Network Coding Aided Cooperative Quantum Key Distribution Over Free-Space Optical Channels

Hung Viet Nguyen[1], Phuc V. Trinh[2], Anh T. Pham[2], Zunaira Babar[1], Dimitrios Alanis[1], Panagiotis Botsinis[1], Daryus Chandra[1], Soon Xin Ng[1], and Lajos Hanzo[1]
[1]School of ECS, University of Southampton, SO17 1BJ, UK.
[2]Computer Communications Lab., The University of Aizu, Japan 965-8580.

***Abstract*—Realistic public wireless channels and Quantum Key Distribution (QKD) systems are amalgamated. Explicitly, we conceive Network Coding aided Cooperative Quantum Key Distribution over Free Space Optical (NC-CQKD-FSO) systems for improving the Bit Error Ratio (BER) and either the key rate or the reliable operational distance. Our system has provided a 55% key rate improvement against the state-of-the-art benchmarker.**

I. Introduction and Overview

A pair of popular Quantum Key Distribution (QKD) protocols, namely the BB84 protocol proposed by Bennett and Bassard in 1984 [1] and the E91 protocol advocated by Ekert in 1991 [2], have established compelling cryptographic approaches that are capable of providing perfect security, despite the rapid advances in computational power. Explicitly, this is ensured by exploiting the unique characteristics of quantum physics rather than classic mathematical complexity. A number of secure QKD protocols [3] have been inspired by these seminal protocols.

Depending on how the source data is encoded, QKD systems can be further classified into Continuously Variable (CV-)QKD [4], [5] and Discrete Variable (DV-)QKD categories [1], [2], [6]. In the CV-QKD systems, the data is encoded into continuous variables and conveyed by the amplitude and/or phase of weakly modulated of light pulses, which may contain several photons. These pulses are transmitted through quantum channels, and then are observed at the receiver by either homodyne or heterodyne detection [7]. By contrast, in the DV-QKD systems, which are technologically more mature [8]–[10], the source data values are mapped onto the discrete state of a single photon, namely the polarization of the photon. These photons are then transmitted over the quantum channel and detected at the receiver side by using photon detectors.

As regards to the realisation of QKD based information security, QKD systems can be constructed either based upon trustworthy device-dependent elements [11], [12] or upon Device-Independent (DI) protocols [13]. The DI-QKD systems are capable of tolerating imperfections in the transmitter or receiver implementation without posing any security risks [9], [10], provided that a high detection efficiency can be achieved, as evidenced by experimental demonstrations [10], [14]. The implementation efforts of DV-QDK device-dependent systems have been focused both on satellite communications [15], [16] as well as on terrestrial communications [17], [18] and on the emerging hand-held communication [19], [20] scenarios. Most contributions assumed having perfect classical communication and a single source-to-destination transmission link [15]–[20].

In the context of terrestrial communications [17], [18], the quantum channels of the QKD schemes may be realised with the aid of employing both Optical Fiber (OF) [9], [21], [22] and Free Space Optical (FSO) systems [14], [23]–[25]. Although QKD-based OF technology has become mature [9], [22], the laying of OF is not always economical. Compared to the OF-based solutions, FSO based systems offer higher scalability and better cost efficiency while maintaining a comparable data rate of up to 10 Gbps [26]. As a result, FSO links are being considered for numerous applications, including last-mile access [27], fiber backup [28], back-haul links of next-generation wireless cellular networks [29], and disaster recovery [30]. To elaborate, in contrast to OF based schemes, the dispersion effects imposed by FSO links remain moderate in the upper layers of the atmosphere [30]. This advantageous property of FSO's reserves the consistency of the photon's polarization during its propagation over atmospheric channels, which is beneficial for QKD systems.

Prior studies of QKD-based FSO systems presented in [23]–[25] have mainly focused their attention on the analytical characterization of atmospheric channel's effects. One of the challenges in QKD-based FSO systems is to counteract the detrimental effects of absorption, scattering, diffraction as well as the turbulence-induced fading of atmospheric channels. These channel impairments significantly limit both the maximum key rate and the achievable communication distance of QKD-based FSO systems. Recently, a QKD-based FSO system using multiple-input multiple-output (MIMO) schemes has been proposed for increasing the key rate and for allowing receivers to communicate simultaneously with a number of transmitters via several wavelengths [24]. On the other hand, a relay-assisted QKD-based FSO system has been invoked for quantum communication over long-distance atmospheric channels [25]. By employing multiple passive relays that

The authors are with the School of Electronics and Computer Science, University of Southampton, Southampton, SO17 1BJ, UK (email: [1]{hvn08r, zb2g10, da4g11, pb1y14, dc2n14, sxn, lh}@ecs.soton.ac.uk) and with Computer Communications Laboratory, University of Aizu, Japan 965-8580 (email: [2]phuc.v.trinh@ieee.org, [2]pham@u-aizu.ac.jp).

The financial support of the EPSRC under the grant EP/L018659/1, that of the European Research Council, Advanced Fellow Grant and that of the Royal Society's Wolfson Research Merit Award is gratefully acknowledged. Additionally, the authors acknowledge the use of the IRIDIS High Performance Computing Facility, and associated support services at the University of Southampton, in the completion of this work.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2017.2712288, IEEE Access

simply redirect the quantum bits without any observations or quantum measurement, longer communications links have been created with the aid of relaying.

In the QKD-based FSO systems of [14], [23]–[25], the popular BB84 based protocol [1] is used for supporting secret key sharing between two users, where a raw key at the source (S) is mapped to randomly polarised photons for transmission over an FSO quantum channel. At the destination (D), these transmitted photons are detected by using randomly selected bases, as exemplified by [23] . Then, the source and destination have to exchange information about the bases used for transmission and detection. Later, the information is used for filtering out specific bit intervals, during which the pair of bases used by S for its transmission are the same as those used by D for detection. It should be noted that a pair of classical public channels are required for exchanging the information pertaining to the bit interval and to the polarization bases used both at S and D, namely one from S to D and one from D to S. As a result, there are two versions of the shared key at S and D, which have to be identical. However, they may turn out to be different due to errors caused by the quantum channel and the detection process at D as well as owing to those imposed by the pair of classical public channels.

Network coding of [31], [32] is capable of increasing the throughput, while minimising the amount of energy required. This is achieved by allowing the intermediate nodes of the network to combine multiple data packets received via the incoming links before transmission to the destination [33]. It was demonstrated in [34] that the network coding is capable of significantly improving multiple-user systems' performance.

In [23]–[25], the information exchange regarding the choice of the random bases applied at S and D were considered to be conveyed over error-free public channels [23]–[25]. Against the above background, the novel contribution of our paper is as follows:

- *We conceive Network Coding aided Cooperative Quantum Key Distribution over Free Space Optical (NC-CQKD-FSO) systems, where network coding is invoked for improving the realistic public communication used for information exchange between the communicating parties in multiple-user QKD systems.*
- *We derive tight bounds of the fraction $gamma$ of photons received via FSO quantum channels both in the far-field and near-field regimes. This allows us accurately characterise the overall performance of our proposed NC-CQKD-FSO systems.*
- *We formulate a framework for incorporating realistic public wireless channels into QKD systems, where both the BER-performance and the key-rate bounds are quantified in support of our theoretical analysis.*
- *We investigate both the BER performance and key-rate of a Single-User QKD-FSO system and of our NC-CQKD-FSO system, in order to quantify benefits of the proposed NC-CQKD-FSO system, when considering realistic public channels in the context of terrestrial communication scenarios.*

The rest of the paper is organised as follows. Preliminaries and definitions are presented in Section II in order to facilitate the portrayal of our proposed system in Section III, where the system model is described before detailing our system parameters and the associated evaluation criteria. The benefits of our system proposed in Section III-A are analysed and demonstrated in Section IV, before our conclusions are offered in Section V.

II. Preliminaries and Definitions

In support of the subsequent sections, we provide relevant background on the physical interpretation concerning the polarization of photons and on photon detection.

A. Photon polarization

Depending on the specific form of the electromagnetic plane wave pertaining to the monochromatic laser signal generating photons, photons may be linearly polarized (LP) or elliptically polarized (EP) [35]. In the context of considering QKD systems, we only consider LP photons having polarizations of say $0^0, 90^0, -45^0, 45^0$ [36]. Accordingly, the basis associated with the polarization of $0^0, 90^0$ can be characterised by:

$$|0^0\rangle \;=\; 1|0^0\rangle + 0i|90^0\rangle, \tag{1}$$

$$|90^0\rangle \;=\; 0|0^0\rangle + i|90^0\rangle. \tag{2}$$

As a result, when a measurement (observation) relying on the basis polarization of 0^0 or 90^0 is applied to the state $|0^0\rangle$, we should obtain the probability $p = |1|^2 = 1$ of detecting a photon in state $|0^0\rangle$ or the probability $p = |0i|^2 = 0$ of detecting a photon in state $|90^0\rangle$, respectively. Similar results can be obtained for the basis associated with the polarization of $-45^0, 45^0$.

The relationship between the two bases can also be expressed by:

$$|0^0\rangle \;=\; \frac{1}{\sqrt{2}}|45^0\rangle + \frac{i}{\sqrt{2}}|-45^0\rangle, \tag{3}$$

$$|90^0\rangle \;=\; \frac{1}{\sqrt{2}}|45^0\rangle - \frac{i}{\sqrt{2}}|-45^0\rangle. \tag{4}$$

Accordingly, when a measurement made at the polarization of -45^0 or 45^0 is applied to the photon prepared at state $|0^0\rangle$, we have the probability $p = |\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$ of detecting it in state $|45^0\rangle$ and $p = |\frac{i}{\sqrt{2}}|^2 = \frac{1}{2}$ of detecting it in state $|-45^0\rangle$. Similar results may be obtained, when considering the inverse relationship as:

$$|45^0\rangle \;=\; \frac{1}{\sqrt{2}}|0^0\rangle + \frac{i}{\sqrt{2}}|90^0\rangle, \tag{5}$$

$$|-45^0\rangle \;=\; \frac{1}{\sqrt{2}}|0^0\rangle - \frac{i}{\sqrt{2}}|90^0\rangle. \tag{6}$$

B. Photon detection in QKD systems

Let us use the simplified schematic of Fig. 1 along with the numerical example detailed in Table I to illustrate the photon detection process as well as the associated errors in the QKD systems of [23], [25].

