Quantum secured 10-Gbit/s ethernet passive optical access network and its machine-learning-assisted implementation

Jia-Le Kang, Ming-Hui Zhang,* Xiao-Peng Liu, and Chen He
School of Information Science and Technology, Northwest University, Xi'an 710127, Shaanxi, People's Republic of China

(Received 15 September 2023; accepted 22 January 2024; published 26 February 2024)

The extension from point-to-point quantum key distribution (QKD) to multipoint communication is an inevitable trend toward the large-scale development of QKD networks. At present, it is a relatively simple and cost-effective implementation to integrate quantum access networks (QANs) into existing Ethernet passive optical access networks (EPONs). This work proposes a quantum secured 10 Gbit/s EPON (10G-EPON), in which a plug-and-play twin-field QKD (PnP-TF-QKD) architecture is developed, requiring a single untrusted laser and a pair of shared detectors. The PnP-TF-QKD implementation is compatible with standard 10G-EPON and can support up to 64 users. In addition, prior to the deployment of QKD on EPON, it is crucial to predict in advance whether the attainable QAN indicators, such as the secure key rate, the maximum feeder fiber length, etc., meet the requirements of a certain circumstance. However, this task is often complex and time consuming. Therefore, we present a machine-learning-based user-demand-oriented prediction model to facilitate the evaluation of QAN parameters. The plug-and-play twin-field quantum access network (PnP-TF-QAN) and its machine-learning-assisted implementation method provide guidance for further experiments and actual deployments of large-scale QANs.

DOI: 10.1103/PhysRevA.109.022617

I. INTRODUCTION

Quantum key distribution (QKD) access network is a promising solution for secure communication among multiple users [1–6]. Building a dedicated fiber network solely for quantum transmission will be cost-prohibitive. Nowadays, integrating quantum access networks (QANs) into existing classical Ethernet passive optical access networks (EPONs) would be a more practical and cost-effective solution [7–12]. EPON, deployed in optical access networks, connects optical network units (ONUs) to the nearest optical line terminal (OLT) [13] via a feeder fiber, a power-splitter, and several drop fibers [14,15]. However, the coexistence of QKD and EPON is greatly challenged due to various noises caused by classical signals with high power, such as Raman-scattering noise (SRS) and four-wave mixing noise (FWM) [16–18]. Among them, quantum signals are the most seriously interfered by SRS noise, which greatly limits the transmission distance and secure key rate of QKD [19,20].

Currently, QKD is usually integrated into EPON using two architectures [1,7–9]: uplink QAN (with a QKD receiver located at the OLT position) and downlink QAN (with a QKD receiver at each ONU side). For these existing coexistence schemes, the number of detectors or lasers will increase as the network capacity expands, and their actual implementation can lead to significant expenditures, posing a huge challenge for large-scale deployment. Generally, uplink integration experiences more SRS noise than downlink [7–9]. For an uplink QAN, a trusted laser source is required for each user [21,22]. However, this is not feasible for a practical quantum network with a large number of users. The potential security loophole of a laser source can bring huge risks to the entire network. For a downlink QAN, a pair of detectors should be set up at each user for independent measurement. The cost of network construction increases significantly since the number of detectors required varies linearly with the number of access users. Therefore, it is necessary to develop an economic coexistence scheme for QKD and EPON.

Inspired by bidirectional TF-QKDs [21,23–31], we propose a plug-and-play twin-field quantum access network (PnP-TF-QAN) architecture with a single untrusted source and two shared detectors. It completely removes the assumption of a trusted laser source for each user in uplink QAN and requires a single untrusted laser source located at the relay. The potential source imperfections play a crucial role in the final secure communication [32]. The security of our QAN in the presence of an unknown and untrusted source is ensured by its analogous architecture with that in Refs. [33,34], which had been formally demonstrated to be secure. In addition, unlike downlink QAN where each user has to prepare two detectors to perform the independent measurement, this architecture performs measurement via a relay in accordance with the principle of time division multiplexing (TDM). Therefore, PnP-TF-QAN can be realized with fewer common optical components and further flexibly implemented in a fiber network. Furthermore, as a bidirectional architecture, the system automatically compensates for any birefringent effects in optical fibers as well as polarization-related losses. Integrating the PnP-TF-QKD with a $1 \times N$ star topology into 10G-EPON, is the main innovation of this work, which is different from the existing simple point to point PnP-TF-QDK works [33]. Compared with a dedicated quantum access network [2–4], this coexistence scheme is more cost-effective since it does

*zhangmh@nwu.edu.cn

not require the construction of additional fibers solely for the transmission of quantum signals.

The proposed PnP-TF-QAN can be integrated into a classical 10G-EPON with a maximum of 64 users. Two alternative integration architectures are presented, a full coexistence scheme (classical and quantum signals sharing a feeder fiber and several drop fibers) and a partial coexistence scheme (classical and quantum signals just sharing drop fibers, while the feeder fiber is private). The full coexistence scheme suffers relatively large noise interference, and it can perform key distribution on 20.9 km of fiber by attenuating 10G-EPON signals to around −10.5 dBm. The partial coexistence scheme can realize a transmission distance of approximately 17.4 km under full-power 10G-EPON signals.

In addition, integrating QKD into a classical 10G-EPON can be approached in two scenarios. In the first scenario, QKD is integrated into an existing 10G-EPON with a predetermined topology. To maximize the key rate, several iterations are required to attenuate OLT power and find an appropriate attenuated value of 10G-EPON signals. The second scenario involves simultaneous deployment of QKD and 10G-EPON, where the number and location of users are fixed, but the OLT location is undetermined. This scenario typically includes two user requirements: (a) Achieving a longer transmission distance and maintaining a workable key rate. (b) Obtaining a higher key rate while compromising the transmission distance. Prior to the practical deployment of QKD, it is crucial to predict the QKD performance based on field conditions.

However, such prediction and evaluation are often time consuming and require expertise, especially when considering noise interference and equipment defects. For example, in the single-feeder fiber condition, assuming an initial OLT power of 4 dBm, a drop fiber length of 1 km, and a network capacity of 32 users, the realistic demand is for a longer transmission distance. The traditional method will take 1.25 s to obtain the maximum attenuation value of OLT ($P_{\mathrm{OLT}}^{\mathrm{opt}}$) and the longest feeder length L_F, as well as the key rate R and the spontaneous Raman-scattering noise (noise). The above time does not include the time spent on adjusting system devices in actual scenarios. In practice, each trial iteration usually takes a few minutes. Consequently, the total time consumed throughout the process is at least at the hour level when lots of trials are attempted.

To facilitate the field implementation, we give a user-demand-oriented prediction model based on machine learning, which can directly predict those QAN indicators with small deviations in a short time. This model offers a solution for early evaluation of large-scale QAN deployment. Under the same system assumptions in the last paragraph, the machine-learning method can effectively predict the relevant parameters with a mere time cost of 3.12×10^{-4} s. Therefore, at least five orders of magnitude time will be saved.

II. FULL COEXISTENCE SCHEME OF PNP-TF-QAN AND 10G-EPON

A. Full coexistence architecture

The full coexistence architecture of PnP-TF-QAN and 10G-EPON is shown in Fig. 1.

10G-EPON. In a standard 10G-EPON, classical downstream signals with a wavelength of 1578 nm emitted by OLT are broadcast to all ONUs through drop fibers. ONUs selectively receive downstream signals according to the logical link identifier (LLID). Each ONU is allowed to send upstream signals with a wavelength of 1270 nm to OLT in a certain allocated time slot. In general, the maximum length of feeder fiber is 20 km, while the length of drop fiber varies from several hundred meters to 1 km.

PnP-TF-QAN over a 10G-EPON. For quantum signals, we adopt a Sagnac-based plug-and-play (PnP) architecture to realize key distribution among multi-users. The security of such architecture can be guaranteed by using power and timing monitoring, which is an effective way to prevent most attacks using light injection [33,35–37]. For a Trojan-horse attack, Eve can replace the original pulse with a stronger one and estimate the initial phase value sent by Alice and Bob. Our scheme can detect such attacks through the pulse power monitoring unit. As the reflected signals containing phase information are attenuated, Eve will need to use higher energy pulses to eavesdrop on enough information from the reflected signals. In such a scenario, the power monitoring unit will trigger an alarm when the pulse energy surpasses the specified threshold. Moreover, the phase randomizer (PR) can effectively isolate Alice and Bob from any potential reference pulses Eve may have prepared in advance.

