Proceedings Paper:
Razavi, M, Lo Piparo, N, Panayi, C et al. (2013) Architectural Considerations in Hybrid Quantum-Classical Networks. In: 2013 Iran Workshop on Communication and Information Theory (IWCIT). Iran Workshop on Communication and Information Theory (IWCIT), 08-09 May 2013, Tehran, Iran. IEEE. ISBN: 978-1-4673-5023-5. ISSN: 2374-3212.

https://doi.org/10.1109/IWCIT.2013.6555772

Architectural Considerations in Hybrid Quantum-Classical Networks

(Invited Paper)

Mohsen Razavi, Nicoló Lo Piparo, Christiana Panayi, and David E. Bruschi
School of Electronic and Electrical Engineering
University of Leeds, Leeds, LS2 9JT, United Kingdom
Email: m.razavi@leeds.ac.uk

***Abstract*—Three network architectures, compatible with passive optical networks, for future hybrid quantum-classical networks are proposed and compared. These setups rely on three different schemes for quantum key distribution (QKD): BB84, entanglement-based QKD, and measurement-device-independent QKD (MDI-QKD). It turns out that, while for small-to-moderate-size networks BB84 supports the highest secret key generation rate, it may fail to support large numbers of users. Its cost implications are also expected to be higher than other setups. For large networks, MDI-QKD offers the highest key rate if fast single-photon detectors are employed. Entanglement-based networks offer the longest security distance among the three setups. MDI-QKD is, however, the only architecture resilient to detection loopholes and possibly the most favorable with its less demanding end-user technology. Entanglement-based and MDI-QKD setups can both be combined with quantum repeater systems to allow for long-distance QKD with no trust constraints on the service provider.**

I. Introduction

Emerging technologies in quantum communications are anticipated to find their way, sooner or later, into people's homes and be part of service packages offered by telecommunication operators [1], [2]. The integration of the two technologies—quantum and classical—is, however, a challenging task. Classical systems are designed to transfer large amounts of data quickly and reliably, whereas quantum systems' imminent objective is information security. The two systems will consequently be run in two different regimes of operation. Classical communications relies on low error-rate wireless or wired (mainly in the form of optical fibers) communication links, whereas quantum communications relies on the single-photon technology and must wrestle with many implementation challenges. In order to facilitate the deployment of quantum systems, in *coexistence* with our current and future classical services, *hybrid* quantum-classical networks need to be developed. This paper addresses this issue from the architectural standpoint and compares several possible configurations for such networks.

The proper design of such hybrid networks requires rigorous planning by experts in both disciplines. Infrastructural investments in classical communications are, however, mostly market driven. This implies that, by the time that technological as well as socio-economical trends make the deployment of quantum systems indispensable, such systems are required to mostly adapt themselves to the existing infrastructure for their classical counterparts. While it is difficult to fully predict the structure of future optical networks, the increasing demand for data communications by the end users has necessitated some form of fiber-to-the-home (FTTH) architecture. In this paper, we make the assumption that passive optical networks (PONs) will be used to connect home users to their immediate central office and consider quantum cryptography protocols that can lend themselves to such configurations.

The main quantum application considered in this paper is quantum key distribution (QKD). QKD enables two users to securely exchange a secret key—a random sequence of bits—which can later be used for different cryptography protocols. QKD is one of the most imminent quantum technologies, with commercial prospects and immediate public benefits. Since its introduction at the IBM Research Laboratory in 1984 [3], and its first tabletop demonstration in 1989 [4], QKD technology has continued to develop, becoming both cheaper and more accessible. In particular, via its growing industry, all components of a point-to-point QKD link are now commercially available. Over the past years, QKD has been demonstrated over distances as long as 260 km at gigahertz transmission rates [5]–[7]. Secret key generation rates on the order of megahertz have also been achieved over optical fibers carrying classical data [2].

Despite all the progress in QKD, the whole topic of *public* QKD is still at its infancy. There are only a handful of theoretical or experimental investigations that address multiuser scenarios such as one-to-many [1], [8], [9] or any-to-any [10]–[13] networking. Similarly, there are only a few examples of co-transmission of quantum and classical signals over the same optical channel [1], [2], [9], [11], [14]–[16]. Further progress on these, and other, issues is required before we can offer QKD to every home user. To this end, it is crucial to come up with a roadmap and to have a vision for how such hybrid networks may look like in the future.

To respond to the above needs, this paper sheds some light on the architectural aspects of hybrid quantum-classical networks. It considers several viable solutions and compares and contrasts them in terms of their performance, reliability and cost for the end users. By looking at the compatibility of the proposed configurations to that of quantum repeaters [17]–[20], we also discuss the possible extension of these setups to wide area networks (WANs).

The rest of this paper is organized as follows. In Sec. II, we review point-to-point QKD over dark and commercial fibers. We then compare three viable architectures for quantum

communications over PON systems in Sec. III. Section IV investigates the possible extension of these networks to long-distance WANs using quantum repeater setups. We conclude the paper in Sec. V.