①-② of Table I: As seen in Fig. 1, a raw key in the form of a bit sequence S_A having $L_{S_A} = 10$ bits in Table I is mapped to the pulse sequence F_A having an average power of $n_S = 1$ photons/pulse, which results in $L_{F_A} = 10$ photons. The mapping carried out at the polarization controller of Fig. 1 uses the random basis sequence B_A containing both vertical $\oplus$ and diagonal $\otimes$ bases to apply the following rule [23]:

$$\oplus \quad \Rightarrow \begin{cases} 0^0 & : \text{ If bit ‘0‘ is transmitted} \\ 90^0 & : \text{ If bit ‘1‘ is transmitted} \end{cases}, \qquad (7)$$

$$\otimes \quad \Rightarrow \begin{cases} -45^0 & : \text{ If bit ‘0‘ is transmitted} \\ +45^0 & : \text{ If bit ‘1‘ is transmitted} \end{cases}. \qquad (8)$$

③-⑤ of Table I: An FSO transmission channel is used for carrying the photon stream F_A to the destination (D). Since the FSO channel imposes deleterious effects, such as diffraction, atmospheric turbulence and extinction [26], only a certain fraction γ of the photon stream F_A transmitted by S arrives at D and this particular fraction is represented by the sequence F_B in Table I. Then, at the receiver of D, the 50:50 beam splitter (BS) of Fig. 1 passively provides the random bases represented by the sequence B_B of Table I, which can only be extracted from the detection results $\hat{F}_A$ provided by the outputs of all the APDs processing the signal orginated from the photon sequence F_B. Hence, again the APDs at D have to detect from the sequence F_B, which only contains a fraction γ of the photon stream F_A transmitted by S, where the errors caused by the background noise n_B and dark current noise n_D have also been included [23]. Explicitly, the erroneous detection occurring at the 3^{rd} bit interval of $\hat{F}_A$ in Table I is indicated by the gray background cell, while the ND (no detection) notation in the 10^{th} bit interval of both F_B and $\hat{F}_A$ represents the $(1-\gamma)$ fraction of F_A that has not arrived at D and hence cannot be detected by the APDs. The ND in the 10^{th} interval of $\hat{F}_A$ leads to the NA (not available) value in the 10^{th} interval of B_B in Table I.

⑥-⑧ of Table I: Then, S transmits information to D about the bases B_A used for transmission at S through perfect classical communication channels, which results in the availability of B_A at D. Then the sequence B_A is used in conjunction with the sequence B_B for ruling[1] out those specific photons from $\hat{F}_A$, which correspond to the particular bit intervals, where the bases B_A and B_B are not identical, in order to introduce a series of sift events. In other words, a *sift* event occurs, when D has detected a photon and the same basis is applied by both S and D for transmitting and detecting a specific photon. As a result, a shared key K_B is generated and stored at D, where the key K_B contains bits recovered from the transmission of the raw key S_A. In the mean time, the bases B_B previously extracted from the detection results $\hat{F}_A$ at D are made available to S via perfect public classical channels. Similarly, the sifting process of Fig. 3 is carried out at S for generating the resultant secret shared key K_A. It should be noted that the D is unaware of having an erroneous bit in the shared key K_B, namely the 3^{rd} bit, which is different from that of the shared key S_A stored at S. The error-event occurring in the 3^{rd} bit interval happens when D detects an incorrect polarization in a sift event.

Accordingly, the BER of the QKD system illustrated in the numerical example of Table I can be calculated as

$$BER \quad = \quad \frac{N_{error-at-S} + N_{error-at-D}}{N_{sift-at-S} + N_{sift-at-D}} = \frac{1+1}{8+8}, \qquad (9)$$

where there is $N_{error-at-S} = 1/N_{error-at-D} = 1$ error event occurring at the 3^{th} bit interval of K_A/K_B of Table I, while there exist $N_{sift-at-S} = 8/N_{sift-at-D=8}$ sift-events in occurring at the Source/Destination in a transmission session, respectively. Note that We detail the derivation of the average BER in next subsection.

C. Errors Probability in QKD systems

Let us now determine the average value of the BER in Eq. (9). As mentioned above, the transmitted polarised pulse sequence F_A has an average power of n_S photons per pulse and only a fraction γ of photons transmitted arrives at the D. Hence, the received polarised pulse sequence F_B of Fig. 1 has the average received power of γn_S photons per pulse.

The BS of Fig. 1 equally splits the received power, which is equivalent to randomly forwarding the incoming photons to two distinct outputs, hence at the input of each PBS we have the average signal power per pulse of $\frac{\gamma n_S}{2}$ photons. It should be noted that the HWP of Fig. 1 is used for appropriately rotating the polarization, in order for identical APDs to be used for detection in both bases, namely $\oplus$ and $\otimes$.

Then the signal output by the BS is passed to the PBSs of Fig. 1, which is used for directing the polarized photons to the designated APDs. If a photon at the input of a PBS is polarized according to the same basis as that of the PBS itself, then this photon can get through the PBS to reach the designated APD associated with the PBS. As a result, the entire signal power of $\frac{\gamma n_S}{2}$ is passed through the PBS to the designated APD. Again, this case corresponds to the measurement characterised by Eq. (1) and Eq. (2), where the basis used for measuring the quantum state is identical to the basis, in which the quantum state was prepared. By contrast, when a photon arriving at the input of a PBS is polarized in a different basis from that of the PBSs, this photon is randomly directed to either of the two distinct outputs of the PBS. Hence, the average signal power is split equally between both outputs of the PBS, leading to the average signal power of $\frac{\gamma n_S}{4}$ at the input of both associated APDs. Again, this case corresponds to the measurement characterised by Eq. (3), Eq. (4), Eq. (5) and Eq. (6), where the measurement basis is different from the basis of the quantum state.

Additionally, background noise n_B per basis contaminates transmitted pulses and each APD is subject to the dark-count noise having an average power of n_D. As a result,

[1] The process of discarding detected photons for which the bases used for transmision and detection are different is defined as the sifting process [23].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2017.2712288, IEEE Access

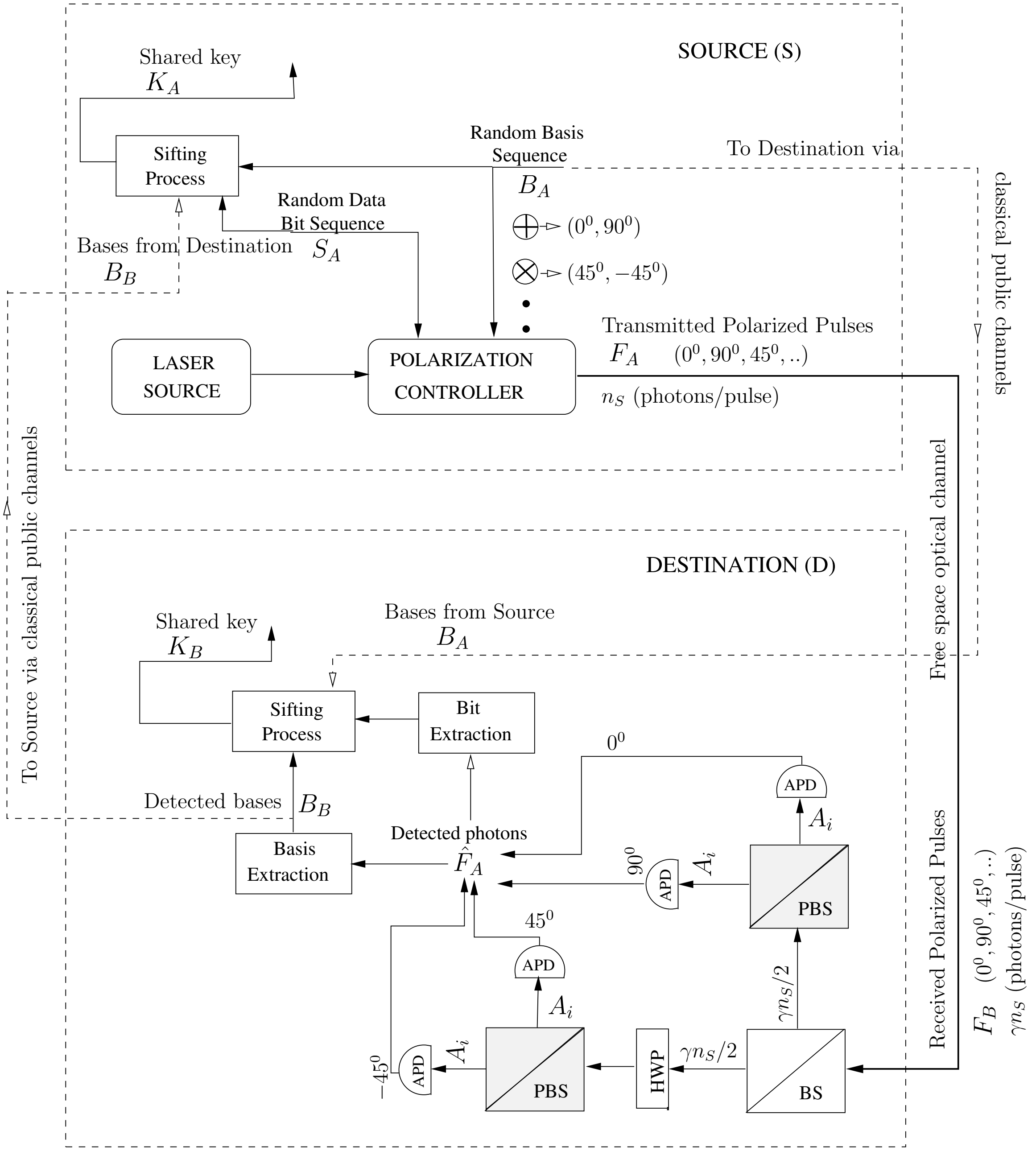


Fig. 1: A simplified schematic of QKD systems [23], [25]. The beam splitter (50:50) (BS) is used for selecting random choices of the polarization bases, namely $\oplus$ and $\otimes$. The half-wave plate (HWP) is invoked for converting the basis $\otimes$ to the basis $\oplus$ and vice versa. The polarizing beam splitters (PBS) are used for directing the incoming photons to the designated avalanche photo-diodes (APD).