The indistinguishability in modes between photons can be automatically calibrated and stabilized with the PnP architecture. Some expensive and sophisticated devices, including an untrusted laser source and two detectors, are placed at Charlie station, and Alice and Bobs just need to prepare simple optical components for encoding [38–40]. The PnP-TF-QAN divides the channel by TDM, which means that Alice can distribute keys with the assigned Bob within a specific time slot, and the detector is occupied by them during this time slot. We further illustrate the signal flow in the PnP-TF-QAN over a 10G-EPON system through the following six steps, describing the communication cycle between Alice and Bob_1 as depicted in Fig. 1.

Step 1. Charlie generates a horizontally polarized laser pulse with a wavelength of 1550.12 nm, which experiences the least SRS noise [9,41]. The pulse is then divided into clockwise and counterclockwise pulses after passing through a 50 : 50 BS.

Step 2. The clockwise (counterclockwise) pulse travels through a PBS (a PBS and a power splitter) and reaches Alice (Bob_1). The remaining Bobs refrain from processing the incoming quantum signals until their designated time slots are reached.

Step 3. After the pulse is received, FM in Alice (Bob_1) reflects the pulse to a vertically polarized state. The reflected pulses directly pass through PM and IM without being modulated, preventing information leakage caused by bright pulses. The other components are located on Alice's (Bob's) side, including an optical filter (F) and a phase randomizer (PR). In addition, a monitoring unit consisting of $q/(1-q)$ BS and an intensity detector (ID) is included, ensuring the security of the QAN with an untrusted laser source. More details about how these components work can be found in Refs. [33,34].

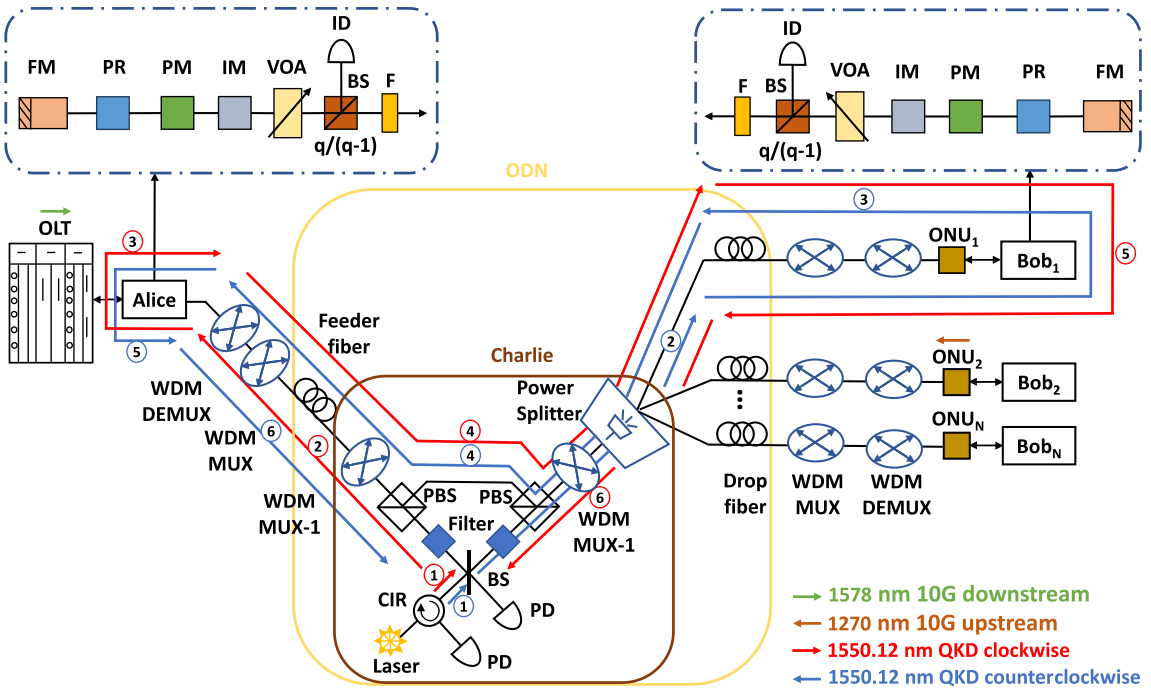

FIG. 1. Full coexistence architecture of PnP-TF-QAN and 10G-EPON. For a classical 10G-EPON, ONUs access the OLT via feeder and drop fibers as well as a power splitter. For the PnP-TF-QAN, the server (Alice) and multiple clients (Bobs) distribute keys via the optical distribution network (ODN). The modules located at Alice and Bob each contain a Faraday mirror (FM), a phase randomizer (PR), a phase modulator (PM), an intensity modulator (IM), a variable optical attenuator (VOA), a monitoring unit with a $q/(1-q)$ beam splitter (BS) and an intensity detector (ID), as well as an optical filter (F). The detection module and an untrusted laser source are located at the relay (Charlie), where the detection module consists of a beam splitter (BS) and two detectors (PD). PBS: polarization beam splitter, CIR: circulator, WDM MUX (DEMUX): wavelength division multiplexer (demultiplexer). The clockwise and counterclockwise pulses describing the quantum signal flow between Alice and Bob_1 are represented by the red solid lines with red numbers and blue solid lines with blue numbers, respectively.

Step 4. The vertically polarized clockwise (counterclockwise) pulses and classical downstream (upstream) signals emitted from OLT (ONU_1) are multiplexed by WDM MUX, respectively, and then transmitted to the counterpart Bob_1 (Alice). At this point, the WDM DEMUX at Alice's (Bob_1's) side works only when the counterclockwise (clockwise) multiplexed signals arrive. There is no drop fiber between WDM MUX and WDM DEMUX, and their positions are interchangeable. Here, the other two multiplexers (WDM MUX-1) serve the purpose of combining the quantum signals generated in the current round by the laser with the multiplexed signals from the previous rounds. If the quantum signals are not emitted, WDM MUX-1 does not work, and the multiplexed signals can directly pass through. Once the multiplexed signals arrive at Bob_1 (Alice), WDM DEMUX is used to separate quantum signals from classical signals and similarly the WDM MUX does not work at this time. After demultiplexing, classical signals achieve one downlink (uplink) transmission, and quantum clockwise (counterclockwise) pulse enters Bob_1's (Alice's) encoding module.

Step 5. Bob_1 (Alice) uses PM and IM to encode and modulate the arriving pulse and reflect them into horizontal polarization again via FM. The pulses are then attenuated to single-photon level with the VOA. If ONU_1 (OLT) is preparing to send classical upstream (downstream) signals at this time, the attenuated clockwise (counterclockwise) pulses are multiplexed with them, respectively.

Step 6. Clockwise and counterclockwise pulses finally interfere with each other at the Charlie station [21]. Since the clockwise and counterclockwise pulses pass through the same length of the fiber, they always reach Charlie at the same time and a high-visibility interference result can be observed. Here, the Filter device refers to a double-layer filter specifically designed to eliminate classical signals that may leak to Charlie when the multiplexed signals pass through PBS.