II. Point-to-Point QKD

In this section, we first review three main QKD schemes, namely, BB84 [3], entanglement-based [21], and measurement-device-independent (MDI) [22] protocols, in the two-user scenario. The extension to the multi-user case will be discussed in Sec. III. Here, we first consider the case when the two users are allocated a dedicated channel. We will then consider using a commercial fiber channel when both classical and quantum signals use the same medium.

A. QKD over dedicated channels

1) BB84: The BB84 protocol enables two parties, namely, Alice and Bob, to securely exchange, or, more precisely, extend a secret key sequence; see Fig. 1(a). It performs this task through the following steps. Alice first encodes single photons with a raw key and send them to Bob. Encoding is done in two, randomly chosen, nonorthogonal polarization/phase bases. The bases will be revealed later, via authenticated classical communications, in order that Alice and Bob turn their raw keys into sifted keys by keeping only the bits for which the same basis has been used for encoding and decoding. In the next step, Alice and Bob attempt to correct for possible discrepancies in their sifted keys by using error-correction techniques. If they find the quantum bit error rate (QBER) too high, they will abort the protocol, otherwise they apply privacy amplification to their corrected keys to bring the amount of leaked information to eavesdroppers below a desired threshold. In a variant of BB84, known as the decoy-state protocol [23], by accepting a minor performance degradation, weak laser pulses replace ideal single photons. In this paper, we use the latter protocol for its practical implementation advantages.

The secret key generation rate per transmitted pulse, for a BB84 protocol that uses decoy coherent states and threshold detectors for its implementation, in the limit of an infinitely long key, is lower bounded by $\max[0, R_{\rm BB84}]$, where [23]

$$R_{\rm BB84} = q\left(-fQ_\mu H(E_\mu) + Q_1[1-H(e_1)]\right), \qquad (1)$$

where $H(p) = -p\log_2 p - (1-p)\log_2(1-p)$, for $0 \le p \le 1$, $f \ge 1$ is the error correction inefficiency,

$$Q_\mu = 1-(1-Y_0)e^{-\eta\mu} \text{ and } E_\mu = [e_0 Y_0 + e_d(1-e^{-\eta\mu})]/Q_\mu \qquad (2)$$

are, respectively, the overall gain and the QBER,

$$Q_1 = Y_1\mu e^{-\mu} \text{ and } e_1 = (Y_0/2 + e_d\eta)/Y_1 \qquad (3)$$

are, respectively, the gain and the error rate of a single-photon state, μ is the average number of photons in a signal pulse, $Y_1 = Y_0 + \eta(1-Y_0)$ is the yield of a single-photon state, η is the total transmissivity of the link including the efficiency of Bob's detectors, e_d represents the misalignment error, and Y_0 is the probability of a click on the receiver's side without having any incident photons from Alice. In a point-to-point link, Y_0, the yield of the vacuum state, models the photodetectors' dark current and the background noise. In a hybrid network, Y_0 must also include the interference noise from other active, quantum or classical, users. Variations in Y_0 will correspondingly modify the gain and error-rate terms in (2) and (3), and would result in a change in the key rate, as we investigate in the following sections. In (1), $q = 1/2$ if the two bases are chosen with the same probability. If one uses the asymmetric protocol in [24], in which one basis is used more often than the other, q can approach 1.

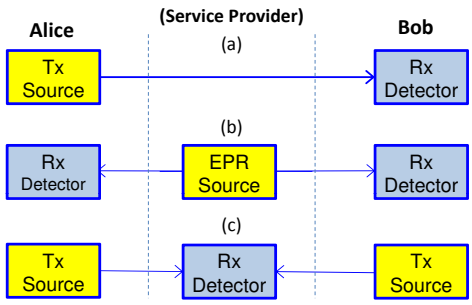

Fig. 1. Three different QKD schemes: (a) BB84, where one user is the transmitter, and the other one the receiver; (b) entanglement-based QKD, where the source could be with a third untrusted party (service provider), and the users must be able to do detection measurements; and (c) MDI-QKD, where both users have BB84 encoders and measurements can be done by the third party.

2) Entanglement-based QKD: An alternative approach to BB84 is entanglement-based QKD. In this protocol, Alice and Bob ideally share a maximally entangled state, on which they perform one of the two BB84 measurements. Again, if they both use the same measurement basis, they expect to get correlated measurement results, which constitute their sifted keys. The rest of the protocol is similar to that of BB84. Eavesdropping attacks will be detected by the criteria set by the Bell's inequalities [21], or excessive QBER [25]. In the link of Fig. 1(b), when ideal Einstein-Podolsky-Rosen (EPR) states are used, the secret key generation rate per EPR pair sent is lower bounded by

$$R_{\rm EPR} = qQ_e\left(-fH(e_Q) + 1 - H(e_Q)\right), \qquad (4)$$

where, ignoring double-click events,

$$Q_e = \eta_A\eta_B + (\eta_A + \eta_B - 2\eta_A\eta_B)Y_0 + (1-\eta_A\eta_B)Y_0^2 \qquad (5)$$

is the chance of getting a click on both sides, and

$$e_Q Q_e = e_d\eta_A\eta_B + 1/2[(\eta_A+\eta_B-2\eta_A\eta_B)Y_0 + (1-\eta_A\eta_B)Y_0^2], \qquad (6)$$

where e_Q is the QBER. In (5) and (6), η_A and η_B are, respectively, the total transmission efficiencies from the EPR source of Fig. 1(b) to Alice and Bob's detectors, including their detectors' quantum efficiencies.