each APD is also subject to the additive noise having the average power of $n_N = n_B/2 + n_D$. Provided that the APD can only capture a fraction η of the total power of the signal arrived, we have an average power A_i per pulse (bit interval) captured by the APDs, as listed in Table II for the different cases corresponding to different x-polarization of the transmitted pulses and y-polarization of the APDs, $x, y \in \left(0^0, 90^0, -45^0, 45^0\right)$. The state of the pulse having the average power A_i listed in Table II may be represented by a coherent state of $|\sqrt{A_i}\rangle$ [37]

$$|\sqrt{A_i}\rangle \quad = \quad \sum_{n=0}^{\infty} a_n |n\rangle, \tag{10}$$

where we have $a_n = \frac{(\sqrt{A_i})^n}{\sqrt{n!}} e^{-\frac{A_i}{2}}$, while $|n\rangle$ represents the state of the pulse when there are n photons detected within the pulse duration. Accordingly, we have the probability of detecting $n = 0$ and $n = 1$ photon within a pulse duration (bit interval) as:

$$P(n = 0|_{A_i}) \quad = \quad |a_0|^2 = e^{-A_i}, \tag{11}$$

	Bit intervals	1	2	3	4	5	6	7	8	9	10
Order	**SOURCE (S)**										
①	Raw key of the bit stream (S_A)	1	0	1	0	1	1	0	1	1	0
①	Bases for transmission at source (B_A)	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\otimes$
②	Polarised photons transmitted (F_A)	90^0	0^0	45^0	-45^0	90^0	45^0	-45^0	45^0	90^0	-45^0
⑥	Detection bases at destination (B_B)	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	NA
⑦	Sift process at source (x means occurrence of the sift event)	x	x	x	x	x		x	x	x	
⑧	Resultant shared key at source (K_A)	1	0	1	0	1	NA	0	1	1	NA
	DESTINATION (D)										
③	Polarised photons received at destination (F_B)	90^0	0^0	45^0	-45^0	90^0	45^0	-45^0	45^0	90^0	ND
④	Polarised photons detected at destination ($\hat{F}_A$)	90^0	0^0	-45^0	-45^0	90^0	0^0	-45^0	45^0	90^0	ND
⑤	Detection bases at destination (B_B)	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	NA
⑥	Bases selected at transmitter (B_A)	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\otimes$
⑦	Sift process at destination (x means occurence of the sift event)	x	x	x	x	x		x	x	x	
⑧	Resultant shared key at destination (K_B)	1	0	0	0	1	NA	0	1	1	NA

TABLE I: A simplified numerical example of the communications in the QKD system portrayed in Fig. 1, when supported by perfect classical channel. The circled numbers indicate the relative order of processes occurring in the system. The gray cells indicate erroneous results that are unknown to the system, while NA/ND indicates that no-available values/no-detections are determined by the system.

Basis and polarization of transmitted and detected photons	The average received power A_i (photons/pulse), $i \in (1,2,3)$
$x = y$	$A_1 = \eta(\frac{\gamma n_S}{2} + n_N)$
$x \neq y$ and $x, y \in \oplus$	$A_2 = \eta n_N$
$x \neq y$ and $x, y \in \otimes$	$A_2 = \eta n_N$
$x \in \oplus$ and $y \in \otimes$	$A_3 = \eta(\frac{\gamma n_S}{4} + n_N)$
$x \in \otimes$ and $y \in \oplus$	$A_3 = \eta(\frac{\gamma n_S}{4} + n_N)$

TABLE II: The average signal power captured by an APD in Fig. 1, where x is the polarization of the transmitted photons, while y is the designated polarization of an APD, $x, y \in (0^0, 90^0, -45^0, 45^0)$.

$$P(n = 1|_{A_i}) \quad = \quad |a_1|^2 = A_i e^{-A_i}. \qquad (12)$$

Let us define P_{sift} to be the probability of a sift-event, where only a single photon is detected from all ADPs of Fig. 1 and the APD detecting the photon has the same basis as that used at S for transmission during the bit interval. Accordingly, the sift-event is encountered in two cases. More specifically, Case 1 relates to sift event having no errors in the shared key, while Case 2 relates to that having errors in the shared key, as in the 3^{rd} bit interval of Table I.

In Case 1, $n = 0$ photon is registered by both APDs of a PBS (top or left PBS of Fig. 1) having a basis that is different from the basis used for transmission at S. At the same time, in the other two APDs of the other PBS (top or left PBS of Fig. 1) having an identical basis, an APD associated with the identical polarization detects $n = 1$ photon, while the other APD associated with a different polarization detects $n = 0$ photon. As summarised in Table II, in Case 1 there exist two APDs having an average input power of A_3, given the associated detection result of $n = 0$, while one APD of the other two APDs has an average input power of A_1 given the associated detection result of $n = 1$. Additionally, the fourth APD has an average input power of A_2, given the associated detection result of $n = 0$ photon. As a result, the probability of Case 1 is given by:

$$P_{Case1} \quad = \quad \left[P_{(n=0|A_3)}\right]^2 P_{(n=1|A_1)} P_{(n=0|A_2)}. \qquad (13)$$

In contrast to Case 1, in Case 2 $n = 1$ photon is detected by the APD having the same basis but a different polarization, when compared to the photon that has arrived. At the same time, the APD having the same polarization as the photon that has just arrived detects erroneously $n = 0$ photon. Simultaneously, the other two APDs associated with the basis that is different from that of the photon that has just arrived both detect as $n = 0$ photon. In this case, errors are imposed on the system, as demonstrated by the numerical example detailed in Table I, where there is an error at the 3^{rd} bit interval. Accordingly, upon similarly mapping Case 2 to the value x, y of the polarization given in Table II, the error probability $P_{error} = P_{Case2}$ can be calculated from Eq. (11) and Eq. (12) as:

$$P_{error} \quad = \quad P_{Case2} = \left[P_{(n=0|A_3)}\right]^2 P_{(n=0|A_1)} P_{(n=1|A_2)} \qquad (14)$$

By substituting Eq. (11) and Eq. (12) into Eq. (13) and Eq. (14), the probability P_{sift} may be formulated as:

$$\begin{aligned} P_{sift} \quad &= \quad \underbrace{e^{-\eta(\gamma n_S + 4n_N)} \eta(\gamma n_S/2 + n_N)}_{P_{Case1}} + \\ &\quad \underbrace{e^{-\eta(\gamma n_S + 4n_N)} \eta n_N}_{P_{Case2}}, \\ &= \quad \frac{\eta(\gamma n_S + 4n_N)}{2e^{\eta(\gamma n_S + 4n_N)}}, \qquad (15) \end{aligned}$$

where probability $P_{error} = P_{Case2}$ characterising the occurrence of an error-event can be calculated by

$$P_{error} \quad = \quad \frac{\eta n_N}{e^{\eta(\gamma n_S + 4n_N)}}. \qquad (16)$$

Based on an approach similar to that of Eq. (9), the QKD system has a BER of:

$$\begin{aligned} BER &= \frac{P_{error}}{P_{sift}}, \\ &= \frac{n_N}{\gamma n_S/2 + 2n_N}. \end{aligned} \tag{17}$$

III. Multi-user Quantum Key Distribution System

In this section, we portray our NC-CQKD-FSO system by firstly describing the general system architecture in Section III-A in order to facilitate the presentation of the associated performance criteria used for evaluating it in Section III-B. This leads to insights presented in Section III-C both concerning our FSO schemes and the Network Coding (NC) schemes detailed in Section III-D.

A. System Model

For the sake of readability, we continue to use another numerical example to illustrate the operating principle of our NC-CQKD-FSO system model having two groups, where each group supports $M = 2$ users, as illustrated in Fig. 2, with group A serving user U_1^A and user U_2^A, while group B supporting user U_1^B and user U_2^B. Accordingly, a user in group A commences the key-sharing process in order to form a secret key with a user in group B, where the key-sharing process is based on the popular QKD protocol BB84 [1], mapping the bits of the raw key to the photons for transmitting over the FSO quantum channel.

For example, user U_1^A wishes to have a secret key shared with user U_1^B, while user U_2^A and user U_2^B also wish to have another secret shared key. More specifically, as seen in Fig. 2 a quantum channel represented by a thick arrow is used for conveying photons between the two couples of users. The users in the NC-CQKD-FSO system are configured for supporting one another, hence the classical channels represented by the thin arrows are invoked for cooperatively carrying information-bearing bits between the users. Note that due to the symmetric nature of the system, a similar architecture and similar communication protocols can be used for realising the key sharing process in the reverse direction, where the users in group B initialise the process in order to create shared keys with the users in group A. It should be noted that the example of the system model portrayed in Fig. 2 can be generalised for conceiving a larger NC-CQKD-FSO system associated with a $M > 2$ users, where we have $M = \{4, 8, 12, 16, ...\}$.

Let us use the simplified model of Fig. 3 for characterising the communication protocol between two users of the NC-CQKD-FSO system, namely U_i^A(S) of group A and U_j^B(D) of group B, where S initialises the protocol. These two users receive support from the other users in the NC-CQKD-FSO system via the classical channels. More specifically, a simplified numerical example is detailed in Table III.

①-③ of Table III: Similar to the example of Table I, a raw key in the form of a bit stream S_A having $L_{S_A} = 10$ bits in Table III is mapped to the photon stream F_A by applying the mapping rule given in Eq. (7) and Eq. (8) upon basis sequence B_A , where $n_S = 1$ photon having a random polarization is used for carrying a single bit.

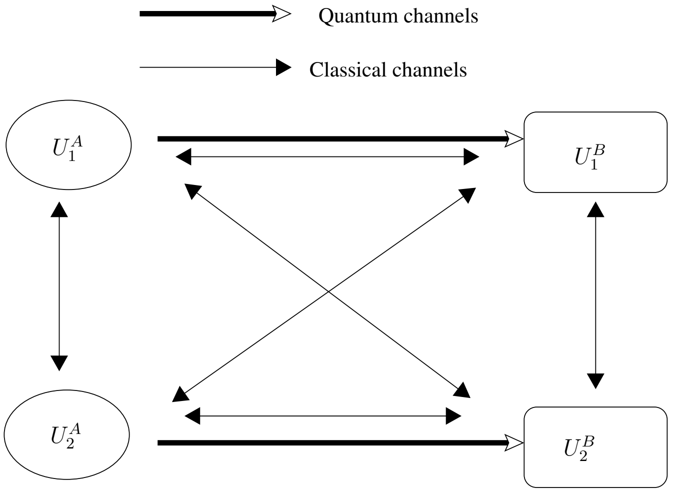


Fig. 2: The proposed multi-user quantum key distribution system comprising two groups, namely group A and group B, establishing shared keys between one user in group A and one user in group B.