B. Noise analysis

According to the work in Ref. [9], classical signals at the wavelength of 1550.12 nm can be efficiently filtered with WDM MUX in coexistence systems, thus focusing only on nonlinear FWM and SRS noises. In general, FWM noise originating from ONUs and OLT can be neglected due to the substantial wavelength separation between classical signals and quantum signals [9,41–43]. SRS noise can be minimized by adjusting the spacing between classical signals to determine the optimal wavelength of quantum signals as well as regulating polarizations of the system [9,41]. There are two types of SRS: stimulated Raman-scattering noise (StRS) and spontaneous Raman-scattering noise (SnRS) [16,19,41]. StRS noise is generated when the power of input pulses exceeds the Raman threshold, which rarely occurs in normal communication. SnRS noise can be further divided into forward SnRS noise and backward SnRS noise according to the

propagation direction of photons. The effect of SnRS noise caused by ONUs is negligible since the wavelength interval between ONU signals and quantum signals is greater than 190 nm [9,44]. Therefore, SnRS noise caused by OLT is the main noise source for our coexistence architectures. For single-feeder fiber architecture, the powers of forward SnRS (denoted P_F^{SF}) and backward SnRS (denoted P_B^{SF}) caused by OLT signals can be described as [1,8,19,45]

$$P_F^{SF} = P_{\mathrm{OLT}}\beta\Delta\lambda\Delta t\frac{e^{-\alpha_q L}-e^{-\alpha_c L}}{\alpha_c-\alpha_q}, \tag{1}$$

$$P_B^{SF} = P_{\mathrm{OLT}}\beta\Delta\lambda\Delta t\frac{(1-e^{-(\alpha_c+\alpha_q)L})}{\alpha_c+\alpha_q}, \tag{2}$$

where L indicates the total length of coexistence fiber, including the feeder fiber L_F and drop fiber L_D, P_{OLT} is the power of OLT signals, β is the Raman-scattering coefficient, $\Delta\lambda$ is the bandwidth of quantum channel, Δt is the time-filtering coefficient of detector, α_q and α_c represent the fiber attenuation coefficients of quantum and classical OLT signals, respectively.

C. Simulation results of full coexistence scheme

Simulation parameters of the 10G-EPON. According to the IEEE 802.3av standard, for 10G-EPON, the central wavelength of downstream and upstream classical signals is 1578 and 1270 nm, respectively. The original OLT power ranges from 2 to 7 dBm, here is 3.4 dBm for simulation. The detection threshold of ONUs is −33 dBm. The attenuation coefficients of OLT and ONU are 0.31 and 0.57 dB/km, respectively. The insertion losses of other components are 0.5 dB (PBS), 4 dB (BS), 0.5 dB (CIR), 1.5 dB (WDM MUX and WDM DEMUX), and 2.5 dB (Filter). The insertion losses of 1 : 4, 1 : 8, 1 : 16, 1 : 32, and 1 : 64 power splitters are 7.2, 10.5, 13.8, 17.1, and 20.1 dB, respectively. The lengths of feeder fiber and drop fiber are set as 3 and 1 km, respectively.

Simulation parameters of PnP-TF-QAN. For the PnP-TF-QAN, the simulation parameters are set as follows: the dark count rate $p_d = 2\times10^{-6}$, the number of the pulses $N = 10^{11}$, the detector efficiency $\eta_d = 15\%$, the error correction coefficient $f = 1.16$, the attenuation coefficient $\alpha_q = 0.35$ dB/km, the repetition frequency of the laser is 625 MHz.

Specifically, we simulate the key rate of PnP-TF-QKD using the three-intensity decoy-state method with full parameter optimization. The strict analysis of the finite data size can be seen in Appendix. We adopt the channel model given in Ref. [21] and the final secure key rate can be expressed as

$$R = P_X^2 P(k_c,k_d)\left[1-fh\left(e_{k_c k_d}\right)-h\left(e^{ph}_{k_c k_d}\right)\right], \tag{3}$$

where $(k_c,k_d)\in\{(1,0),(0,1)\}$ represents the successful detection event, P_X is the probability of choosing the X basis (signal state), $P(k_c,k_d)$ denotes the conditional probability that Charlie announces the outcome k_c,k_d when both parties choose the X basis, $h(x) = -x\log_2 x-(1-x)\log_2(1-x)$ is the binary entropy function. And the terms $e_{k_c k_d}$ and $e^{ph}_{k_c k_d}$ respectively denote the bit-error rate and phase-error rate in the X basis. Here the phase misalignment is set to 2% in our simulation, which is contiguous with the real-world experiment with a high-precision phase-locking device [46].

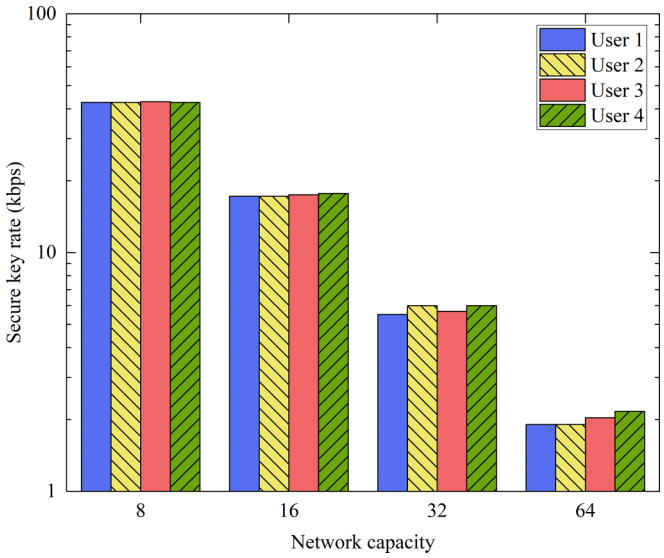

FIG. 2. Comparison of secure key rates among the first four users for full coexistence scheme with different network capacities.

The simulation proves that the PnP-TF-QAN integrated into 10G-EPON can achieve the maximum network capacity of 64 users by adding an attenuation of 5 dB on OLT power. When the network capacity is expanded to 128 users, even if the classical OLT power is attenuated to the minimum value, ONUs cannot receive signals from the OLT, and the quantum key generation rate is still negative, which means that neither 10G-EPON nor QAN will work properly. For example, when the OLT power is 3.4 dBm and the feeder fiber length is 2 km, an attenuation of 5 dB will bring the signal power received by ONUs below the detection threshold (−33 dBm) and the key rate is still a negative value (−0.5 kbps).

Figure 2 gives the key rates of the first four users under network capacities of 8, 16, 32, and 64, among which the corresponding key rates of User_1 are 42, 17.4, 5.6, and 1.9 kbps, respectively. The key rates of the first four users under the same network capacity may vary slightly as fluctuations in real experiments are taken into account.

In fact, the single-mode fibers commonly used in access networks, including ITU-T G.652, ITU-T G.657, and ITU-T G.654, exhibit quantum signal attenuation of approximately 0.19 to 0.2 dB/km at 1550 nm. Taking into account the additional attenuation introduced by the real system, the attenuation coefficient is usually set to 0.35 dB/km [9]. To clearly illustrate the difference between the simulation model and the real-world system, we simulated the effect of additional attenuation in the real environment on QAN performance. It is evident that the additional attenuation in the real world system leads to a lower secure key rate and a shorter transmission distance compared with the simulation model with an attenuation of 0.2 dB/km (ideal channel attenuation), as shown in Figs. 3 and 4. Hereinafter, we set the attenuation coefficient $\alpha_q = 0.35$ in the simulation.

Furthermore, the average key rate for all users with different network capacities is shown in Fig. 3. It can be seen that network capacity has a significant influence on the key rate and transmission distance. For example, an 8-user network

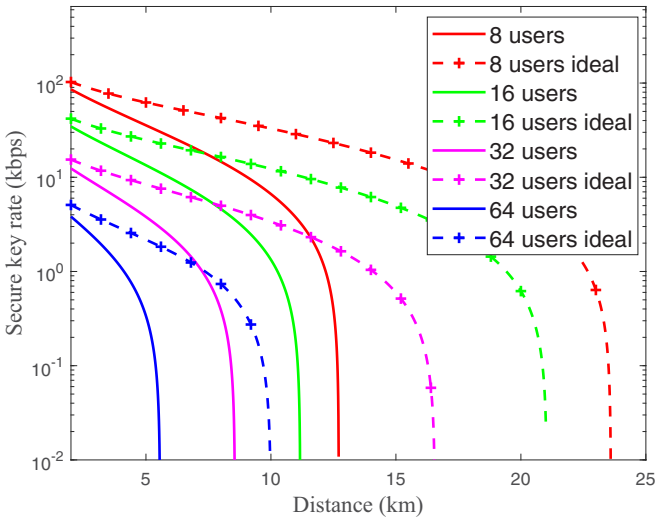

FIG. 3. Secure key rates vs transmission distance with different network capacities. The solid lines represent the results in the real-world scenario with an attenuation of 0.35 dB/km and the dotted lines with plus markers illustrate the results in the simulation model with an attenuation of 0.2 dB/km.

with the attenuation of 0.35 dB/km can achieve a transmission distance of 12.71 km, almost 2.29 times that of a 64-user network (only 5.54 km). At the distance of 4 km, the key rate is 46.9 kbps for an 8-user network and 1.02 kbps for a 64-user network.

