rev. 92(3), 030302 (2015). https://doi.org/10.1103/physreva.92.030302
275. Liu, L.-J., et al.: A quantum secret sharing scheme with verifiable function. Eur. Phys. J. D 74(7), 1–8 (2020). https://doi.org/10.1140/epjd/e2020-10010-3
276. Li, F., Yan, J., Zhu, S.: General quantum secret sharing scheme based on two qudit. Quantum Inf. Process. 20(10), 328 (2021). https://doi.org/10.1007/s11128-021-03270-2
277. Hsu, L.-Y., Li, C.-M.: Quantum secret sharing using product states. Phys. Rev. 71(2), 022321 (2005). https://doi.org/10.1103/physreva.71.022321
278. Mashhadi, S.: General secret sharing based on quantum Fourier transform. Quantum Inf. Process. 18(4), 114 (2019). https://doi.org/10.1007/s11128-019-2233-6
279. Tsai, C., Hwang, T.: Multi-party quantum secret sharing based on two special entangled states. Sci. China Phys. Mech. Astron. 55(3), 460–464 (2012). https://doi.org/10.1007/s11433-012-4633-9
280. Chong-Qiang, Y., et al.: Multiparty semi-quantum secret sharing with d-level single-particle states. Int. J. Theor. Phys. 58(11), 3797–3814 (2019). https://doi.org/10.1007/s10773-019-04248-8
281. Shi, R., et al.: Quantum secret sharing between multiparty and multiparty with Bell states and Bell measurements. Sci. China Phys. Mech. Astron. 53(12), 2238–2244 (2010). https://doi.org/10.1007/s11433-010-4181-0
282. Zhou, R.-G., et al.: Dynamic multiparty quantum secret sharing with a trusted party based on generalized GHZ state. IEEE Access 9, 22986–22995 (2021). https://doi.org/10.1109/access.2021.3055943
283. Yang, Y., Wen, Q.: Threshold quantum secret sharing between multiparty and multi-party. Sci China G Phys. Mech. Astron. 51(9), 1308–1315 (2008). https://doi.org/10.1007/s11433-008-0114-6
284. Senthoor, K., Sarvepalli, P.K.: Communication efficient quantum secret sharing. Phys. Rev. 100(5), 052313 (2019). https://doi.org/10.1103/physreva.100.052313
285. Wang, M.-M., Chen, X.-B., Yang, Y.-X.: Quantum secret sharing for general access structures based on multiparticle entanglements. Quantum Inf. Process. 13(2), 429–443 (2014). https://doi.org/10.1007/s11128-013-0660-3
286. Deng, F.-G., Zhou, H.-Y., Long, G.L.: Circular quantum secret sharing. J. Phys. Math. Gen. 39(45), 14089–14099 (2006). https://doi.org/10.1088/0305-4470/39/45/018
287. Yang, C.-W., Tsai, C.-W.: Efficient and secure dynamic quantum secret sharing protocol based on Bell states. Quantum Inf. Process. 19(5), 1–14 (2020). https://doi.org/10.1007/s11128-020-02662-0
288. Wang, T.-Y., et al.: Analysis of efficient and secure dynamic quantum secret sharing protocol based on Bell states. Quantum Inf. Process. 20, 1–10 (2021). https://doi.org/10.1007/s11128-020-02916-x
289. Tittel, W., Zbinden, H., Gisin, N.: Experimental demonstration of quantum secret sharing. Phys. Rev. 63(4), 042301 (2001). https://doi.org/10.1103/physreva.63.042301
290. Guo, G.-P., Guo, G.-C.: Quantum secret sharing without entanglement. Phys. Lett. 310(4), 247–251 (2003). https://doi.org/10.1016/s0375-9601(03)00074-4
291. Wang, M.-M., Tian, L.-T., Qu, Z.-G.: Efficient multiparty quantum secret sharing scheme in high-dimensional system. In: International Conference on Cloud Computing and Security, pp. 23–31. Springer (2018)
292. Gao, M., Yang, W., Liu, Y.: A novel quantum (t, n) threshold group signature based on d-dimensional quantum system. Quantum Inf. Process. 20, 1–13 (2021)
293. Hu, W., et al.: A novel dynamic quantum secret sharing in high-dimensional quantum system. Quantum Inf. Process. 20(5), 1–28 (2021). https://doi.org/10.1007/s11128-021-03103-2
294. Pinnell, J., et al.: Experimental demonstration of 11-dimensional 10-party quantum secret sharing. Laser Photon. Rev. 14(9), 2000012 (2020). https://doi.org/10.1002/lpor.202000012
295. Hai-Qiang, M., Ke-Jin, W., Jian-Hui, Y.: Experimental single qubit quantum secret sharing in a fiber network configuration. Opt. Lett. 38(21), 4494–4497 (2013). https://doi.org/10.1364/ol.38.004494
296. Choi, I., et al.: Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber. Opt. Express 22(19), 23121–23128 (2014). https://doi.org/10.1364/oe.22.023121