④-⑤ of Table III: A fraction γ of F_A that arrived the receiver of D in Fig. 1 is represented by F_B. Then, the photon stream F_B is detected for ultimately providing detection results $\hat{F}_A$, which can be extracted for forming the sequence B_B of Table III representing the random bases passively generated by the BS of Fig. 1 for detecting the photons transmitted from S via the FSO channel. From another perspective, the photon detector at the receiver of D recovers an estimated version $\hat{F}_A$ of the polarised photons F_B arriving at D, which is a fraction γ of the photon stream F_A transmitted by S. The detection results of $\hat{F}_A$ also contain erroneous detections, for example the erroneous detection occurring at the 3^{rd} bit interval of $\hat{F}_A$ in Table III. We also use the similar notation as those in the example detailed in Table I, where the erroneous decisions made by the system are indicated by gray background cells, while the NA notation in the Table III represents the values that are unknown to the system.

⑥-⑦ of Table III: Let us now consider imperfect error-infested classical public channels[2] for exchanging information between S and D about the bases B_A and B_B applied at S and D, respectively. As a result, an estimated version $\hat{B}_A$ of the bases B_A used at S becomes available at D, where an error occurs at the 6^{th} bit interval, as seen in Table III. This error results in an incorrect sift-event at D, which is highlighted by the grey cell at the 6^{th} bit interval of D side of Table III. In the reverse direction spanning from D to S, the basis sequence B_B extracted from the detection results $\hat{F}_A$ in Fig. 1 is also transmitted to S via classical public channels. Hence, S receives an estimated version $\hat{B}_B$ subject to potential errors occurring in the classical public channels. For example, there is an error at the 5^{th} bit interval of $\hat{B}_B$ in Table III,

[2] In our multi-user QKD system, other users in the system can cooperatively transmit basis-related side information. Hence, the information may simultaneously travel through different channels.

which leads to an incorrect sift-event at S.

$\textcircled{8}$ of Table III: Those errors at the $3^{rd}, 5^{th}$ and 6^{th} bit intervals cause the corresponding errors at the resultant keys, namely K_A at S and K_B at D in Table III. As demonstrated by the numerical example of Table III, it should be noted that K_A and K_B generated by the QKD system may be different due to the fact that errors may be inflicted both by the FSO quantum channel and during detection at D as well as by the classical public channels.

In our system, it should be noted that the estimated bases $\hat{B}_B$ and $\hat{B}_A$ are subject to the typical impairments of the classical public channels among all users, which rely on our cooperative protocol, where each user in the system is capable of supporting the others with the aid of Network Coding (NC) [31], [32]. More specifically, to transmit information from a user in group A to a user in group B, all users of group A broadcast their information during the broadcast phases. At the end of the broadcast phases, each user in group A invokes network-coding encoding based on its own information and that recovered from transmissions of the other users in group A during the broadcast phases, in order to construct network-coded information for transmission during the ensuing cooperative phases. Owing to the broadcast nature of wireless transmission, each user in group B can detect a specific version of the information transmitted by a user from group A both during the broadcast and the cooperative phases. Then a network-decoding process is carried out by each user of group B for retrieving its desired information transmitted by its communication party in group A. A similar protocol is invoked for the reverse-direction transmission from group B to group A.

B. Error Ratio in Network Coding Aided Cooperative Quantum Key Distribution Systems

Let us commence with the scenario of having error-free (perfect) classical channels for exchanging information between a pair of users, one in group A and one in group B. The differences between K_A and K_B are caused by the deleterious influence of the FSO channels and by the detection errors at D, which can be characterised[3] by [23]

$$BER_{perfect} \quad = \quad \frac{P_{error}}{P_{sift}}, \qquad (18)$$

where P_{sift} and P_{error} are determined by Eq. (15).

1) Single-User QKD-FSO System: Next, let us consider a single user (SU) QKD-FSO system[4], where the public channel between S and D is a realistic (error prone) wireless channel. Accordingly, we may define a basis-error event in the link spanning from S to D as a sift event at D, where the information representing the basis used at S is erroneously received at D. In other words, the basis-error event happens at D when the sift event occurs at D and simultaneously the wireless channel from S to D is in outage. Hence the probability of the basis-error event is calculated as:

$$P^{SU}_{basis-error-SD} \quad = \quad P_{S-D}P_{sift}, \qquad (19)$$

where P_{S-D} is the outage probability on the classic wireless channel spanning from S to D during a single bit interval of the QKD-FSO system. Similarly, a basis-error event for the direction from D to S occurs at a probability of

$$P^{SU}_{basis-error-DS} \quad = \quad P_{D-S}P_{sift}, \qquad (20)$$

where P_{D-S} represents the outage probability on the classic wireless transmission channel emerging from D to S during a single bit interval of the QKD-FSO system.

It is reasonable to assume that the errors caused by the classical channels can be assumed to flip the bit values representing bases with the same probability. This results in the same probability of changing a specific basis to as that of the reverse corruption. As a result, we may assume the probability P_{sift} to be the same for both scenarios of employing perfect and realistic classical public channels.

Again, the errors due to the basis-error event in both directions, namely from S to D as well as from D to S may cause differences in the shared keys K_A and K_B, as demonstrated by the specific example detailed in Table III. Since K_A and K_B represent the bits successfully recovered in sift events, the differences between K_A and K_B caused by the basis-error event in the direction from S to D can only arise from basis-error events, provided that a sift event has occurred. As a result, the differences reflected by BER corresponding to the S-to-D direction can be equivalently characterised by the conditional probability

$$\begin{aligned} BER^{SU}_{base-SD} \quad &= \quad \text{Prob}(\text{basis-error}_{SD}|\text{sift}) \qquad (21) \\ &= \quad \frac{P_{basis-error-SD}}{P_{sift}}, \end{aligned}$$

where the term "basis-error$_{SD}$" represents the basis-error event caused in the transmission direction from S to D over the classic wireless channel. Similarly, the BER associated with the D-to-S direction can be represented by:

$$BER^{SU}_{base-DS} \quad = \quad \frac{P_{basis-error-DS}}{P_{sift}}. \qquad (22)$$

Due to the fact that there might be overlapping between error events characterised by Eq. (18), those reflected by Eq. (21) and those given by Eq. (22), the accumulated BER of the SU-QKD-FSO system can only be upper-bounded

$$BER^{SU} \leq \underbrace{BER_{perfect} + BER^{SU}_{base-SD} + BER^{SU}_{base-DS}}_{BER^{SU}_{upper}}. \qquad (23)$$

2) Multi-User QKD-FSO System: Let us now consider a multi-user NC-CQKD-FSO system, where again basis-related information is exchanging between S and D over different classic wireless channels within the NC-CQKD-FSO system. We may consider the outage probability P^{NC}_{S-D} between two end users, namely user U^A_1 and user U^B_1, to be equivalent

[3] The Qubit Error Ratio (QBER) estimation proposed in [23], [25], which reflects the differences between two photon streams of F_A and $\hat{F}_A$ directly associated with the shared keys, namely K_A and K_B. Hence, the value of the QBER is the same as BER of Eq. (17).

[4] The SU-QKD-FSO system supports a pair of users, namely U^A_1 and U^B_1, which communicate with one another via public channels for setting up a pair of shared keys, as previously investigated in [23], [24] for the case of having error-free public channels.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2017.2712288, IEEE Access

	Bit intervals	1	2	3	4	5	6	7	8	9	10
Order	**SOURCE (S)**										
①	Raw key of the bit stream (S_A)	1	0	1	0	1	1	0	1	1	0
①	Bases for transmission at source (B_A)	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\otimes$
②	Polarised photons transmitted (F_A)	90^0	0^0	45^0	-45^0	90^0	45^0	-45^0	45^0	90^0	-45^0
⑥	Estimated detection bases at destination ($\hat{B}_B$)	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	NA
⑦	Sift process at source (x means occurrence of the sift event)	x	x	x	x			x	x	x	
⑧	Resultant shared key at source (K_A)	1	0	1	0	NA	NA	0	1	1	NA
	DESTINATION (D)										
③	Transmitted polarised photons present at destination (F_B)	90^0	0^0	45^0	-45^0	90^0	45^0	-45^0	45^0	90^0	ND
④	Polarised photons detected at destination ($\hat{F}_A$)	90^0	0^0	-45^0	-45^0	90^0	0^0	-45^0	45^0	90^0	ND
⑤	Detection bases at destination (B_B)	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	NA
⑥	Estimated bases selected at source ($\hat{B}_A$)	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$
⑦	Sift process at destination (x means occurence of the sift event)	x	x	x	x	x	x	x	x	x	
⑧	Resultant shared key at destination (K_B)	1	0	0	0	1	0	0	1	1	NA

TABLE III: A numerical example of the communications in the QKD system portrayed in Fig. 1, when considering imperfect error-infested classical channels, where the circled numbers indicate the relative order of processes occurring in the system. The gray cells indicate erroneous results that are unknown to the system, while NA/ND indicates that no-values/no-detections are determined by the system.

to P_{S-D} of Eq. (19). As a result of substituting P^{NC}_{S-D} into Eq. (19), we arrive at the probability of basis-error event for the S-to-D direction of our NC-CQKD-FSO system as:

$$P^{NC}_{basis-error-SD} = P^{NC}_{S-D} \times P_{sift}. \quad (24)$$

Similarly, by using Eq. (20), Eq. (21), Eq. (22) and the approximation of Eq. (23), we can upper-bound the BER of the multi-user NC-CQKD-FSO system as:

$$BER^{NC} \le \underbrace{BER_{perfect} + BER^{NC}_{base-SD} + BER^{NC}_{base-DS}}_{=BER^{NC}_{upper}}. \quad (25)$$

Additionally, due to the fact that there are on average ψ photons transmitted per pulse, typically the ratio of the Key Rate per Pulse (KRpP) is used for evaluating the performance of the QKD systems [17], [38], [39]. Naturally, the KRpP may be calculated from the BER in different systems, namely $BER_{perfect}$ of Eq. (18) for the system relying on idealised error-free classical public channels, BER^{SU} of Eq. (23) derived for the SU-QKD-FSO system, or BER^{NC} of Eq. (25) used for the NC-CQKD-FSO system, are as follows:

$$KRpP = (1 - BER)P_{sift}\psi. \quad (26)$$

Accordingly, we may also compute the Key Rate (KR) of the QKD systems as:

$$KR = (1 - BER)P_{sift}\psi R_b, \quad (27)$$

where R_b is the original bit rate of the raw key.