In addition to network capacity, QKD performance is largely dependent on OLT power. The attenuation of OLT power will reduce the noise interference of classical signals, resulting in a higher key rate. However, the attenuation value is associated with the detection threshold of ONUs. Excessive attenuation will cause ONUs to not receive classical

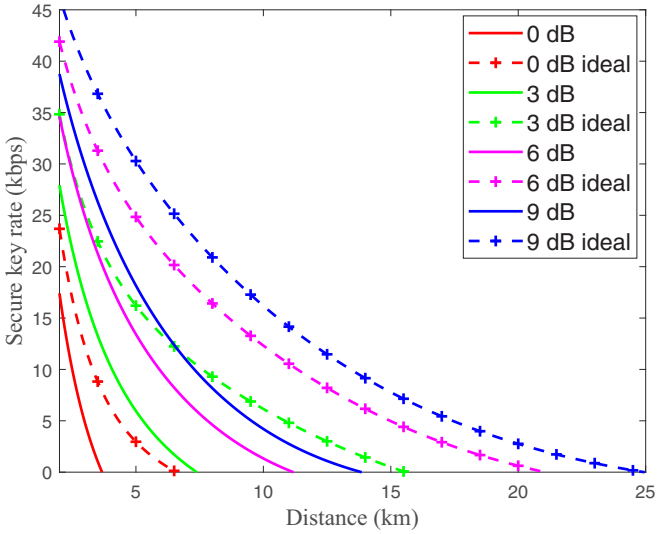

FIG. 4. Secure key rates vs transmission distance with different OLT power attenuations. The solid lines represent the results in the real-world scenario with an attenuation of 0.35 dB/km and the dotted lines with plus markers illustrate the results in the simulation model with an attenuation of 0.2 dB/km.

downstream signals normally. Figure 4 considers a 10G-EPON configuration with a network capacity of 16 users and an initial OLT power of 3.4 dBm. It is found that the key rate of PnP-TF-QKD increases significantly when the attenuation of 3 to 9 dB is added to the original power. Specially, in the real-world circumstance (0.35 dB/km), it can transmit 13.8 km with 9 dB attenuation, while transmitting 3.63 km without any attenuation. In other words, with 9 dB attenuation to OLT power, the transmission distance will increase by nearly 2.8 times. See Fig. 4 for detailed results.

III. PARTIAL COEXISTENCE SCHEME OF PNP-TF-QAN AND 10G-EPON

A. Partial coexistence architecture

For the full coexistence scheme with 10G-EPON, both quantum signals and classical signals are conveyed through a common feeder fiber and shared drop fibers. This configuration leads to significant SnRS noise that severely interferes with quantum signals, particularly in longer feeder fibers. As a result, the secure key rate of QKD is greatly influenced by the attenuation of OLT power. To minimize SnRS noise and meet the cost-effective power requirements, a partial coexistence scheme with two private feeder fibers and shared drop fibers is further proposed, as shown in Fig. 5. For dual-feeder fiber architecture, SnRS noise is generated only on drop fibers, and the powers of forward SnRS (denoted by P_F^{DF}) and backward SnRS (denoted by P_B^{DF}) are respectively expressed as

$$P_F^{DF} = P_{\mathrm{OLT}}\beta\Delta\lambda\Delta t\frac{e^{-\alpha_q L_D} - e^{-\alpha_c L_D}}{\alpha_c - \alpha_q}, \tag{4}$$

$$P_B^{DF} = P_{\mathrm{OLT}}\beta\Delta\lambda\Delta t\frac{(1 - e^{-(\alpha_c+\alpha_q)L_D})}{\alpha_c + \alpha_q}. \tag{5}$$

The communication process of the partial coexistence scheme is similar to that of the full coexistence scheme. The new components include a WDM filter and a double-layer filter. The WDM filter, which brings a loss of 1.5 dB, serves to filter out noise with a wavelength of 1550.12 nm and prevents the quantum signals emitted by Bobs from leaking to the OLT [9,41]. The double-layer filter, termed "Filter," serves the purpose of eliminating classical signals that may leak into quantum channel. Besides, the common power splitter is replaced by $2 \times N$ power splitter, with losses of 10.8 dB (2 : 8), 14.1 dB (2 : 16), 17.4 dB (2 : 32), and 20.4 dB (2 : 64), respectively. Compared with full coexistence scheme, the partial coexistence scheme allows OLT downstream signals to pass through the feeder fiber at full power, and the quantum signals in the dedicated feeder fiber can completely block the noise generated by classical signals.

B. Simulation results of partial coexistence scheme

We simulate and analyze the secure key rates of the first four users under network capacities 8, 16, 32, and 64 without any attenuation. The results are presented in Fig. 6.

Figure 7 further simulates the relationship between the average secure key rate and transmission distance under different network capacities for the partial coexistence scheme (without any attenuation), where the results of the full

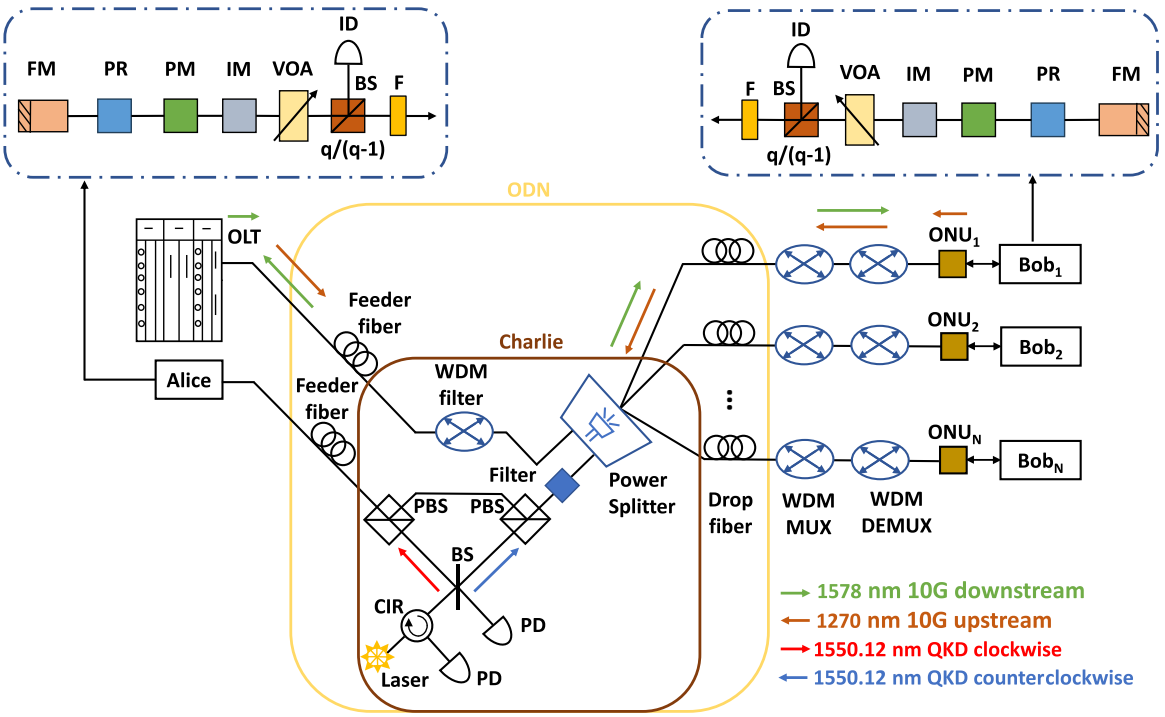

FIG. 5. Partial coexistence architecture of PnP-TF-QAN and 10G-EPON.

coexistence scheme (with an extra 6 dB attenuation) are included for comparison. It can be seen that the dual-feeder fiber architecture greatly improves the performance of QKD in terms of transmission distance and key generation rate. In particular, for an 8-user network, the transmission distance of the partial coexistence scheme can reach 16.79 km, which is nearly 32.1% higher than the 12.71 km of the full coexistence scheme. At the transmission distance of 10 km, the partial coexistence scheme results in a key rate of 16.14 kbps, while the full coexistence scheme achieves only 6.37 kbps, a decrease of almost 60.5%.