297. Wiesner, S.: Conjugate coding. ACM Sigact News 15(1), 78–88 (1983). https://doi.org/10.1145/1008908.1008920
298. Yin, H.-L., et al.: Experimental quantum secure network with digital signatures and encryption. Natl. Sci. Rev. 10(4), nwac228 (2023). https://doi.org/10.1093/nsr/nwac228
299. Chen, C.-Y., et al.: Quantum cryptography and its applications over the internet. IEEE Netw. 29(5), 64–69 (2015). https://doi.org/10.1109/mnet.2015.7293307
300. Tian, J.-H., Zhang, J.-Z., Li, Y.-P.: A voting protocol based on the controlled quantum operation teleportation. Int. J. Theor. Phys. 55(5), 2303–2310 (2016). https://doi.org/10.1007/s10773-015-2868-8
301. Tanuwidjaja, H.C., et al.: Privacy-preserving deep learning on machine learning as a service—a comprehensive survey. IEEE Access 8, 167425–167447 (2020). https://doi.org/10.1109/access.2020.3023084
302. Lindell, Y., Pinkas, B.: Privacy preserving data mining. J. Cryptol. 15(3), 177–206 (2002). https://doi.org/10.1007/s00145-001-0019-2
303. Senekane, M., Mafu, M., Taele, B.M.: Privacy-preserving quantum machine learning using differential privacy. In: 2017 IEEE AFRICON, pp. 1432–1435. IEEE (2017)
304. Yao, A.C.: Protocols for secure computations. In: 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982), pp. 160–164. IEEE (1982)
305. Rivest, R.L., et al.: On data banks and privacy homomorphisms. Found. Secure Comput. 4(11), 169–180 (1978)
306. Dwork, C.: Differential privacy. In: International Colloquium on Automata, Languages, and Programming, pp. 1–12. Springer (2006)
307. Dong, Y., et al.: Privacy-preserving distributed machine learning based on secret sharing. In: Information and Communications Security: 21st International Conference, ICICS 2019, Beijing, China, December 15–17, 2019, Revised Selected Papers 21, pp. 684–702. Springer (2020)
308. Wei, W., Tang, C., Chen, Y.: Efficient privacy-preserving K-means clustering from secret-sharing-based secure three-party computation. Entropy 24(8), 1145 (2022). https://doi.org/10.3390/e24081145
309. Araki, T., et al.: High-throughput semi-honest secure three-party computation with an honest majority. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 805–817 (2016)
310. Hegde, A., et al.: SoK: efficient privacy-preserving clustering. *Cryptology ePrint Archive* (2021)
311. Kozlowski, W., Dahlberg, A., Wehner, S.: Designing a quantum network protocol. In: Proceedings of the 16th International Conference on Emerging Networking Experiments and Technologies, pp. 1–16 (2020)
312. Van Meter, R., Touch, J.: Designing quantum repeater networks. IEEE Commun. Mag. 51(8), 64–71 (2013). https://doi.org/10.1109/mcom.2013.6576340

313. Van Meter, R., et al.: A quantum internet architecture. In: 2022 IEEE International Conference on Quantum Computing and Engineering (QCE), pp. 341–352. IEEE (2022)
314. Wei, S.-H., et al.: Towards real-world quantum networks: a review. Laser Photon. Rev. 16(3), 2100219 (2022). https://doi.org/10.1002/lpor.202100219
315. Kozlowski, W., Wehner, S.: Towards large-scale quantum networks. In: Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication, pp. 1–7 (2019)
316. Cao, Y., et al.: Multi-tenant secret-key assignment over quantum key distribution networks. Opt. Express 27(3), 2544–2561 (2019). https://doi.org/10.1364/oe.27.002544
317. Wang, J., et al.: Integrated photonic quantum technologies. Nat. Photonics 14(5), 273–284 (2020). https://doi.org/10.1038/s41566-019-0532-1
318. O'brien, J.L., Furusawa, A., Vučković, J.: Photonic quantum technologies. Nat. Photonics 3(12), 687–695 (2009). https://doi.org/10.1038/nphoton.2009.229
319. Kwek, L.-C., et al.: Chip-based quantum key distribution. AAPPS Bull. 31, 1–8 (2021). https://doi.org/10.1007/s43673-021-00017-0
320. Sibson, P., et al.: Integrated silicon photonics for high-speed quantum key distribution. Optica 4(2), 172–177 (2017). https://doi.org/10.1364/optica.4.000172
321. Ding, Y., et al.: High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. npj Quantum Inf. 3(1), 25 (2017). https://doi.org/10.1038/s41534-017-0026-2
322. Liu, Q., et al.: Advances in chip-based quantum key distribution. Entropy 24(10), 1334 (2022). https://doi.org/10.3390/e24101334