C. Free Space Optical Quantum Channels

Both the BER-performance of the SU-QKD-FSO system of Eq. (23) and that of the NC-CQKD-FSO system in Eq. (25) are dependent on $BER_{perfect}$ formulated in Eq. (18). The value of $BER_{perfect}$ is mainly influenced by the associated FSO transmission integrity, which is characterised by the fraction γ. In this section, we provide details regarding the estimation of γ, which results in different estimates of P_{sift} and P_{error} in Eq. (15) as well as of $BER_{perfect}$ in Eq. (18).

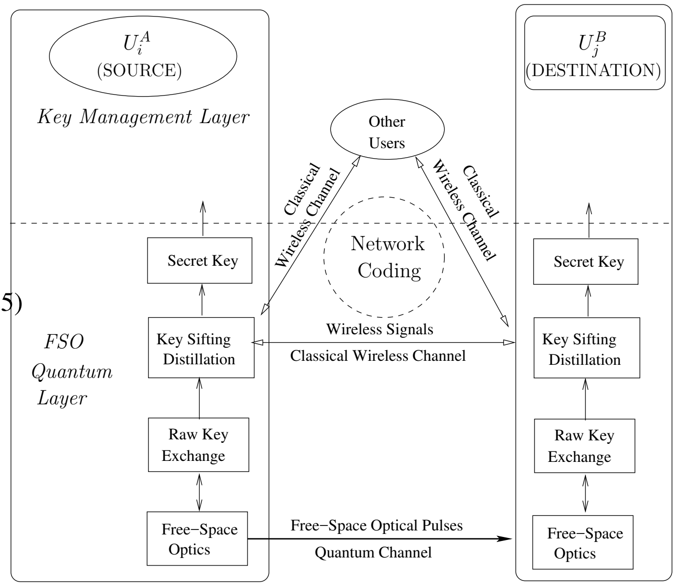


Fig. 3: Communication procedure between a source and a destination through both the FSO quantum channel and the classical wireless channels in the NC-CQKD-FSO system of Fig. 2.

The term γ of Eq. (15) invoked for characterising the power transfer properties of the FSO channel over a distance L imposed on the QKD system's performance is approximated by [23]–[25]

$$\gamma = \mu e^{-\alpha L}, \quad (28)$$

where μ represents the diffraction losses or the normalised version of the fraction γ, while α is the extinction coefficient.

1) Diffraction loss: The value of μ depends on the Fresnel number of

$$D_f^0 \quad = \quad \left(\frac{\pi d_1 d_2}{4\lambda L}\right)^2, \tag{29}$$

where d_1 is the transmit aperture diameter and d_2 is the receiver's aperture diameter, while λ is the wavelength of the optical signal.

In the near-field region having $D_f^0 >> 1$, the parameter μ is bounded by [23], [40]

$$\mu_{NF,LB} \quad \leq \quad \mu \leq \mu_{NF,UB}, \tag{30}$$

where the upper bound $\mu_{NF,UB}$ can be calculated by [23]

$$\mu_{NF,UB} \quad = \quad \min(D_f^0, 1), \tag{31}$$

while the lower bound $\mu_{NF,LB}$ is given by [23]

$$\begin{aligned}\mu_{NF,LB} \quad = \quad & \frac{8\sqrt{D_f^0}}{\pi} \int_0^1 \exp\left(\frac{-D(d_2 x)}{2}\right) \\ & \times \left(\arccos(x) - x\sqrt{1-x^2}\right) J_1\left(4x\sqrt{D_f^0}\right) dx,\end{aligned} \tag{32}$$

where $J_1(.)$ is the first-order Bessel function. The spherical-wave structure function $D(\rho)$ of Eq. (32) is calculated for the worse-case scenario of having $d_1 = d_2$ as [23]:

$$D(\rho) \quad = \quad 51\sigma_R^2 \left(D_f^0\right)^{5/12} \rho^{5/3}, \tag{33}$$

where σ_R^2 is the Rytov variance [41] of

$$\sigma_R^2 \quad = \quad 1.24 \left(\frac{2\pi}{\lambda}\right)^{7/6} C_n^2 L^{11/6}, \tag{34}$$

with C_n^2 ranging from 10^{-13} to 10^{-17} representing the altitude-dependent index of the refractive structure parameter [42].

By contrast, in the far-field region having $D_f^0 << 1$, the value of μ can be calculated by [40]

$$\begin{aligned}\mu_{FF} \quad = \quad & \frac{8\sqrt{D_f^0}}{\pi} \int_0^1 \exp\left(\frac{-D(d_2 x)}{2}\right) \\ & \times \left(\mathrm{arcos}^{-1}(x) - x\sqrt{1-x^2}\right) J_1\left(4x\sqrt{D_f^0}\right) dx,\end{aligned} \tag{35}$$

where the spherical-wave structure function $D(\rho)$ of Eq. (35) can be calculated by

$$D(\rho) \quad = \quad 1.09 \left(\frac{2\pi}{\lambda}\right)^2 C_n^2 L \rho^{5/3}. \tag{36}$$

2) Bounds γ, P_{sift} and P_{error} : By substituting $\mu_{NF,UB}$ of Eq. (31), $\mu_{NF,LB}$ of Eq. (32) and μ_{FF} of Eq. (35) into Eq. (28), we obtain the corresponding bounds of the fraction γ, namely $\gamma_{NF,UB}, \gamma_{NF,LB}$ and γ_{FF}. As readily seen in Fig. 4(a), $\gamma_{NF,UB}$ and γ_{FF} can loosely serve as the upper bound and lower bound in both near-field and far-field regions. Hence, in reference [23] $\gamma_{NF,UB}$ and γ_{FF} were convenient used as bounds for covering both the near-field and far-field regions as:

$$\underbrace{\mu_{FF} \mathrm{e}^{-\alpha L}}_{=\gamma_{FF}} \quad \leq \quad \gamma \leq \underbrace{\mu_{NF,UB} \mathrm{e}^{-\alpha L}}_{=\gamma_{NF,UB}}, \tag{37}$$

However, the near-field model may produce a range of γ values in the near-field region that is more accurate than that provided by the far-field model. Similarly, the far-field model may provide more accurate values of γ in the far-field region than those suggested the near-field model. As a result, when a more accurate value range of γ is sought, the following bounds should be used

$$\gamma_{LB} \quad \leq \quad \gamma \leq \gamma_{UB}, \tag{38}$$

where the upper bound γ_{UB} is determined by:

$$\gamma_{UB} = \left\{ \begin{array}{rcl} \gamma_{NF,UB} & : & \text{If } D_f^0 > T_{near} \\ (\gamma_{NF,UB} + \gamma_{FF})/2 & : & \text{If } T_{far} \leq D_f^0 \leq T_{near} \\ \gamma_{FF} & : & \text{If } D_f^0 < T_{far} \end{array} \right., \tag{39}$$

while the lower bound γ_{LB} is calculated by:

$$\gamma_{LB} = \left\{ \begin{array}{rcl} \gamma_{NF,LB} & : & \text{If } D_f^0 > T_{near} \\ (\gamma_{NF,LB} + \gamma_{FF})/2 & : & \text{If } T_{far} \leq D_f^0 \leq T_{near} \\ \gamma_{FF} & : & \text{If } D_f^0 < T_{far} \end{array} \right., \tag{40}$$

where the region having $T_{far} \leq D_f^0 \leq T_{near}$ is the transition region between the near-field and far-field regimes. The bounds of γ_{UB} and γ_{LB}, as plotted in Fig. 4(b), are tighter compared to those of Eq. (37), as plotted in Fig. 4(a). As a result, we will use the approximation of γ in Eq. (38) for our subsequent calculations.

When we have a convex function $f(x) \equiv xe^{-x}$ for $0 \leq x < 2$ associated with a positive derivative for $0 \leq x < 1$, P_{sift} of Eq. (15) may be approximated by

$$\underbrace{\frac{\eta(\gamma_{LB} n_S + 4n_N)}{2e^{\eta(\gamma_{LB} n_S + 4n_N)}}}_{=P_{sift}^{Min}} \leq P_{sift} \leq \underbrace{\frac{\eta(\gamma_{UB} n_S + 4n_N)}{2e^{\eta(\gamma_{UB} n_S + 4n_N)}}}_{=P_{sift}^{Max}}, \tag{41}$$

provided that the condition $\eta(\gamma_{LB} n_S + 4n_N) < 1$ is satisfied.

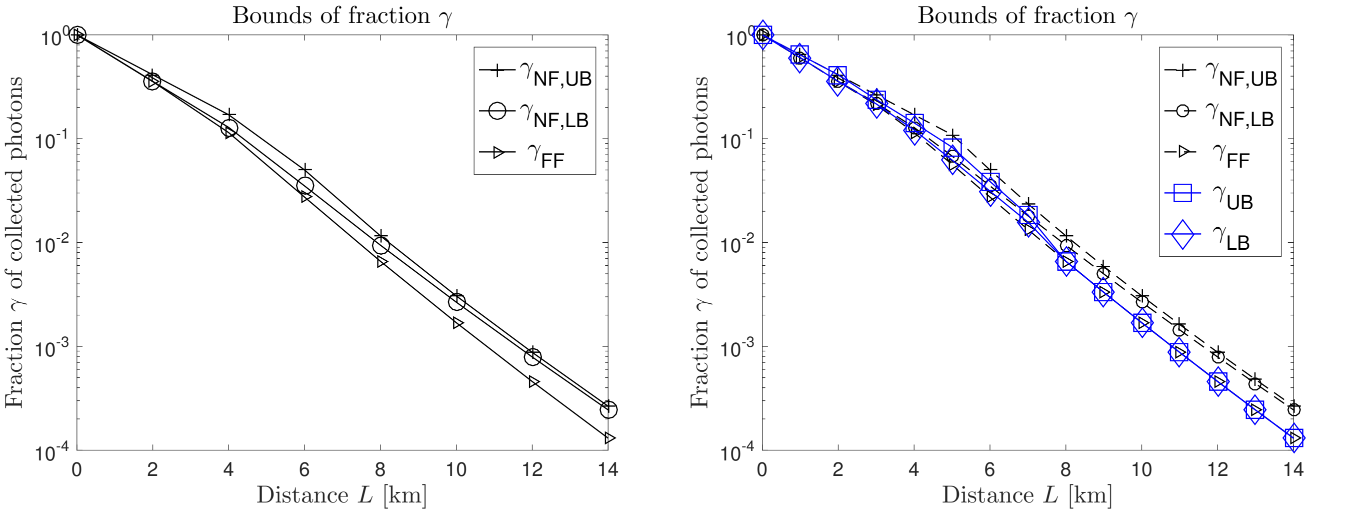
Similarly, considering a concave function $g(x) \equiv e^{-x}$ having a negative derivative for $x \geq 0$, the probability P_{error} of Eq. (16) may obey the following approximation

$$\underbrace{\frac{\eta n_N}{e^{\eta(\gamma_{UB} n_S + 4n_N)}}}_{=P_{error}^{Min}} \leq P_{error} \leq \underbrace{\frac{\eta n_N}{e^{\eta(\gamma_{LB} n_S + 4n_N)}}}_{=P_{error}^{Max}}. \tag{42}$$