Figure 8 analyzes the performance of two coexistence architectures with different power attenuation. It can be seen that the single-feeder fiber architecture is more sensitive to power attenuation, and an extra attenuation promotes the performance to be greatly improved. In contrast, power attenuation can hardly enhance the performance of dual-feeder fiber architecture. In particular, with a 9 dB extra attenuation,

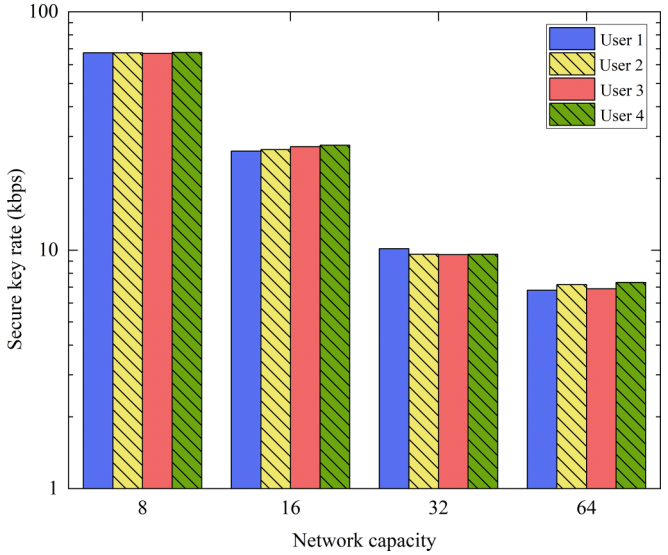

FIG. 6. Comparison of secure key rates among the first four users for partial coexistence scheme with different network capacities.

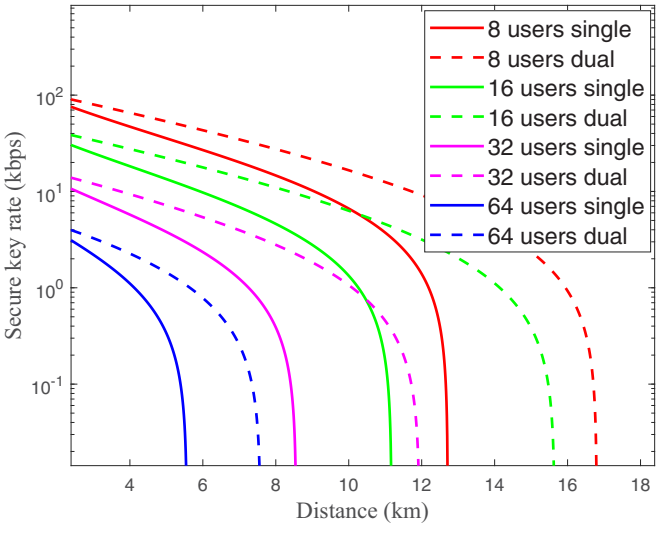

FIG. 7. Secure key rates vs transmission distance with different network capacities. The solid lines represent the results of the full coexistence scheme and the dotted lines represent the results of the partial coexistence scheme.

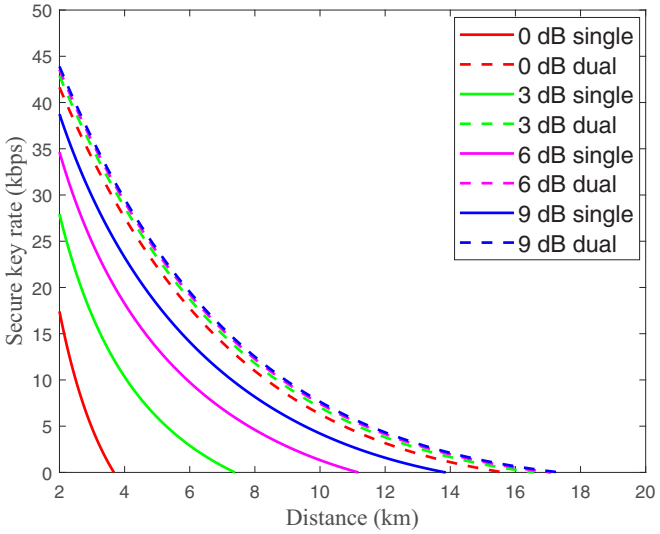

FIG. 8. Secure key rates vs transmission distance with different OLT power attenuations.

the transmission distance and key rate of dual-feeder fiber architecture increase by 9.7% and 11.1%, respectively, at the observation distance of 6 km. On the other hand, the distance and key rate are significantly increased by 2.8 times and 3.92 times, respectively, for single-feeder fiber architecture. The results illustrate that OLT signals can be transmitted at full power without significant influence on QKD performance under the partial coexistence scheme.

IV. MACHINE-LEARNING-ASSISTED IMPLEMENTATION

Before actually deploying QKD, two possible scenarios need to be considered: One is integrating QKD into existing 10G-EPONs, and the other is establishing a new coexistence architecture.

For the first scenario, some inherent parameters of 10G-EPON, such as network capacity, drop fiber length L_D, feeder fiber length L_F, wavelength of quantum signals (λ_q), and original OLT power $P_{\mathrm{OLT}}^{\mathrm{ori}}$, are given. An appropriate power attenuation for 10G-EPON signals needs to be found to maximize the secure key rate. However, it is often time consuming to find the optimal OLT power attenuation and predict QKD performance through iterations and extensive trial-and-error efforts before integrating QKD into 10G-EPON. Therefore, we develop a machine-learning-assisted prediction model that can rapidly provide the optimal attenuation value for OLT power ($P_{\mathrm{OLT}}^{\mathrm{opt}}$), the achievable key rate R, and the detected noise photons prior to system implementation. The input and output vectors of the neural network for the first scenario can be written as $\vec{I}_1 = \{\text{Network capacity}, L_D, L_F, P_{\mathrm{OLT}}^{\mathrm{ori}}, \lambda_q\}$ and $\vec{O}_1 = \{P_{\mathrm{OLT}}^{\mathrm{opt}}, R, \text{noise}\}$, respectively.

The second scenario can be further divided into two categories according to the geographical location of deployment. Networks in remote areas, such as mountains and islands, typically have a small number of users, require a longer feeder fiber, and tolerate a relatively low key rate. On the contrary, networks in central cities usually have a larger user capacity, so it is desirable to sacrifice some transmission distance to get higher key rates. It becomes even more complex to determine an appropriate OLT power and obtain a corresponding achievable secure key rate given various requirements and possibly external factors. Therefore, the machine-learning-assisted prediction method is essential for effective system planning and implementation when building a new coexistence system in a specific domain. For the joint deployment of 10G-EPON and QKD, L_F is no longer used as input since the location of OLT is not determined. In addition, an extra parameter, flag, is added to the input vector to calibrate different user requirements and perform corresponding predictions. Specifically, when flag $= 0$, it indicates that the network is deployed in remote areas, and transmission distance is the primary consideration. When flag $= 1$, it means that users are in dense urban areas, and the length of feeder fiber can be reduced appropriately in exchange for a higher key rate. Therefore, the input vector for the second scenario is $\vec{I}_2 = \{\text{Network capacity}, L_D, P_{\mathrm{OLT}}^{\mathrm{ori}}, \lambda_q, \text{flag}\}$ and the output vector is $\vec{O}_2 = \{P_{\mathrm{OLT}}^{\mathrm{opt}}, L_F, R, \text{noise}\}$.

A. Dataset generation and training

The parameters used for training dataset generation are listed in Table I. The OLT power interval is selected based on the IEEE 802.3av standard. The length of drop fiber is typically accessible from a few hundred meters to 1 km, depending on the specific implementation environments, here, it is assumed to range from 0.5 to 1 km. Considering the wavelength fluctuation of quantum signals in practice, the wavelength interval is 1550.10–1550.14 nm, taking 1550.12 nm as the central wavelength.