3) MDI-QKD: The third scheme is a combination of the two schemes above and relies on the reverse EPR protocol [26]. In MDI-QKD, Alice and Bob both encode their photons according to the BB84 protocol and send them to a middle station where a third, possibly *untrusted*, party performs a Bell-state measurement (BSM) on the transmitted photons; see Fig. 1(c). The results of the BSMs are sent to Alice and Bob, who, after sifting, will come up with correlated sifted keys. Post processing will be performed similarly to other QKD protocols. Decoy states can also be used in MDI-QKD, as

we do in this paper, giving rise to the following secret key generation rate per pulse sent by Alice and Bob [27]

$$R_{\rm MDI} = [Q_{11}(1 - H(e_{11;X})) - fQ_{\mu\nu;Z}H(E_{\mu\nu;Z})], \quad (7)$$

where μ (ν) is the average number of photons for signal states sent by Alice (Bob), and

$$Q_{11} = \mu\nu e^{-\mu-\nu}Y_{11}, \quad (8)$$

$$\begin{aligned} Y_{11} \quad = \quad & (1-\gamma_{\rm dc})^2\left[\eta_a\eta_b/2 + (2\eta_a + 2\eta_b - 3\eta_a\eta_b)\gamma_{\rm dc}\right. \\ & \left. +4(1-\eta_a)(1-\eta_b)\gamma_{\rm dc}^2\right], \end{aligned} \quad (9)$$

$$e_{11;X}Y_{11} = Y_{11}/2 - (0.5 - e_d)(1-\gamma_{\rm dc})^2\eta_a\eta_b/2, \quad (10)$$

$$\begin{aligned} Q_{\mu\nu;Z} &= Q_C + Q_E, \\ E_{\mu\nu;Z}Q_{\mu\nu;Z} &= e_dQ_C + (1-e_d)Q_E, \end{aligned} \quad (11)$$

where

$$\begin{aligned} Q_C &= 2(1-\gamma_{\rm dc})^2 e^{-\mu'/2}\times \\ &\left[1-(1-\gamma_{\rm dc})e^{-\eta_a\mu_a/2}\right]\left[1-(1-\gamma_{\rm dc})e^{-\eta_b\mu_b/2}\right], \\ Q_E &= Y_0(1-\gamma_{\rm dc})^2 e^{-\mu'/2}[I_0(2x) - (1-\gamma_{\rm dc})e^{-\mu'/2}]. \end{aligned} \quad (12)$$

In above equations, $I_0(x)$ is the modified Bessel function of the first kind and

$$\begin{aligned} x &= \sqrt{\eta_a\mu\eta_b\nu}/2, \\ \mu' &= \eta_a\mu + \eta_b\nu, \end{aligned} \quad (13)$$

where η_a (η_b) is the transmission efficiency for the Alice's (Bob's) link, and $\gamma_{\rm dc} = Y_0/2$. The BSM operation is assumed to be partial performed by, e.g., the linear optics module used in [22].

Aside from the technical differences between the above three schemes, what distinguishes them for us, in this paper, is their architectures. In Fig. 1(a), each user needs to have both the transmitter (encoder) and the receiver (decoder) modules, and the role of the service provider is to create a clear path between them. In Fig. 1(b), users only need measurement modules, and the source is being controlled by the service provider. Finally, in Fig. 1(c), all measurements are performed by the service provider and the users are equipped with BB84 encoders. In the following section, we discuss how the difference in the structure of each link will manifest itself in the performance, reliability, and the cost of the corresponding network.

B. QKD over commercial channels

In order to have cost-efficient hybrid networks, it is essential that quantum and classical systems use the same infrastructure. Considering the high cost of laying optical fibers under the ground, and the increasing demand for data communications, the available bandwidth must efficiently be used. Communicating quantum and classical signals over the same optical fiber is, however, one of the key challenges in integrating quantum and classical systems. At first sight, one possible solution is the assignment of different wavelength channels and/or bands to each system. This seems to be particularly practical because of the range of equipment and expertise available in both the conventional (around 1550 nm) and the original (around 1310 nm) bands of an optical fiber.

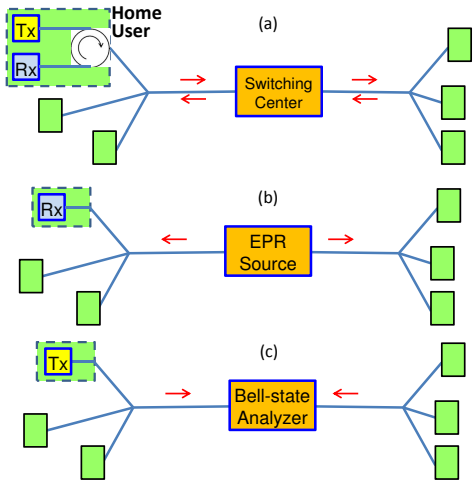

Fig. 2. Three different LAN/MAN architectures for QKD networks based on (a) BB84, (b) entanglement-based QKD, and (c) MDI-QKD.