323. Chen, Y.-A., et al.: An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature 589(7841), 214–219 (2021). https://doi.org/10.1038/s41586-020-03093-8
324. Vergoossen, T., et al.: Modelling of satellite constellations for trusted node QKD networks. Acta Astronaut. 173, 164–171 (2020). https://doi.org/10.1016/j.actaastro.2020.02.010
325. Van Meter, R., et al.: Path selection for quantum repeater networks. Networking Sci. 3(1-4), 82–95 (2013). https://doi.org/10.1007/s13119-013-0026-2
326. Cirac, J.I., et al.: Quantum state transfer and entanglement distribution among distant nodes in a quantum network. Phys. Rev. Lett. 78(16), 3221–3224 (1997). https://doi.org/10.1103/physrevlett.78.3221
327. Chanelière, T., et al.: Storage and retrieval of single photons transmitted between remote quantum memories. Nature 438(7069), 833–836 (2005). https://doi.org/10.1038/nature04315
328. Le, L., et al.: Entanglement routing for quantum networks: a deep reinforcement learning approach. In: ICC 2022-IEEE International Conference on Communications (2022)
329. Damgård, I.B., et al.: Secure identification and QKD in the bounded-quantum-storage model. In: Advances in Cryptology-CRYPTO 2007: 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007. Proceedings 27, pp. 342–359. Springer (2007)
330. Fitzsimons, J.F.: Private quantum computation: an introduction to blind quantum computing and related protocols. npj Quantum Inf. 3(1), 23 (2017). https://doi.org/10.1038/s41534-017-0025-3
331. Broadbent, A.: Delegating private quantum computations. Can. J. Phys. 93(9), 941–946 (2015). https://doi.org/10.1139/cjp-2015-0030
332. Chuang, I.L.: Quantum algorithm for distributed clock synchronization. Phys. Rev. Lett. 85(9), 2006–2009 (2000). https://doi.org/10.1103/physrevlett.85.2006
333. Cuomo, D., Caleffi, M., Cacciapuoti, A.S.: Towards a distributed quantum computing ecosystem. IET Quantum Commun. 1(1), 3–8 (2020). https://doi.org/10.1049/iet-qtc.2020.0002
334. Illiano, J., et al.: Quantum internet protocol stack: a comprehensive survey. Comput. Netw. 213, 109092 (2022). https://doi.org/10.1016/j.comnet.2022.109092
335. Xia, Y., et al.: Quantum-enhanced data classification with a variational entangled sensor network. Phys. Rev. X 11(2), 021047 (2021). https://doi.org/10.1103/physrevx.11.021047
336. Pant, M., et al.: Routing entanglement in the quantum internet. npj Quantum Inf. 5(1), 25 (2019). https://doi.org/10.1038/s41534-019-0139-x
337. Coutinho, B.C., et al.: Robustness of noisy quantum networks. Commun. Phys. 5(1), 105 (2022). https://doi.org/10.1038/s42005-022-00866-7
338. Helsen, J., Wehner, S.: A benchmarking procedure for quantum networks. npj Quantum Inf. 9(1), 17 (2023). https://doi.org/10.1038/s41534-022-00628-x
339. Amirloo, J., Razavi, M., Majedi, A.H.: DLCZ quantum repeaters: rate and fidelity analysis. In: International Conference on Quantum Information, p. JMB54. Optica Publishing Group (2008)
340. Razavi, M., Farmanbar, H., Lütkenhaus, N.: Long-distance quantum communication with multiple quantum memories. In: Optical Fiber Communication Conference, p. JWA48. Optica Publishing Group (2008)
341. Yin, J., et al.: Satellite-based entanglement distribution over 1200 kilometers. Science 356(6343), 1140–1144 (2017). https://doi.org/10.1126/science.aan3211
342. Yin, J., et al.: Satellite-to-ground entanglement-based quantum key distribution. Phys. Rev. Lett. 119(20), 200501 (2017). https://doi.org/10.1103/physrevlett.119.200501
343. Wang, S., et al.: Twin-field quantum key distribution over 830-km fibre. Nat. Photonics 16(2), 154–161 (2022). https://doi.org/10.1038/s41566-021-00928-2
344. Sharma, P., et al.: Quantum key distribution secured optical networks: a survey. IEEE Open J. Commun. Soc. 2, 2049–2083 (2021). https://doi.org/10.1109/ojcoms.2021.3106659
345. Moghaddam, E.E., Beyranvand, H., Salehi, J.A.: Resource allocation in space division multiplexed elastic optical networks secured with quantum key distribution. IEEE J. Sel. Area. Commun. 39(9), 2688–2700 (2021). https://doi.org/10.1109/jsac.2021.3064641