The training datasets were generated using the search algorithm. In the first scenario, we randomly extract 25 points from the interval of L_D, 18 points from the interval of L_F, and 5 points each from the intervals of $P_{\mathrm{OLT}}^{\mathrm{ori}}$ and λ_q, which would yield a total of 56 250 datasets. Each dataset includes input parameters and corresponding outputs. In the second scenario, we randomly extract 25 points from the interval of L_D, 10 points each from the interval of $P_{\mathrm{OLT}}^{\mathrm{ori}}$ and λ_q, and the flag is included in the input vector, resulting in a total of 25 000 datasets.

Before training, input data are normalized to the interval $(-1, 1)$, which is crucial to the final prediction performance of the model. After the iterative training of neural network, two kinds of prediction models are obtained for the above two scenarios.

TABLE I. The intervals of the dataset generation parameters.

Network capacity	L_D (km)	L_F (km)	$P_{\mathrm{OLT}}^{\mathrm{ori}}$ (dBm)	λ_q (nm)	Flag
{4, 8, 16, 32, 64}	0.5–1.0	2–20	2–7	1550.10–1550.14	{0, 1}

TABLE II. Searched parameters vs predicted parameters obtained by BPNN for full coexistence scheme in the first scenario.

Approach	Network capacity	$P_{\mathrm{OLT}}^{\mathrm{ori}}$ (dBm)	L_D (km)	L_F (km)	λ_q (nm)	$P_{\mathrm{OLT}}^{\mathrm{opt}}$ (dBm)	R (kbps)	Noise
BPNN	8	3	1	12.5	1550.12	−12.76	9.69	2.37×10^{-7}
Searched	8	3	1	12.5	1550.12	−12.8	9.69	2.35×10^{-7}
BPNN	32	4	0.8	8	1550.12	−5.12	0.89	2.1×10^{-7}
Searched	32	4	0.8	8	1550.12	−5.1	0.91	2.1×10^{-7}
BPNN	64	5	0.6	5	1550.12	−3.12	0.13	1.23×10^{-7}
Searched	64	5	0.6	5	1550.12	−3.1	0.13	1.23×10^{-7}

B. Predicting results of BPNN

1. Full coexistence scheme

We predict the performance of the full coexistence scheme with network capacities of 8, 32, and 64 in two scenarios. For the first scenario that integrating PnP-TF-QKD into an existing 10G-EPON system, it can be found that the deviation of predicted results from original values is only 0.3%–2%, as illustrated in Table II, where noise corresponds to the SnRS noise.

Besides, with a network capacity of 32 users, we further compare two other commonly used neural networks: radial basis function neural networks (RBFNN) and generalized regression neural networks (GRNN). The results show that BPNN achieves the highest prediction accuracy, as illustrated in Table III. The same conclusion can be obtained under other system conditions.

For the second scenario that constructing a new coexistence system, the machine-learning-assisted prediction model has a maximum deviation of 1.77% from the original searched values, as shown in Table IV. In a 32-user network, the length of feeder fiber can expand to 9.6 km when users pursue a longer transmission distance (flag = 0). For higher key generation requirements (flag = 1), the key rate can be significantly improved by 14.29 times (from 0.315 to 4.5 kbps) with a 43.2% transmission distance sacrifice.

2. Partial coexistence scheme

The dual-feeder fiber architecture can significantly decrease SnRS noise and enable OLT signals to be transmitted with full power. Nevertheless, the attenuation of OLT power also improves the key rate and transmission distance to some extent. We utilize the machine-learning-assisted prediction model to evaluate the maximum attenuation of OLT power for the partial coexistence scheme under two scenarios.

As illustrated in Table V, the deviation between the predicted values and the searched values is 0.3%–3.4% in the first scenario for the partial coexistence scheme, proving that the prediction model can almost perfectly predict the performance of the system. Furthermore, compared with single-feeder fiber architecture, dual-feeder fiber architecture shows significant improvements in the secure key rate, with enhancements of 9.4%, 2.19 times, and 6.77 times for 8-, 32-, and 64-user networks, respectively.

For the second scenario, the maximum deviation of predicted results from searched values is 2.31%, as shown in Table VI. Compared with the single-feeder fiber architecture, the noise level of dual-feeder fiber architecture is reduced by nearly two orders of magnitude, ranging from 10^{-8} to 10^{-9}, and the transmission distance is further increased by 21.34%, 26.41%, and 59.52% for network capacities of 8, 32, and 64, respectively. These findings highlight significant improvements in the performance of partial coexistence schemes, especially for networks with a large numbers of users.

TABLE III. Optimal parameters found by different neural networks for full coexistence scheme in the first scenario.

Networks	$P_{\mathrm{OLT}}^{\mathrm{opt}}$ (dBm)	R (kbps)	Noise
BPNN	−5.07	0.89	2.1×10^{-7}
GRNN	−5.02	0.83	2.05×10^{-7}
RBFNN	−5.08	0.88	2.09×10^{-7}

V. CONCLUSION

This work proposes a quantum secured 10 Gbit/s Ethernet passive optical access network, in which a bidirectional twin-field quantum access structure with a single untrusted source and two detectors is developed. The PnP-TF-QAN completely eliminates the assumption that each user needs to prepare a trusted laser source in traditional upstream QANs as well as eliminates the need for expensive detectors at each user in downstream QANs. This enables the cost-effective implementation of QANs with a reduced number of optical devices. It can be integrated on a classical 10G-EPON for up to 64 users with two feasible architectures, namely, full coexistence scheme and partial coexistence scheme. The full coexistence scheme with a single shared feeder fiber is suitable for integration in those EPON systems that are less sensitive to power consumption. By attenuating 10G-EPON signals to nearly −10.5 dBm, it achieves a transmission distance of 20.9 km with an applicable secure key rate. The partial coexistence scheme with two private feeder fibers successfully eliminates the SnRS noise in the feeder fiber and further improves the key rate and transmission distance. For a newly deployed coexistence system, the two coexistence architectures can be flexibly selected based on the actual implementation conditions and specific requirements of users.

In addition, before deploying QKDs in the field, it is necessary to predict the corresponding performance of QKD in advance according to the characteristics of 10G-EPON and field conditions, which determines whether QKD deployment is reasonable. However, this work is often time consuming and expertise dependent in practical

TABLE IV. Searched parameters vs predicted parameters obtained by BPNN for full coexistence scheme in the second scenario.

Approach	Network capacity	$P_{\mathrm{OLT}}^{\mathrm{ori}}$ (dBm)	L_D (km)	λ_q (nm)	flag	$P_{\mathrm{OLT}}^{\mathrm{opt}}$ (dBm)	L_F (km)	R (kbps)	Noise
BPNN	8	3	1	1550.12	1	−13.92	8.59	24.44	1.84×10^{-7}
Searched	8	3	1	1550.12	1	−14	8.6	24.5	1.82×10^{-7}
BPNN	8	3	1	1550.12	0	−11.59	16.36	2.43	3.07×10^{-7}
Searched	8	3	1	1550.12	0	−11.6	16.4	2.45	3.07×10^{-7}
BPNN	32	4	0.8	1550.12	1	−6.1	4.8	4.53	1.72×10^{-7}
Searched	32	4	0.8	1550.12	1	−6.1	5	4.5	1.69×10^{-7}
BPNN	32	4	0.8	1550.12	0	−4.89	8.75	0.314	2.2×10^{-7}
Searched	32	4	0.8	1550.12	0	−4.9	8.8	0.315	2.2×10^{-7}
BPNN	64	5	0.6	1550.12	1	−4.09	1.92	3.2	9.8×10^{-8}
Searched	64	5	0.6	1550.12	1	−4.1	1.9	3.21	9.75×10^{-8}
BPNN	64	5	0.6	1550.12	0	−3.39	4.18	0.69	1.16×10^{-7}
Searched	64	5	0.6	1550.12	0	−3.4	4.2	0.7	1.15×10^{-7}

experiments. To facilitate practical implementation, we develop a user-demand-oriented prediction model based on machine learning. It can directly predict QKD performance in a short time with small deviations instead of relying on time-consuming iterations and extensive trial-and-error efforts. In conclusion, the quantum-secured 10G-EPON scheme and machine learn-assisted implementation method are conducive to the deployment of future large-scale QANs to a certain extent.