The challenge will still remain, however, because of different regimes of power at which the two systems operate. For classical optical systems, it is customary to send milliwatts of power for data transmission, whereas in QKD we are dealing with single-photon pulses. This implies that, even if we assign two different wavelength channels to each system, the crosstalk noise from the classical signals can still bury our single-photon signals.

The main source of crosstalk in hybrid links is backward Raman scattering [1], [2], [15], [16]. For the receiver part of a quantum node, the strongest crosstalk contribution comes from the classical transmitter at that node. As a general wavelength allocation rule, one should try to assign the farthest possible channels to the classical transmitter and the quantum receiver of each user [2]. This will minimize the required spectral filtering for the quantum user. In general, however, in addition to spectral filtering one should use different temporal techniques to further reduce the crosstalk noise. In [2], authors have used very short temporal gates for their self-differencing detectors. In [1], the off time in an on-off keyed (OOK) classical signal has been used for quantum transmission. This method is, however, limited to time-division multiple access (TDMA) networks that use OOK signaling.

Regardless of the method used for multiplexing classical and quantum signals and its corresponding demultiplexing-filtering technique, it is expected, especially in the network scenario, that some background noise would leak from classical signals to quantum channels. In our forthcoming analysis, we assume that this background noise is constant. We also assume that the classical side of the network will be run independently and only focus on the quantum side of each setup [13].

III. Local/Metropolitan Area Quantum-Classical Networks

Based on the three setups of Fig. 1, one can design three different configurations for a local/metropolitan area network (LAN/MAN); see Fig. 2. Such QKD networks are expected to have the following desired features. First, every two users must be able to exchange a secret key without trusting any

other users. Their architecture must also be compatible with the structure of PONs. Their total cost per user, and for the end user, needs to be kept low as well. Each user is able to classically communicate data, on the same platform but possibly on a different channel setting than that of the quantum system. The last requirement, we assume, has been achieved by proper channel allocation and the use of relevant equipment to multiplex and demultiplex classical and quantum signals.

A. BB84 Network

Figure 2(a) shows a possible QKD setup between two PONs based on the BB84 protocol. The extension to multiple PONs is straightforward and will be neglected here. In this configuration, the above requirements have been met by allocating quantum encoder (Tx) as well as quantum decoder (Rx) components to each user. The users in this network are connected via a switching center, which routes packets between designated users. By using proper multiple-access techniques, multiple pairs of users can exchange secret keys. In this paper, we assume that users are time multiplexed, and that all necessary coordination steps are conducted over the classical channels. As shown in [13], TDMA minimizes the interference from other quantum users and is also compatible with most PON systems in operation today. We also assume that the switching center can enable two users belonging to the same PON to communicate with each other.

Assuming N home users for each of the two PONs, the secret key exchange rate between any two network users is given by

$$R_1 = R_{\rm BB84} R_p/N, \tag{14}$$

where R_p/N is the rate at which coherent QKD pulses are sent by the Alice user in a TDMA setup with N time slots [13]. In (14), $R_{\rm BB84}$ is given by (1) at $\eta = \eta_d \eta_L/N^2$, where η_d is the quantum efficiency of single-photon detectors and η_L is the path-coupling loss over a distance L. Here, we assume that the length of fiber between any two users is identical and it is equal to L. The factor N^2 is due to the splitters' loss at the PONs. In principle, one can use wavelength-division multiplexing to avoid this loss, but then the required channel resources are linearly increasing as well. In this paper, we restrict ourselves to a single-wavelength per PON, noting that by including additional wavelength channels the capacity of all setups in Fig. 2 will correspondingly improve. We also consider a fixed amount of crosstalk noise for each user. Given that the backscattered Raman noise is the major source of crosstalk, the recipient QKD user's classical transmission is considered to be the main contributor to this noise.

B. Entanglement-based QKD Network

With similar assumptions as above, one can devise a QKD network based on entanglement-based protocols; see Fig. 2(b). Here, the service provider sends pairs of entangled photons to any two users who wish to exchange a secret key, and the respective users will only need to perform QKD measurements on the received photons. That will in principle include the case where the two users belong to the same PON, although, in this case, additional switches (not shown in the figure) and time coordination may be needed. The secret key generation rate is then given by

$$R_2 = R_{\rm EPR} R_p/N, \tag{15}$$

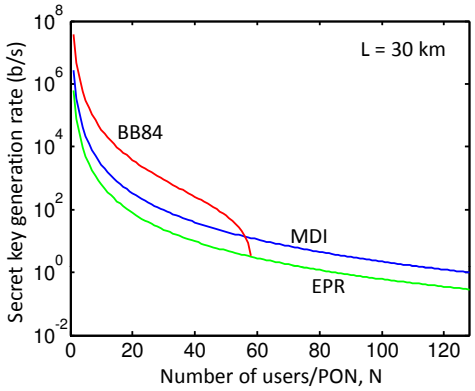

Fig. 3. Rate versus number of users for the three network architectures of Fig. 2. In all curves, dark count is 10^{-6} per pulse, $\eta_d = 0.5$, and $L = 30$ km. Crosstalk noise is 10^{-6} per pulse for BB84 and EPR protocols, and twice as much for MDI-QKD. R_p is assumed to be 1 G pulse/s for BB84 and MDI-QKD, and 10 M pulse/s for the EPR protocol. We also assume 0.2 dB/km channel loss, $e_d = 0$, $f = 1.16$, $q = 1$, and $\mu = \nu = 0.48$.