Accordingly, by applying the bounds presented in Eq. (41) and Eq. (42) to Eq. (18), we may approximately calculate the $BER_{perfect}$ according to:

$$\underbrace{\frac{P_{error}^{Min}}{P_{sift}^{Max}}}_{=BER_{perfect,LB}} \quad \leq BER_{perfect} \leq \quad \underbrace{\frac{P_{error}^{Max}}{P_{sift}^{Min}}}_{=BER_{perfect,UB}} \quad . \tag{43}$$

As a benefit of having the tight bounds of γ characterised by Eq. (38) and plotted in Fig. 4(b), the discrepancy between the bounds of P_{sift} in Eq. (41), P_{error} in Eq. (42) and $BER_{perfect}$ in Eq. (43) can be readily observed in Fig. 5(a), Fig. 5(b) and Fig. 5(c), respectively. This observation suggests that we may obtain fairly accurate results, even when we employ the worst-case bound of γ, P_{sift} and P_{error} for producing BER_{upper}^{SU} of Eq. (23) and BER_{upper}^{NC} presented in the subsequent sections.



(a) Bounds of γ characterised by Eq. (37)

(b) Bounds of γ characterised by Eq. (38) for a transition region of ($T_{far} = 0.5 \leq D_f^0 \leq T_{near} = 5$)

Fig. 4: Comparison between the bounds of γ vs. the distance when considering the FSO parameters of Table IV.

D. Network Coding aided Cooperative Transmission over Classical Public Channels

In order to proceed with the sifting process, where information related to the bit interval and to the bases used has to to be communicated to both parties of the key sharing protocol, public classical channels may be used for connecting the two parties.

Let us first characterise transmissions over public channels between two users in the SU-QKD-FSO system corresponding to the case of having $M = 1$, where two direct wireless links[5] between U_1^A (S) and U_1^B (D) may be supported by a near-capacity channel coding scheme, which can be designed for operating close to the channel capacity [43]. As an upper-bound performance, we assume that a perfect capacity-achieving coding scheme is employed for operating at exactly the Continuous-Input Continuous-Output Memoryless (CCMC) channel capacity, which has an outage probability of [44]

$$P_{SD}^{SU} = P_{DS}^{SU} = 1 - \exp\left(\frac{1-2^R}{SNR}\right), \tag{44}$$

where R is the information rate of the transmission link, while SNR is the signal to noise ratio at the receiver. We consider the model of a single wireless transmission link associated with the transmitted and received signals of x and y, respectively

$$y = hx + n \tag{45}$$

where again $h = h_s h_f$ is the complex-valued fading coefficient that comprises two components, namely the block fading coefficient h_s, which is constant for all symbols within a transmission frame and a fast fading (small-scale fading) coefficient h_f, which fluctuates on a symbol-by-symbol basis. Finally, n is the AWGN process having a variance of $N_0/2$ per dimension.

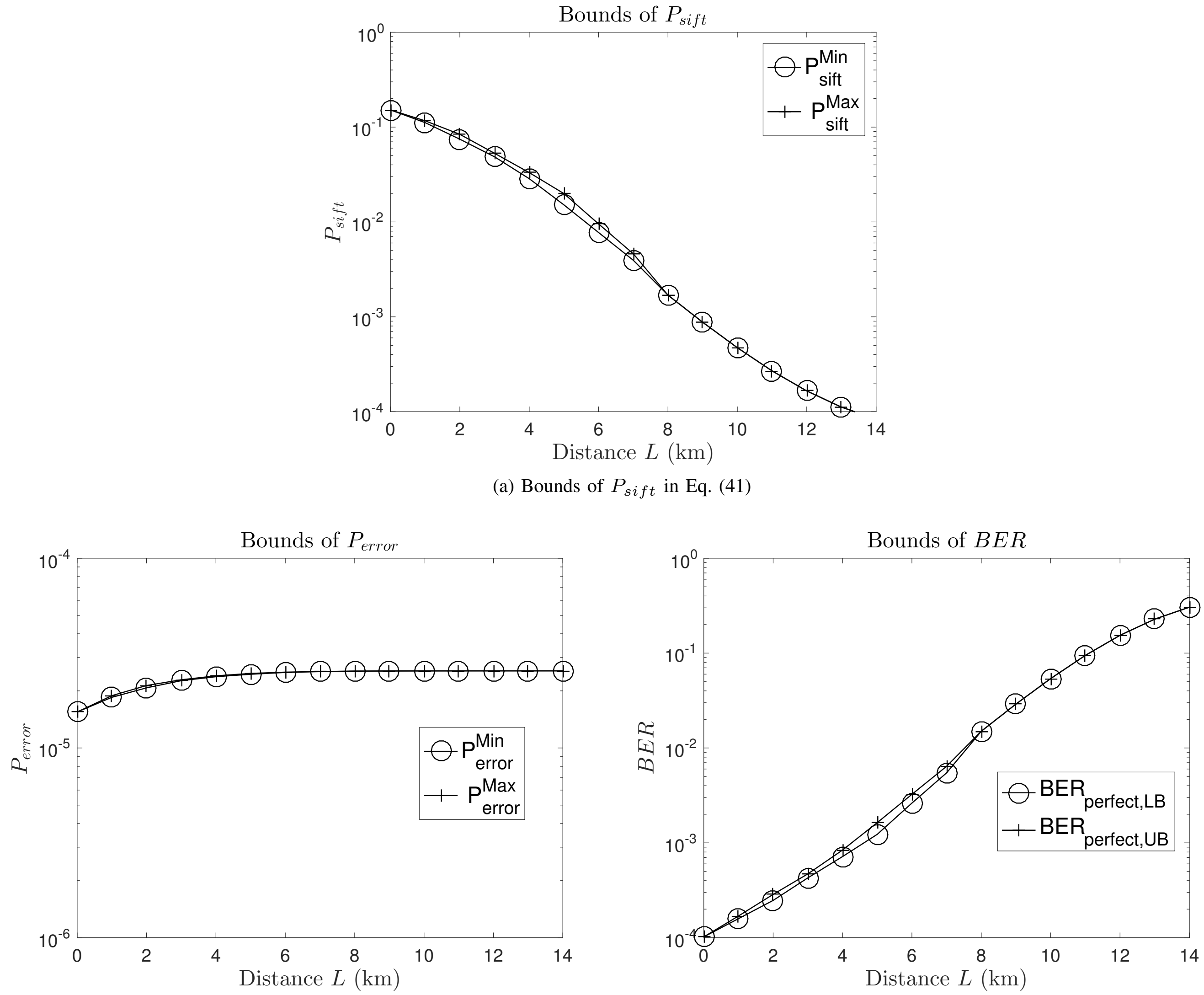
By contrast, in the multi-user NC-CQKD-FSO system portrayed by Fig. 2 and Fig. 3, the transmission over public channels from group A having M users to group B containing M users is arranged on a session by session basis, where the network coding scheme of [34] is reformulated for supporting the NC-CQKD-FSO system. In each public transmission session of the NC-CQKD-FSO system, there are two sets of phases, namely the broadcast phase (BP) and the cooperative phase (CP). Let us consider an example of the system having $M = 2$ for demonstrating the details of both transmission phases, where each of the $M = 2$ users transmits $k_1 = 1$ information message during the BP and $k_2 = 1$ parity message during the CP as seen below:

$$\begin{aligned}
&\underline{\text{Broadcast phases}}\\
&\text{BP 1} \quad : U_1^A \xrightarrow{m_1(1)} U_1^B, U_2^B \text{ and } U_2^A,\\
&\text{BP 2} \quad : U_2^A \xrightarrow{m_2(2)} U_1^B, U_2^B \text{ and } U_1^A,\\
&\underline{\text{Cooperative phases}}\\
&\text{CP 1} \quad : U_1^A \xrightarrow{\boxplus 1(1)=m_1(1)+m_2(2)} U_1^B, U_2^B \text{ and } U_2^A,\\
&\text{CP 2} \quad : U_2^A \xrightarrow{\boxplus 2(2)=m_1(1)+2m_2(2)} U_1^B, U_2^B \text{ and } U_1^A,
\end{aligned}$$

where $m_i(j)$ is the message broadcast by user U_i^A during BP j, while the parity message $\boxplus i(j)$ containing a linear combination of the information messages $m_1(1)$ and $m_2(2)$ is broadcast during CP j. Then, the transmission session can be summarised by a transfer matrix having two rows and 4 columns, where the original version $\boldsymbol{G}_{2\times4}$ corresponds to the case of having a successful transmission in every link [32]

$$\boldsymbol{G}_{2\times4} = \left[\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{array}\right]. \tag{46}$$

[5] In SU-QKD-FSO, there are only two users communicating with one another, hence the two users are considered to be connected by two direct public wireless transmission links.



(a) Bounds of P_{sift} in Eq. (41)

(b) Bounds of P_{error} in Eq. (42)

(c) Bounds of $BER_{perfect}$ in Eq. (43)

Fig. 5: Comparison between the bounds of P_{sift} of Eq. (41), P_{error} of Eq. (42) and $BER_{perfect}$ of Eq. (43) vs. the distance in the FSO system having the parameters listed in Table IV.