ACKNOWLEDGMENTS

This work is supported by China Postdoctoral Science Foundation (Grant No. 221628) and Foundation of Shaanxi Province Education Department.

APPENDIX: FINITE-KEY ANALYSIS

In this section, we give some main formulas to deal with the statistical fluctuation in the finite-key regime. We represent N_X (N_Z) as the number of pulses of Alice and Bob both choosing the X basis (Z basis), and s_X (s_{AB}^Z) as the number of successful detection events in the X basis (signal state) and Z basis (decoy state), respectively.

The parameters s_X, s_{AB}^Z, and the bit error rate e_{k_c,k_d} can be directly calculated with the given channel model [21]. Therefore, the primary challenge lies in estimating the phase error rate e_{k_c,k_d}^{ph}. Its upper bound can be obtained with the following two steps: (i) The Hoeffding's inequality [47] is exploited to obtain a tight key-rate bound. (ii) A tighter security bound is obtained by applying the random sampling method [48].

Now we can utilize the Hoeffding's inequality to bound the observed value s_{AB}^Z:

$$\left|{s_{AB}^Z}^* - s_{AB}^Z\right| \leqslant \delta\left(s_{AB}^Z, \epsilon\right), \tag{A1}$$

where $\delta(x, y) = \sqrt{x/2 \ln(1/y)}$ and ϵ represents the failure probability. The expectation value ${s_{AB}^Z}^*$ is given by

$${s_{AB}^Z}^* = P_A P_B \sum_{n,m} P_{n|A} P_{m|B} Y_{n,m} N_Z, \tag{A2}$$

where P_A (P_B) is the probability of Alice (Bob) choosing decoy intensities μ_A (μ_B), and $P_{n|A} = e^{-\mu_A}(\mu_A)^n/n!$ [$P_{m|B} = e^{-\mu_B}(\mu_B)^m/m!$] is the Poisson distribution that Alice (Bob) sends out n (m) photons.

With the values of $\overline{{s_{AB}^Z}^*}$ and $\underline{{s_{AB}^Z}^*}$, we have

$$\frac{e^{\mu_A+\mu_B}\underline{{s_{AB}^Z}^*}}{P_A P_B N_Z} \leqslant \sum_{n,m} \frac{\mu_A^n \mu_B^m}{n!m!} Y_{nm} \leqslant \frac{e^{\mu_A+\mu_B}\overline{{s_{AB}^Z}^*}}{P_A P_B N_Z}. \tag{A3}$$

According to the analytical method of the three-intensity decoy state TF-QKD, yields $Y_{n,m}$ are required to calculate the upper bound of the bit error rate. For more detail, see Ref. [21]. We then employ the random sampling theory to give a tighter upper bound for e_{k_c,k_d}^{ph},

$$e_{k_c,k_d}^{ph} \leqslant \overline{e_{k_c,k_d}} + \gamma\left(s_X, s_Z, \overline{e_{k_c,k_d}}, \epsilon'\right), \tag{A4}$$

where $s_Z = \sum s_{AB}^Z$ is the total amount of successful detection events in the Z basis, and ϵ' is the failure probability and $\gamma(s_X, s_Z, \overline{e_{k_c,k_d}}, \epsilon')$ can be expressed as

$$\gamma(x, y, z, w) = \sqrt{\frac{(x+y)(1-z)z}{xy \ln 2} \log_2 \frac{x+y}{xyw^2(1-z)z}}. \tag{A5}$$

TABLE V. Searched parameters vs predicted parameters obtained by BPNN for partial coexistence scheme in the first scenario.

Approach	Network capacity	$P_{\mathrm{OLT}}^{\mathrm{ori}}$ (dBm)	L_D (km)	L_F (km)	λ_q (nm)	$P_{\mathrm{OLT}}^{\mathrm{opt}}$ (dBm)	R (kbps)	Noise
BPNN	8	3	1	12.5	1550.12	−12.76	10.56	2.52×10^{-8}
Searched	8	3	1	12.5	1550.12	−12.8	10.6	2.56×10^{-8}
BPNN	32	4	0.8	8	1550.12	−5.12	1.99	6.24×10^{-9}
Searched	32	4	0.8	8	1550.12	−5.1	1.99	6.27×10^{-9}
BPNN	64	5	0.6	5	1550.12	−3.11	0.91	1.83×10^{-9}
Searched	64	5	0.6	5	1550.12	−3.1	0.88	1.86×10^{-9}

TABLE VI. Searched parameters vs predicted parameters obtained by BPNN for partial coexistence scheme in the second scenario.

Approach	Network capacity	$P_{\mathrm{OLT}}^{\mathrm{ori}}$ (dBm)	L_D (km)	λ_q (nm)	flag	$P_{\mathrm{OLT}}^{\mathrm{opt}}$ (dBm)	L_F (km)	R (kbps)	Noise
BPNN	8	3	1	1550.12	1	−12.99	11.84	12.5	2.41×10^{-8}
Searched	8	3	1	1550.12	1	−13	11.91	12.32	2.44×10^{-8}
BPNN	8	3	1	1550.12	0	−10.49	19.92	0.3362	4.38×10^{-8}
Searched	8	3	1	1550.12	0	−10.5	19.9	0.3393	4.35×10^{-8}
BPNN	32	4	0.8	1550.12	1	−5.5	6.85	3.1	5.73×10^{-9}
Searched	32	4	0.8	1550.12	1	−5.5	6.91	3.1	5.71×10^{-9}
BPNN	32	4	0.8	1550.12	0	−4.2	11.05	0.0147	7.68×10^{-9}
Searched	32	4	0.8	1550.12	0	−4.2	11.1	0.0148	7.71×10^{-9}
BPNN	64	5	0.6	1550.12	1	−3.38	4.24	1.41	1.69×10^{-9}
Searched	64	5	0.6	1550.12	1	−3.4	4.2	1.43	1.73×10^{-9}
BPNN	64	5	0.6	1550.12	0	−2.59	6.64	0.0023	2.05×10^{-9}
Searched	64	5	0.6	1550.12	0	−2.6	6.7	0.0024	2.08×10^{-9}

[1] W. Sun, L.-J. Wang, X.-X. Sun, Y.-Q. Mao, H.-L. Yin, B.-X. Wang, T.-Y. Chen, and J.-W. Pan, Experimental integration of quantum key distribution and gigabit-capable passive optical network, J. Appl. Phys. **123**, 043105 (2018).

[2] K.-P. Byung, K.-W. Min, Y.-S. Kim, Y.-W. Cho, S. Moon, and S.-W. Han, User-independent optical path length compensation scheme with sub-nanosecond timing resolution for a $1 \times N$ quantum key distribution network system, Photonics Res. **8**, 296 (2020).

[3] C.-H. Park, M.-K. Woo, B.-K. Park, Y.-S. Kim, H.-J. Baek, S.-W. Lee, H.-T. Lim, S.-W. Jeon, H.-J. Jung, S. Kim, and S.-W. Han, $2 \times N$ twin-field quantum key distribution network configuration based on polarization, wavelength, and time division multiplexing, npj Quantum Inf. **8**, 48 (2022).

[4] M.-K. Woo, B.-K. Park, Y.-S. Kim, Y.-W. Cho, H. Jung, H.-T. Lim, S. Kim, S. Moon, and S.-W. Han, One to many QKD network system using polarization-wavelength division multiplexing, IEEE Access **8**, 194007 (2020).

[5] H.-L. Yin, Y. Fu, C.-L. Li, C.-X. Weng, B.-H. Li, J. Gu, Y.-S. Lu, S. Huang, and Z.-B. Chen, Experimental quantum secure network with digital signatures and encryption, Natl. Sci. Rev. **10**, nwac228 (2023).

[6] Y.-M. Xie, J.-L. Bai, Y.-S. Lu, C.-X. Weng, H.-L. Yin, and Z.-B. Chen, Advantages of asynchronous measurement-device-independent quantum key distribution in intercity networks, Phys. Rev. Appl. **19**, 054070 (2023).