where $R_{\rm EPR}$ is calculated from (4) at $\eta_A = \eta_B = \eta_d\sqrt{\eta_L}/N$, assuming that the distance of each user to the EPR source is identical. R_p/N, here, is the rate at which entangled photons are sent to the two users, and is typically less than the repetition rate for laser pulses [28]. Multiple sources may be used in this architecture to improve the key rate and the number of users supported per unit of time. Again the major source of crosstalk is that produced by the two end users once they transmit classical signals.

C. MDI-QKD Network

Finally, Fig. 2(c) shows the corresponding setup for an MDI-QKD network. In this setup, all users are equipped with BB84 encoders, which, except for the degree of freedom in which information is encoded, ideally generate indistinguishable photons. Under this condition, the secret key generation rate is given by

$$R_3 = R_{\rm MDI} R_p/N, \tag{16}$$

where $R_{\rm MDI}$ is calculated from (7) at $\eta_a = \eta_b = \eta_d\sqrt{\eta_L}/N$, assuming that all users have the same distance to the BSM module. R_p/N, here, is the rate at which coherent QKD pulses are sent to the Bell-state analyzer. In our TDMA setup, it is then assumed that the deadtime of the single-photon detectors used in the BSM module is less than the TDMA time slot [29]. If not, the service provider may need to employ multiple BSM modules with additional switches to direct each photon to the relevant measurement site. Additional arrangements are also needed if the two users of interest are from the same PON. The crosstalk noise in this setup is expected to be twice as high as the other two schemes, because of having two optical line terminals corresponding to the two PONs.

D. Performance Comparison

There are several measures by which QKD systems can be compared. The secret key generation rate, as discussed so far, is one of them. Another one is the security distance within which secret exchange of keys is possible. In the network scenario the number of users supported and their impact on the former two parameters are also matters of interest.

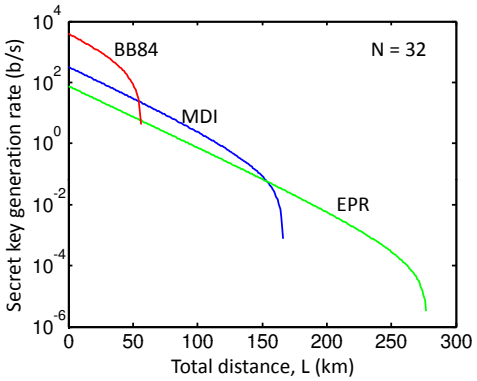

Fig. 4. Rate versus distance for our three network architectures at $N = 32$. All other parameters are the same as that of Fig. 3.

Figure 3 shows the secret key generation rate, based on (14)-(16), for each of the three schemes discussed as a function of the number of users in each PON. We have considered a fixed distance of $L = 30$ km, which covers a metropolitan area, and different pulse repetition rates for each system. In MDI-QKD and BB84, $R_p = 1$ G pulse/s, corresponding to the available pulsed laser technology. For EPR protocol, however, $R_p = 10$ M pulse/s corresponding to the existing technologies for the EPR-pair generation [30]. The cross talk noise is assumed to be the same for BB84 and EPR-based QKD, but twice as much for MDI-QKD. It is evident from the figure that while BB84 offers the best key rate for up to around 60 users, its key rate eventually goes to zero at this value. MDI-QKD offers the best key exchange rate when it comes to moderate or large number of users. The main reason for this effect is the sensitivity of each scheme to the path loss as discussed next.

Among the three proposed network setups, EPR-based QKD has the largest security distance. MDI-QKD comes second with a reasonably long security distance exceeding 100 km. This has been demonstrated in Fig. 4, where, for a fixed number of users at 32, we have plotted the key rate versus distance. As compared to BB84, MDI-QKD and the EPR protocol are less sensitive to channel loss, or correspondingly to dark counts, as their photons should travel half the distance before being detected, and that would result in longer security distances.

Figure 4 highlights an important feature of single-photon-based QKD techniques: their key rate exponentially decays with distance. To remedy this effect and also to extend the security distance, quantum repeaters have been proposed. In Sec. IV, we look at the integration of our proposed setups with that of quantum repeaters to find suitable hybrid WAN architectures.