When it comes to an arbitrary transmission session, the original transfer matrix of Eq. (46) is modified according to the algorithms detailed in [33] for reflecting the actions of the transmission session, in order to construct the modified matrix $\boldsymbol{G}_{2\times 4}^{'}$. Accordingly, $\boldsymbol{G}_{2\times 4,U_1^B}^{'}$ and $\boldsymbol{G}_{2\times 4,U_2^B}^{'}$ represents the results of the transmission session spanning from U_1^A and U_2^A to U_1^B as well as from U_1^A and U_2^A to U_2^B, respectively. It was shown in [32] that a larger transfer matrix associated with a more complex network coding scheme characterised by the transfer matrix $\boldsymbol{G}_{4\times 8}$, $\boldsymbol{G}_{8\times 16}$, or larger, results in a more powerful network coding scheme. Naturally, this comes with the cost of requiring a more complex NC scheme at each user[6] in the NC-CQKD-FSO system of Fig. 2.

We adopt the conventional C mode [34] of the network-coding codec, where no adaptive mechanism is activated during the cooperative phases and where the network-code decoding process is triggered at the end of the cooperative phases of the transmission session. Accordingly, the outage probability of the transmission between[7] a user in group A and a user in group B is bounded by [33]

$$P_{SD}^{NC} \leq \underbrace{\Omega + \binom{E+F}{F} \frac{\left(P_{SD}^{SU}\right)^{M+k_2}\left(1-P_{SD}^{SU}\right)}{1-P_{SD}^{SU}-\frac{E}{F+1}P_{SD}^{SU}} \frac{1-R_o^M}{1-R_o}}_{=P_{SD,upper}^{NC}}, \quad (47)$$

[6] A similar transmission protocol can be used for the direction spanning from group B to group A, hence both a network-coding encoder and decoder are required at each user in the NC-CQKD-FSO system of Fig. 2.

[7] Due to the symmetry of the NC-CQKD-FSO system, the outage probability of the transmission in the direction from a user in group A to a user in group B is equal to that for the inverse direction. Hence, we have $P_{SD}^{NC} = P_{SD}^{NC}$.

$$P_{SD}^{NC} \geq \underbrace{\frac{\binom{E+F}{F}\left(P_{SD}^{SU}\right)^{F+1}\left[\left(\frac{P_{SD}^{SU}}{E+F}\right)^{Mk_1} - \left(1-P_{SD}^{SU}\right)^{Mk_1}\right]}{\left(1-P_{SD}^{SU}\right)^{1-M}\left(\frac{P_{SD}^{SU}}{E+F}+P_{SD}^{SU}-1\right)}}_{=P_{SD,lower}^{NC}}, \tag{48}$$

where we have $E = (Mk_1 - 1)$, $F = Mk_2$ and $R_0 = (1 - P_{SD}^{SU})(P_{SD}^{SU})^{k_2-1}$, while the term Ω of Eq. (47) is given by

$$\Omega = \left[\binom{k_1+k_2-1}{k_2} - \binom{E+F}{F}\right]\frac{\left(P_{SD}^{SU}\right)^{M+k_2}\left(1-P_{SD}^{SU}\right)}{1-P_{SD}^{SU}-\frac{E}{F+1}P_{SD}^{SU}}. \tag{49}$$

It is important to note that Eq. (47) and Eq. (48) hold when the outage of all the wireless transmission link occurs with the same probability P_{SD}^{SU}. This condition can be achieved, when the distance between the users is the same, while the same transmit power is applied for the wireless transmission links of all users. Alternatively, a power control mechanism may be employed for maintaining a similar SNR value at the receiving party of each wireless transmission link.

The estimated P_{SD}^{NC} is especially useful for assisting the design process of large-scale multi-user NC-CQKD-FSO systems, for example $M = 8, 80$ or higher, as illustrated in Fig. 6. Accordingly, the upper bound of Eq. (47) may be used for predicting the worse-case scenario, while the lower bound of Eq. (48) may be used as actual values of P_{SD}^{NC} for large-scale multi-user NC-CQKD-FSO systems.

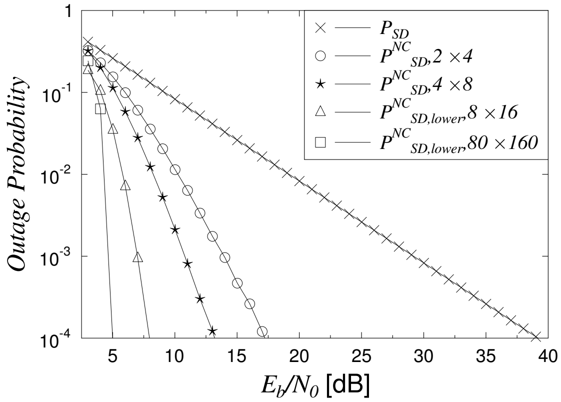


Fig. 6: The outage probability of the network coding assisted wireless public channels in the multi-user NC-CQKD-FSO system, for $M = 2, 4, 8, 80$ user pairs, when employing an idealised capacity-achieving channel coding scheme having a coding rate of $R = 0.5$ operating exactly at the Continuous-Input Continuous-Output Memoryless channel's (CCMC) capacity.

IV. Performance and Analysis

In this section, we first characterise the outage probability, the BER and the key-rate of our QKD system, in order to further highlight benefits of the NC-CQKD-FSO system over the SU-QKD-FSO system.

Parameters	***Values***
Altitude-dependent refractive index	$C_n^2 = 10^{-15}\ m^{-2/3}$
Wavelength	$\lambda = 1550 \times 10^{-9}$ meter
Extinction coefficient	$\alpha = 0.443$ dB/km
Transmit aperture diameter	$d_1 = 0.1$ meter
Receive aperture diameter	$d_2 = 0.1$ meter
Photo-detector efficiency	$\eta = 0.5$
Network coding scheme	$\boldsymbol{G}_{2\times4}$,$\boldsymbol{G}_4$,$\boldsymbol{G}_{8\times16}$
Network coding mode	Convention C mode
Channel coding scheme	'CCMC-achieving'

TABLE IV: Main parameters of the NC-CQKD-FSO system used.

A. BER Performance Evaluation

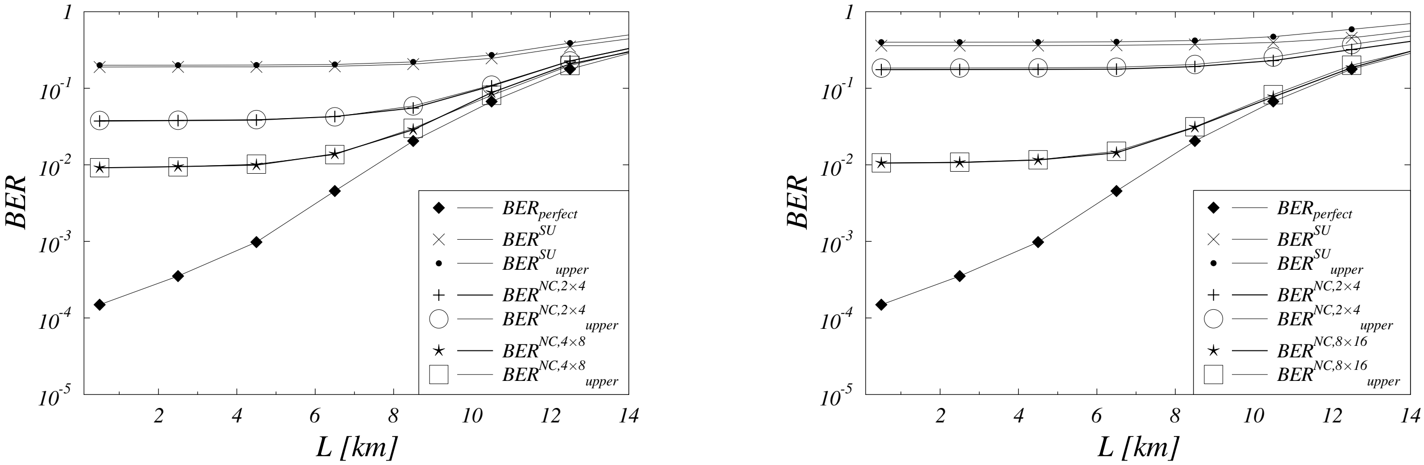
Let us first compare the BER-performance bounds, namely BER_{upper}^{SU} given in Inequality (23) for the SU-QKD-FSO system and BER_{upper}^{NC} defined in Eq. (25) for the NC-CQKD-FSO system to BER^{SU} and BER^{NC}, which were obtained by Monte-Carlo simulations based on the parameters listed in Table IV. As seen in Fig. 7, the BER bounds of BER_{upper}^{SU} and BER_{upper}^{NC} are matched closely the simulated BER curves of BER^{SU} and BER^{NC}. As readily seen from Eq. (23) and Eq. (25), the values of $P_{basis-error-SD}^{SU} = P_{basis-error-DS}^{SU} =$ or in short P_{SD}^{SU} and of $P_{basis-error-SD}^{NC} = P_{basis-error-DS}^{NC}$ or in short P_{SD}^{NC} have a dominant impact on the approximation of the upper bounds, hence the gap between the bounds and the simulated values is proportional to the values of P_{SD}^{SU} and P_{SD}^{NC}. The gap can be seen in Fig. 7, where $P_{SD}^{SU} = \{10^{-1}, 2 \times 10^{-1}\}^{8}$ is satisfied by each of the wireless transmission links in both the SU-QKD-FSO and the NC-CQKD-FSO system. Recall from Fig. 6, where we have $P_{SD}^{SU} >> P_{SD}^{NC}$, that the gap between the bound marked by the square and the simulated curve marked by the stars associated with the NC-CQKD-FSO system in Fig. 7(b) is smaller than that marked by the dot and the cross pertaining to the SU-QKD-FSO system in Fig. 7(b). As a result, the bound BER_{upper}^{NC} may be used for representing the realistic BER-performance BER^{NC} estimated by simulations, namely the BER-performance of the NC-CQKD-FSO system.

B. Improvement in BER performance

Let us adopt the power control mechanism mentioned in Section III-D, which allows both the SU-QKD-FSO and NC-CQKD-FSO systems to meet a certain SNR_r threshold at the receiver of the wireless transmission. This results in guaranteeing that the outage probability P_{SD}^{SU} is better than, namely $P_{SD}^{SU} = \{10^{-1}, 10^{-2}, 10^{-3}, 10^{-4}\}$.