346. Jia, J., et al.: Cost-optimization-based quantum key distribution over quantum key pool optical networks. Entropy 25(4), 661 (2023). https://doi.org/10.3390/e25040661
347. Niu, J., et al.: Noise-suppressing channel allocation in dynamic DWDM-QKD networks using lightgbm. Opt. Express 27(22), 31741–31756 (2019). https://doi.org/10.1364/oe.27.031741
348. Niu, J., et al.: Key-size-driven wavelength resource sharing scheme for QKD and the time-varying data services. J. Lightwave Technol. 39(9), 2661–2672 (2021). https://doi.org/10.1109/jlt.2021.3056109
349. Wang, R., et al.: AI-enabled large-scale entanglement distribution quantum networks. In: Optical Fiber Communication Conference, pp. Tu1I–4. Optica Publishing Group (2021)
350. Nejabati, R., Wang, R., Simeonidou, D.: Dynamic quantum network: from quantum data centre to quantum cloud computing. In: Optical Fiber Communication Conference, pp. Th3D–1. Optica Publishing Group (2022)
351. Bahrani, S., Razavi, M., Salehi, J.A.: Wavelength assignment in hybrid quantum-classical networks. Sci. Rep. 8(1), 3456 (2018). https://doi.org/10.1038/s41598-018-21418-6
352. Bahrani, S., et al.: Wavelength assignment in quantum access networks with hybrid wireless-fiber links. JOSA B 36(3), B99–B108 (2019). https://doi.org/10.1364/josab.36.000b99
353. Cao, Y., et al.: Reinforcement learning based multi-tenant secret-key assignment for quantum key distribution networks. In: 2019 Optical Fiber Communications Conference and Exhibition (OFC), pp. 1–3. IEEE (2019)
354. Sparkes, B., et al.: Gradient echo memory in an ultra-high optical depth cold atomic ensemble. New J. Phys. 15(8), 085027 (2013). https://doi.org/10.1088/1367-2630/15/8/085027
355. Mottola, R., Buser, G., Treutlein, P.: Optical memory in a microfabricated rubidium vapor cell. Phys. Rev. Lett. 131(26), 260801 (2023). https://doi.org/10.1103/physrevlett.131.260801

356. Cho, Y.-W., et al.: Highly efficient optical quantum memory with long coherence time in cold atoms. Optica 3(1), 100–107 (2016). https://doi.org/10.1364/optica.3.000100
357. Chen, Y.-H., et al.: Coherent optical memory with high storage efficiency and large fractional delay. Phys. Rev. Lett. 110(8), 083601 (2013). https://doi.org/10.1103/physrevlett.110.083601
358. Reim, K., et al.: Single-photon-level quantum memory at room temperature. Phys. Rev. Lett. 107(5), 053603 (2011). https://doi.org/10.1103/physrevlett.107.053603
359. Jobez, P., et al.: Coherent spin control at the quantum level in an ensemble-based optical memory. Phys. Rev. Lett. 114(23), 230502 (2015). https://doi.org/10.1103/physrevlett.114.230502
360. Sparkes, B., et al.: ac Stark gradient echo memory in cold atoms. Phys. Rev. 82(4), 043847 (2010). https://doi.org/10.1103/physreva.82.043847
361. Leung, A., et al.: Extending gradient echo memory using machine learning and single photons. In: Conference on Lasers and Electro-Optics/Pacific Rim, pp. Th1D–2. Optica Publishing Group (2018)
362. Buchler, B., et al.: Stopped and stationary light with cold atomic ensembles and machine learning. In: CLEO: QELS_Fundamental Science, pp. FM1G–5. Optica Publishing Group (2018)
363. Khatri, S.: Policies for elementary links in a quantum network. Quantum 5, 537 (2021). https://doi.org/10.22331/q-2021-09-07-537
364. Yun-Hong, G., et al.: Prediction and experimental verification for satellite-to-ground quantum communication key rate based on machine learning. J. Infrared Millim. Waves 40(3), 420–425 (2021)
365. Robertson, E., et al.: Machine learning optimal control pulses in an optical quantum memory. In: European Quantum Electronics Conference, p. eb_10_3. Optica Publishing Group (2023)
366. Shinbrough, K., Lorenz, V.O.: Variance-based sensitivity analysis of λ-type quantum memory. Phys. Rev. 107(3), 033703 (2023). https://doi.org/10.1103/physreva.107.033703
367. I. S. G. (SG13): Future networks. (2023)

How to cite this article: Mafu, M.: Advances in artificial intelligence and machine learning for quantum communication applications. IET Quant. Comm. 5(3), 202–231 (2024). https://doi.org/10.1049/qtc2.12094