E. Cost and Reliability

The design and the development of hybrid quantum-classical networks are expected to be highly impacted by the market and, in that regard, the cost of the system is of paramount importance. While it is difficult to put a price on a technology that is still developing and has not yet introduced at mass scales, we can make certain observations, based on the current trends, and compare the three proposed setups in terms of cost and reliability factors, as we discuss below.

Each quantum network in Fig. 2 is composed of various components. At the the encoder side, we typically need (pulsed) lasers/EPR sources, polarizers/phase interferometers, amplitude modulators and drivers, random number generators, and the corresponding electronics that control the whole system. At the decoder side, among other things, single-photon detectors and their corresponding electronics as well as polarizers and beam splitters are required. Classical communications is also needed to coordinate between the users and also to facilitate the post-processing stages of QKD. Which side will turn out more expensive is partly a matter of equipment used in each part. In order to gain some insight, here, we oversimplify the problem and denote, in all three setups, the total cost of the encoder unit by $C_{\rm enc}$ and that of the decoder unit by $C_{\rm dec}$. The total cost of each of the setups in Fig. 2 is then given by

$$\begin{aligned} C_{\rm BB84} &= 2NC_{\rm enc} + 2NC_{\rm dec} + C_{\rm net}, \\ C_{\rm EPR} &= N_{\rm EPR}C_{\rm enc} + 2NC_{\rm dec} + C_{\rm net}, \\ C_{\rm MDI-QKD} &= 2NC_{\rm enc} + N_{\rm BSM}C_{\rm dec} + C_{\rm net}, \end{aligned} \tag{17}$$

where $C_{\rm net}$ is the cost of the classical components of the network such as switches and transceivers, and $N_{\rm EPR}$ and $N_{\rm BSM}$ are, respectively, the number of EPR sources and BSM modules used in Figs. 2(b) and (c).

The first observation to be made is that the cost of the equipment held by the end user in the BB84 setup is roughly twice as high as that of the other two setups. This is by itself a disadvantage, as service providers will prefer to have the low cost equipment at the end user's side and keep bulky/expensive elements within the network, where they can be shared among all users, thereby reducing the total cost per user. In the architectures of Figs. 2(b) and (c), that could be done by varying $N_{\rm EPR}$ and $N_{\rm BSM}$ according to the traffic demands of the network.

Another point of interest is that it is generally perceived that the encoding task in QKD is possibly less demanding than that of detecting single photons, which at some point may rely on superconducting technology [7], [31], [32]. That would favor setups where the number of detectors have been minimized, which in our case is the MDI-QKD network. Moreover, while in most demonstrated attacks on QKD the detectors are compromised [33]–[38], MDI-QKD enjoys resilience to detection loopholes. That will make MDI-QKD the most reliable solution, among those discussed in this paper, for the public implementation of QKD.

IV. Wide Area Quantum-Classical Networks

Future hybrid quantum-classical networks must accommodate quantum services, such as QKD, to any two users at any distance. Nevertheless, as shown in Fig. 4, the path loss has a deteriorating effect on the secret key generation rate and eventually on the security of the QKD protocol. One solution that achieves better rate-versus-distance scaling is that of quantum repeaters. Quantum repeaters were originally proposed to distribute entanglement between two remote quantum memories [17]. The enabling idea was based on first distributing entanglement over shorter segments, and then extending it to longer distances by performing BSMs, similar

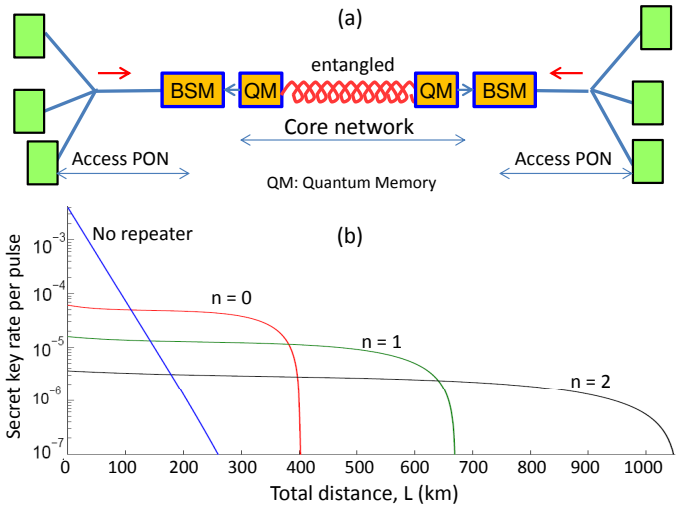

Fig. 5. (a) A possible architecture for hybrid quantum-classical WANs based on MDI-QKD over quantum repeaters. (b) Rate, per pulse, versus distance for a single-node MDI-QKD system that uses entangled memories. Memories are entangled according to the protocol proposed in [39] using optimal values for the source transmission coefficients. Here, n represents the nesting level for the repeater protocol and $\eta_d = 0.3$, $f = 1$, memory writing (reading) efficiency is 0.5 (0.7), and double-photon probability is 10^{-4}. Channel loss is 0.17 dB/km and all other parameters are the same as that of Fig. 3.

to the ones used in MDI-QKD, on middle memories. This approach is naturally compatible with EPR-based and MDI-QKD protocols. In the former case, the EPR source in Fig. 2(b) is replaced by quantum memories, which are now entangled by a quantum repeater. One just needs to read, i.e., convert their internal states into photonic states, to generate entangled photons similar to the ones generated by an EPR source [40]. In the latter, one needs to perform BSMs on the photons read from entangled memories and those sent by the two users; see Fig. 5(a). Extending the BB84 network to longer distances, by adding intermediate nodes, is also possible, but then one needs to trust these middle nodes via which the final key is distributed between the two end users [10], [41]. This scenario is only acceptable if the service provider is considered to be trustworthy.