[7] B. Fröhlich, F. D. James, M. Lucamarini, W. A. Sharpe, Z.-L. Yuan, and J. S. Andrew, A quantum access network, Nature (London) **501**, 69 (2013).

[8] B. Fröhlich, F. D. James, M. Lucamarini, W. S. Andrew, W.-B. T. Simon, Z.-L. Yuan, and J. S. Andrew, Quantum secured gigabit optical access networks, Sci. Rep. **5**, 18121 (2015).

[9] B.-X. Wang, S.-B. Tang, Y.-Q. Mao, W.-H. Xu, M. Cheng, J. Zhang, T.-Y. Chen, and J.-W. Pan, Practical quantum access network over a 10 Gbit/s Ethernet passive optical network, Opt. Express **29**, 38582 (2021).

[10] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu *et al.*, An integrated space-to-ground quantum communication network over 4600 kilometres, Nature (London) **589**, 214 (2021).

[11] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao *et al.*, Field and long-term demonstration of a wide area quantum key distribution network, Opt. Express **22**, 21739 (2014).

[12] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X.-F. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, Measurement-device-independent quantum key distribution over untrustful metropolitan network, Phys. Rev. X **6**, 011024 (2016).

[13] J.-J. Zhang and A. Nirwan, Toward energy-efficient 1G-EPON and 10G-EPON with sleep-aware MAC control and scheduling, IEEE Commun. Mag. **49**, s33 (2011).

[14] B. Skubic, J. Chen, J. Ahmed, L. Wosinska, and B. Mukherjee, A comparison of dynamic bandwidth allocation for EPON, GPON, and next-generation TDM PON, IEEE Commun. Mag. **47**, S40 (2009).

[15] V. Houtsma, D. van Veen, and E. Harstead, Recent progress on standardization of next-generation 25, 50, and 100G EPON, J. Lightwave Technol. **35**, 1228 (2017).

[16] L.-J. Wang, L.-K. Chen, J. Lei, M.-L. Xu, Y. Zhao, K. Chen, Z.-B. Chen, T.-Y. Chen, and J.-W. Pan, Experimental multiplexing of quantum key distribution with classical optical communication, Appl. Phys. Lett. **106**, 081108 (2015).

[17] I. Choi, R. J. Young, and P. D. Townsend, Quantum key distribution on a 10Gb/s WDM-PON, Opt. Express **18**, 9600 (2010).

[18] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "Plug and play" systems for quantum cryptography, Appl. Phys. Lett. **70**, 793 (1997).

[19] J.-Q. Geng, G.-J. Fan-Yuan, S. Wang, Q.-F. Zhang, Y.-Y. Hu, W. Chen, Z.-Q. Yin, D.-Y. He, G.-C. Guo, and Z.-F. Han, Coexistence of quantum key distribution and optical transport network based on standard single-mode fiber at high launch power, Opt. Lett. **46**, 2573 (2021).

[20] J.-Q. Geng, G.-J. Fan-Yuan, S. Wang, Q.-F. Zhang, W. Chen, Z.-Q. Yin, D.-Y. He, G.-C. Guo, and Z.-F. Han, Quantum key distribution integrating with ultra-high-power classical optical communications based on ultra-low-loss fiber, Opt. Lett. **46**, 6099 (2021).

[21] F. Grasselli and M. Curty, Practical decoy-state method for twin-field quantum key distribution, New J. Phys. **21**, 073001 (2019).

[22] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).

[23] M. Lucamarini, Z.-L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, Nature (London) **557**, 400 (2018).

[24] C. H. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution without phase postselection, Phys. Rev. Appl. **11**, 034053 (2019).

[25] K. Maeda, T. Sasaki, and M. Koashi, Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit, Nat. Commun. **10**, 3140 (2019).

[26] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 062323 (2018).

[27] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference, PRX Quantum **3**, 020315 (2022).

[28] T. F. da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J.-P. von der Weid, Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits, Phys. Rev. A **88**, 052303 (2013).

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

[30] H.-L. Yin and Z.-B. Chen, Coherent-state-based twin-field quantum key distribution, Sci. Rep. **9**, 2045 (2019).

[31] W. Wang, R. Wang, C. Hu, V. Zapatero, L. Qian, B. Qi, M. Curty, and H.-K. Lo, Fully passive quantum key distribution, Phys. Rev. Lett. **130**, 220801 (2023).

[32] J. Gu, X.-Y. Cao, Y. Fu, Z.-W. He, Z.-J. Yin, H.-L. Yin, and Z.-B. Chen, Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources, Sci. Bull. **67**, 2167 (2022).

[33] K. Xue, S.-M. Zhao, Q.-P. Mao, and R. Xu, Plug-and-play sending-or-not-sending twin-field quantum key distribution, Quant. Info. Proc. **20**, 320 (2021).

[34] F.-H. Xu, Measurement-device-independent quantum communication with an untrusted source, Phys. Rev. A **92**, 012333 (2015).

[35] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, Phys. Rev. A **73**, 022320 (2006).

[36] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phase-remapping attack in practical quantum-key-distribution systems, Phys. Rev. A **75**, 032314 (2007).

[37] F.-H. Xu, B. Qi, and H.-K. Lo, Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, New J. Phys. **12**, 113026 (2010).

[38] G.-Z. Tang, S.-H. Sun, F.-H. Xu, H. Chen, C.-Y. Li, and L.-M. Liang, Experimental asymmetric plug-and-play measurement-device-independent quantum key distribution, Phys. Rev. A **94**, 032326 (2016).

[39] Y.-J. Choi, O. Kwon, M. Woo, K. Oh, S.-W. Han, Y.-S. Kim, and S. Moon, Plug-and-play measurement-device-independent quantum key distribution, Phys. Rev. A **93**, 032319 (2016).

[40] C.-H. Park, M.-K. Woo, B.-K. Park, M.-S. Lee, Y.-S. Kim, Y.-W. Cho, S. Kim, S.-W. Han, and S. Moon, Practical plug-and-play measurement-device-independent quantum key distribution with polarization division multiplexing, IEEE Access **6**, 58587 (2018).

[41] B.-X. Wang, Y.-Q. Mao, L. Shen, L. Zhang, X.-B. Lan, D.-W. Ge, Y.-Y. Gao, J.-H. Li, Y.-L. Tang, S.-B. Tang, J. Zhang, T.-Y. Chen, and J.-W. Pan, Long-distance transmission of quantum key distribution coexisting with classical optical communication over a weakly-coupled few-mode fiber, Opt. Express **28**, 12558 (2020).

[42] D. N. Vavulin, V. I. Egorov, A. V. Gleim, and S. A. Chivilikhin, Determining influence of four-wave mixing effect on quantum key distribution, J. Phys.: Conf. Ser. **541**, 012066 (2014).

[43] N. A. Peters, P. Toliver, T. E. Chapuran, R. J. Runser, S. R. McNown, C. G. Peterson, D. Rosenberg, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, and K. T. Tyagi, Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments, New J. Phys. **11**, 045012 (2009).

[44] L.-J. Wang, K.-H. Zou, W. Sun, Y.-G. Mao, Y.-X. Zhu, H.-L. Yin, Q. Chen, Y. Zhao, F. Zhang, T.-Y. Chen, and J.-W. Pan, Long-distance copropagation of quantum key distribution and terabit classical optical data channels, Phys. Rev. A **95**, 012301 (2017).

[45] T. E. Chapuran, P. Toliver, N. A. Peters, J. Jackel, M. S. Goodman, R. J. Runser, S. R. McNown, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, C. G. Peterson, K. T. Tyagi, L. Mercer, and H. Dardy, Optical networking for quantum key distribution and quantum communications, New J. Phys. **11**, 105001 (2009).

[46] Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, Y. Peng, Y. Zhou, F.-Y. Guan-Jie, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution over 830-km fibre, Nat. Photonics **16**, 154 (2022).

[47] W. Hoeffding, *The Collected Works of Wassily Hoeffding* (Springer, New York, 2012).

[48] C.-H. F. Fung, X. Ma, and H. F. Chau, Practical issues in quantum-key-distribution postprocessing, Phys. Rev. A **81**, 012318 (2010).