Based on the results obtained in the previous section, MDI-QKD is possibly the favorite option in quantum-classical WANs. Figure 5(b) shows some preliminary results on how MDI-QKD performs on the quantum repeater setup of Fig. 5(a). In our calculations, we have used a particular protocol for quantum repeaters as proposed in [39]. This protocol relies on a probabilistic approach to BSMs. Here, we have, however, assumed that entangled memories are available at any time needed by the users of interest, and have only accounted for the possible degradation of entangled states as distributed by the repeater protocol [42]. Within the parameter setting used, it can be seen that the addition of quantum memories in a quantum repeater setup can stretch the security distance to longer distances than what can be achieved without repeaters. The security distance will increase by increasing the nesting level, n, where 2^n is the number of segments in the quantum repeater. Further analysis is required to estimate the total secret key generation rate once more practical restrictions are considered in the repeater system.

V. Concluding Remarks

In this paper, we discussed the possible deployment of quantum technologies, such as QKD, in future hybrid quantum-classical networks. The main objective was to use the same infrastructure that would be in use for classical optical communications. With demand for FTTH services on the rise, we proposed the extension of three point-to-point QKD schemes over PONs. The three schemes considered were the original BB84 and EPR protocols alongside the recently proposed MDI-QKD scheme. These setups had different configurations in terms of where quantum encoders and decoders would be located and the role of service provider in each case. It turned out that, while for small-to-moderate-size PONs BB84 would offer the highest key rate, MDI-QKD could accommodate a larger number of users at higher distances. We also showed that the MDI-QKD architecture could be combined with quantum repeater setups to enable long-distance quantum communications for WAN users. Nevertheless, many technological challenges must be resolved before having an operational hybrid quantum-classical WAN.

Our comparison will not be complete without considering other emerging technologies. For instance, coherent optical communications seems to be the main player in future optical fiber networks and the integration of QKD with such systems requires further analysis. This includes the use of optical orthogonal frequency division multiplexing for quantum and classical users. Another area of interest is the role of continuous-variable QKD in coherent optical networks [43]. Finally, satellite QKD [44] and its role in long-distance quantum communications, along with possible relativistic effects, must be scrutinized before finalizing the design of future hybrid quantum-classical networks.

Acknowledgment

The authors would like to thank Xiongfeng Ma, Norbert Lütkenhaus, and Divya Ramanujachari for fruitful discussions. This research has received funding from the European Seventh Framework Programme under Grant Agreement 277110 and the UK Engineering and Physical Science Research Council Grant No. EP/J005762/1.

References

[1] I. Choi, R. J. Young, and P. D. Townsend, "Quantum information to the home," *New J. Phys.*, vol. 13, p. 063039, June 2011.

[2] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Phys. Rev. X*, vol. 2, p. 041010, Nov. 2012.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*. Bangalore, India: IEEE, New York, 1984, pp. 175–179.

[4] ——, "The dawn of a new era for quantum cryptography: The experimental prototype is working!" *ACM SIGACT News*, vol. 20, no. 4, pp. 78–82, Oct. 1989.

[5] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, p. 010504, 2007.

[6] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Practical gigahertz quantum key distribution based on avalanche photodiodes," *New J. Phys.*, vol. 11, p. 045019, April 2009.

[7] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," *Opt. Lett.*, vol. 37, no. 6, pp. 1008–1010, March 2012.

[8] P. D. Kumavor, A. C. Beal, S. Yelin, E. Donkor, and B. C. Wang, "Comparison of four multi-user quantum key distribution schemes over passive optical networks," *IEEE/OSA J. Lightwave Technol.*, vol. 23, no. 1, pp. 268–276, Jan. 2005.

[9] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legre, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Langer, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network," *Opt. Exp.*, vol. 19, no. 11, pp. 10 387–10 409, 2011.

[10] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, p. 075001, 2009.

[11] W. Chen, Z.-F. Han, T. Zhang, H. Wen, Z.-Q. Yin, F.-X. Xu, Q.-L. Wu, Y. Liu, Y. Zhang, X.-F. Mo, Y.-Z. Gui, G. Wei, and G.-C. Guo, "Field experiment on a star type metropolitan quantum key distribution network," *IEEE Photon. Technol. Lett.*, vol. 21, no. 9, pp. 575–577, May 2009.

[12] S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang, L.-J. Zhang, F.-Y. Li, D. Liu, Y.-G. Wang, G.-C. Guo, and Z.-F. Han, "Field test of wavelength-saving quantum key distribution network," *Opt. Lett.*, vol. 35, no. 14, pp. 2454–2456, 2010.

[13] M. Razavi, "Multiple-access quantum key distribution networks," *Communications, IEEE Transactions on*, vol. 60, no. 10, pp. 3071–3079, 2012.

[14] T. J. Xia, D. Z. Chen, G. A. Wellbrock, A. Zavriyev, A. C. Beal, and K. M. Lee, "In-band quantum key distribution (QKD) on fiber populated by high-speed classical data channels," in *Opt. Fiber Commun., Technical Digest*. Optical Society of America, 2006, paper OTuJ7.

[15] 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 1550nm QKD with strong classical channels in reconfigurable networking environments," *New J. Phys.*, vol. 11, p. 045012, April 2009.

[16] 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.*, vol. 11, p. 105001, Oct. 2009.

[17] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, no. 26, pp. 5932–5935, Dec. 1998.

[18] M. Razavi and J. H. Shapiro, "Long-distance quantum communication with neutral atoms," *Phys. Rev. A*, vol. 73, p. 042303, April 2006.

[19] M. Razavi, M. Piani, and N. Lütkenhaus, "Quantum repeaters with imperfect memories: Cost and scalability," *Phys. Rev. A*, vol. 80, p. 032301, Sept. 2009.

[20] J. Amirloo, M. Razavi, and A. H. Majedi, "Quantum key distribution over probabilistic quantum repeaters," *Phys. Rev. A*, vol. 82, p. 032304, Sept. 2010.

[21] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.* , vol. 67, p. 661, 1991.

[22] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, March 2012.

[23] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.* , vol. 94, p. 230504, June 2005.

[24] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *Journal of Cryptology*, vol. 18, no. 2, pp. 133–165, 2005.

[25] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bells theorem," *Phys. Rev. Lett.*, vol. 68, p. 557, 1992.

[26] E. Biham, B. Huttner, and T. Mor, "Quantum cryptographic network based on quantum memories," *Phys. Rev. A*, vol. 54, no. 4, p. 2651, 1996.

[27] X. Ma and M. Razavi, "Alternative schemes for measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 86, p. 062319, Dec. 2012.

[28] E. Bocquillon, C. Couteau, M. Razavi, R. Laflamme, and G. Weihs, "Coherence measures for heralded single-photon sources," *Phys. Rev. A*, vol. 79, p. 035801, March 2009.

[29] A. R. Dixon, J. F. Dynes, Z. L. Yuan, A. W. Sharpe, A. J. Bennett, and A. J. Shields, "Ultrashort dead time of photon-counting InGaAs avalanche photodiodes," *Applied Physics Letters*, vol. 94, no. 23, p. 231113, 2009.

[30] M. Razavi, I. Sllner, E. Bocquillon, C. Couteau, R. Laflamme, and G. Weihs, "Characterizing heralded single-photon sources with imperfect measurement devices," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 42, no. 11, p. 114013, 2009.

[31] H. Takesue, S. Nam, Q. Zhang, R. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," *Nature Photonics*, vol. 1, no. 6, pp. 343–348, 2007.

[32] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," *New Journal of Physics*, vol. 11, no. 7, p. 075003, 2009.

[33] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Phys. Rev. A*, vol. 74, p. 022313, 2006.

[34] V. Makarov and J. Skaar, "Faked states attack using detector efficiency mismatch on sarg04, phase-time, dpsk, and ekert protocols," *Quant. Inf. Comput.*, vol. 8, p. 0622, 2008.

[35] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," *Quant. Inf. Comput.*, vol. 7, p. 073, 2007.

[36] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Experimental demonstration of time-shift attack against practical quantum key distribution systems," *Phys. Rev. A*, vol. 78, p. 042333, 2008.

[37] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature photonics*, vol. 4, no. 10, pp. 686–689, 2010.

[38] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," *Nature Communications*, vol. 2, p. 349, June 2011.

[39] N. Sangouard, C. Simon, J. c. v. Minář, H. Zbinden, H. de Riedmatten, and N. Gisin, "Long-distance entanglement distribution with single-photon sources," *Phys. Rev. A*, vol. 76, p. 050301, Nov 2007.

[40] M. Razavi and J. H. Shapiro, "Nonadiabatic approach to entanglement distribution over long distances," *Phys. Rev. A*, vol. 75, p. 032318, 2007.

[41] R. Alléaume, F. Roueff, E. Diamanti, and N. Lütkenhaus, "Topological optimization of quantum key distribution networks," *New Journal of Physics*, vol. 11, no. 7, p. 075002, 2009.

[42] N. Lo Piparo and M. Razavi, "Long-distance quantum key distribution with imperfect devices," *arXiv:quant-ph/1210.8042*, 2012.

[43] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature Photonics*, vol. advance online publication, pp. 1749–4893, April 2013.

[44] C. Bonato, A. Tomaello, V. D. Deppo, G. Naletto, and P. Villoresi, "Feasibility of satellite quantum key distribution," *New Journal of Physics*, vol. 11, no. 4, p. 045017, 2009.