As seen in Fig. 8, a significant BER-performance improvement can be attained by activating the network-coding codec of the NC-CQKD-FSO systems over that of the SU-QKD-FSO using no network-coding. When calculating the ratio $\varPhi = BER^{SU}/BER^{NC}$ between the corresponding BER values of both systems at a given transmission range, of say $L = 0.5$ km, the maximum BER reduction in terms of $\varPhi$ is

[8] The value of P_{SD}^{SU} in Fig. 7 was specifically chosen for the sake of providing a clear presentation.



(a) $P_{SD}^{SU} = 10^{-1}$ resulting in $P_{SD}^{NC,2\times4} = 1.9\times10^{-2}$ and $P_{SD}^{NC,4\times8} = 4.5\times10^{-3}$, which can be seen in Fig. 6.

(b) $P_{SD}^{SU} = 2\times10^{-1}$ corresponding to $P_{SD}^{NC,2\times4} = 9.1\times10^{-2}$ and $P_{SD}^{NC,8\times16} = 5.2\times10^{-3}$, which can be seen in Fig. 6.

Fig. 7: Comparison between the BER-performance bounds given in Inequality (23) for the SU-QKD-FSO system and in Inequality (25) for the NC-CQKD-FSO system to those obtained by Monte-Carlo simulations using the parameters listed in Table IV.

approximately at $\Phi = 2000$ for the case of $P_{SD}^{SU} = 10^{-1}$ in Fig. 8(a), $\Phi = 200$ for the case of $P_{SD}^{SU} = 10^{-2}$ in Fig. 8(b), $\Phi = 20$ for the case of $P_{SD}^{SU} = 10^{-3}$ in Fig. 8(c), and $\Phi = 3$ for the case of $P_{SD}^{SU} = 10^{-4}$ in Fig. 8(c). It may also be seen in Fig. 8 that in order to reach the maximum possible BER-improvement at a minimum system complexity, a suitable network coding scheme should be used. More specifically, the $\boldsymbol{G}_{8\times16}$-based network coding scheme has to be used for the case of having $P_{SD}^{SU} = 10^{-1}$, as seen in Fig. 8(a). By contrast, using less complex $\boldsymbol{G}_{2\times4}$-based network coding scheme is sufficient for $P_{SD}^{SU} = 10^{-4}$, as seen in Fig. 8(d).

C. Improvement in Key Rate Performance

The benefits of employing the NC-CQKD-FSO system can be clearly seen from the key rate KR improvements, as well as from the key rate per pulse gains, as it transpires from Eq. (27). As seen in Fig. 9 that the powerful network coding scheme relying on $\boldsymbol{G}_{8\times16}$ is required for the key rate performance of the NC-CQKD-FSO to reach its best, which is equivalent to the key-rate performance of the SU-QKD-FSO scheme operating over idealised error-free public channels. This is in line with the BER-performance of Fig. 7(b). As seen in Fig. 9(a), Fig. 9(b) Fig. 9(c), when the transmission range L increases, $KRpP$ value portrayed in Fig. 9(a) and the KR value seen in Fig. 9(b) are reduced for all the QKD systems under investigation. It is also suggested that the key rate improvement seen in Fig. 9(c) of the NC-CQKD-FSO over that of SU-QKD-FSO also decreases upon increasing distance L. However, we observe a steady improvement of approximately 55%, when comparing the $KRpP$ or KR of the NC-CQKD-FSO to those of the SU-QKD-FSO system, as seen in Fig. 9(d). The benefits in the key rate KR improvements or in the transmission range L increase may be exploited in the scenarios, where the NC mechanism is activated in the system, when a user requires a higher key rate or moves out of the good transmission range.

V. Conclusions

We have considered realistic error-prone public wireless channels in the context of quantum key distribution (QKD) systems relying on an FSO link. Explicitly, we proposed NC-CQKD-FSO Systems, where our network-coded cooperative systems have been shown to provide a three orders of magnitude BER-performance improvement or up to 55% higher key rates in the scenarios investigated.

References

[1] C. H. Bennett and G. Brassard,, "Quantum cryptography: Public key distribution and coin tossing," in *in Proc. IEEE Int. Conf. Comput. Syst. Signal Process., Bangalore, India 1984*, p. 175179.

[2] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991.

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

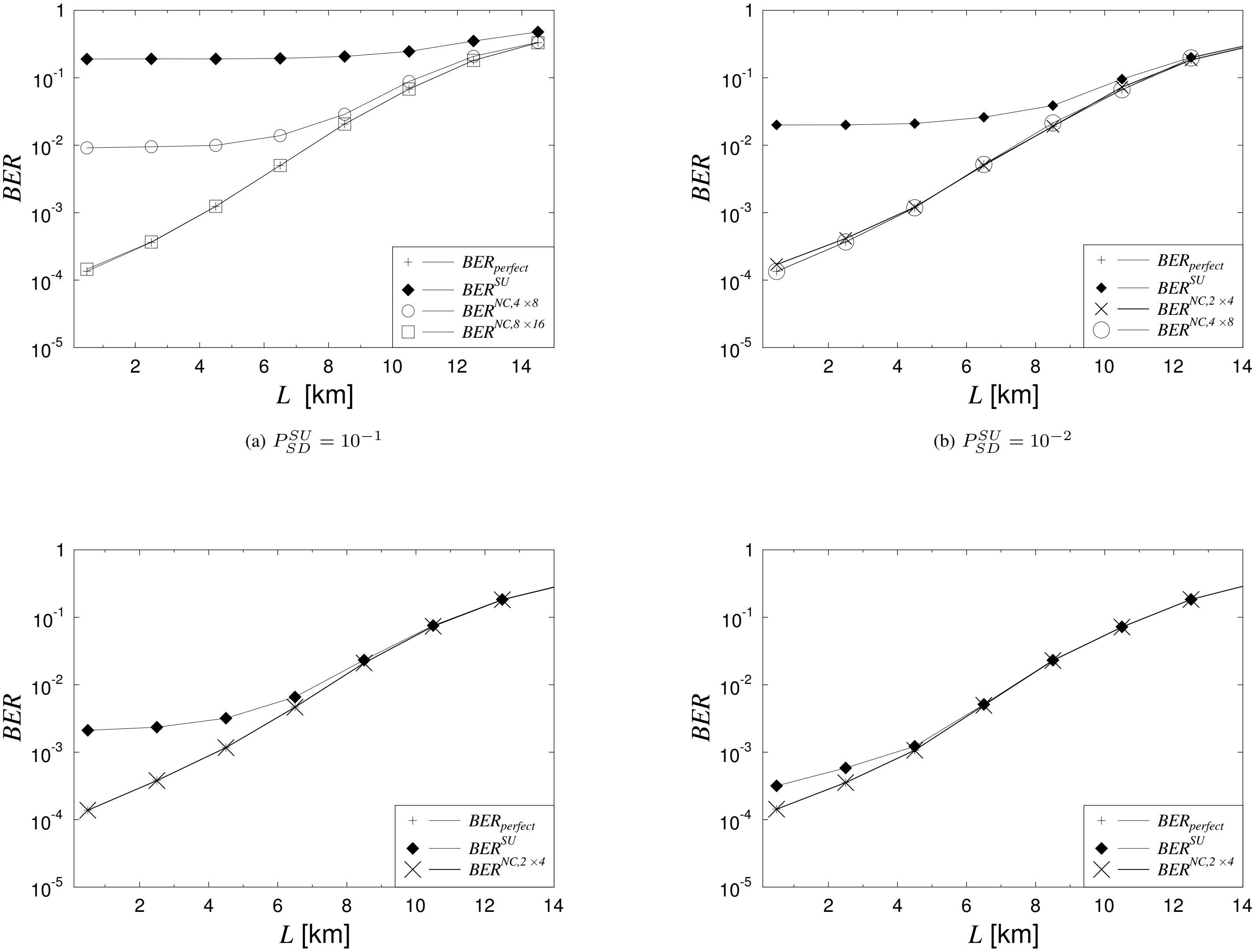
[4] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, p. 010303, Dec 1999.

[5] T. Gehring, V. Haendchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, "Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks," *NATURE COMMUNICATIONS*, vol. 6, OCT 2015.

[6] F. Xu, M. Curty, B. Qi, L. Qian, and H.-K. Lo, "Discrete and continuous variables for measurement-device-independent quantum cryptography," *NATURE PHOTONICS*, vol. 9, pp. 772–773, DEC 2015.

[7] X. Wang, J. Liu, X. Li, and Y. Li, "Generation of stable and high extinction ratio light pulses for continuous variable quantum key distribution," *IEEE Journal of Quantum Electronics*, vol. 51, pp. 1–6, June 2015.

[8] H. P. Yuen, "Security of quantum key distribution," *IEEE Access*, vol. 4, pp. 724–749, 2016.



(a) $P_{SD}^{SU} = 10^{-1}$

(b) $P_{SD}^{SU} = 10^{-2}$

(c) $P_{SD}^{SU} = 10^{-3}$

(d) $P_{SD}^{SU} = 10^{-4}$

Fig. 8: BER-improvement of the NC-CQKD-FSO system, compared to the BER performance of the SU-QKD-FSO system, for different values of $P_{SD}^{SU} = \{10^{-1}, 10^{-2}, 10^{-3}, 10^{-4}\}$.

[9] Y. L. Tang, H. L. Yin, S. J. Chen, Y. Liu, W. J. Zhang, X. Jiang, L. Zhang, J. Wang, L. X. You, J. Y. Guan, D. X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T. Y. Chen, Q. Zhang, and J. W. Pan, "Field test of measurement-device-independent quantum key distribution," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, pp. 116–122, May 2015.

[10] N. Piparo, M. Razavi, and C. Panayi, "Measurement-device-independent quantum key distribution with ensemble-based memories," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, pp. 138–147, May 2015.

[11] V. Scarani and R. Renner, "Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing," *PHYSICAL REVIEW LETTERS*, vol. 100, MAY 23 2008.

[12] 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. 7, pp. 378–381, MAY 2013.

[13] H. Jingzheng, Y. Zhenqiang, C. Wei, W. Shuang, L. Hongwei, G. Guangcan, and H. Zhengfu, "A survey on device-independent quantum communications," *China Communications*, vol. 10, pp. 1–10, Feb 2013.

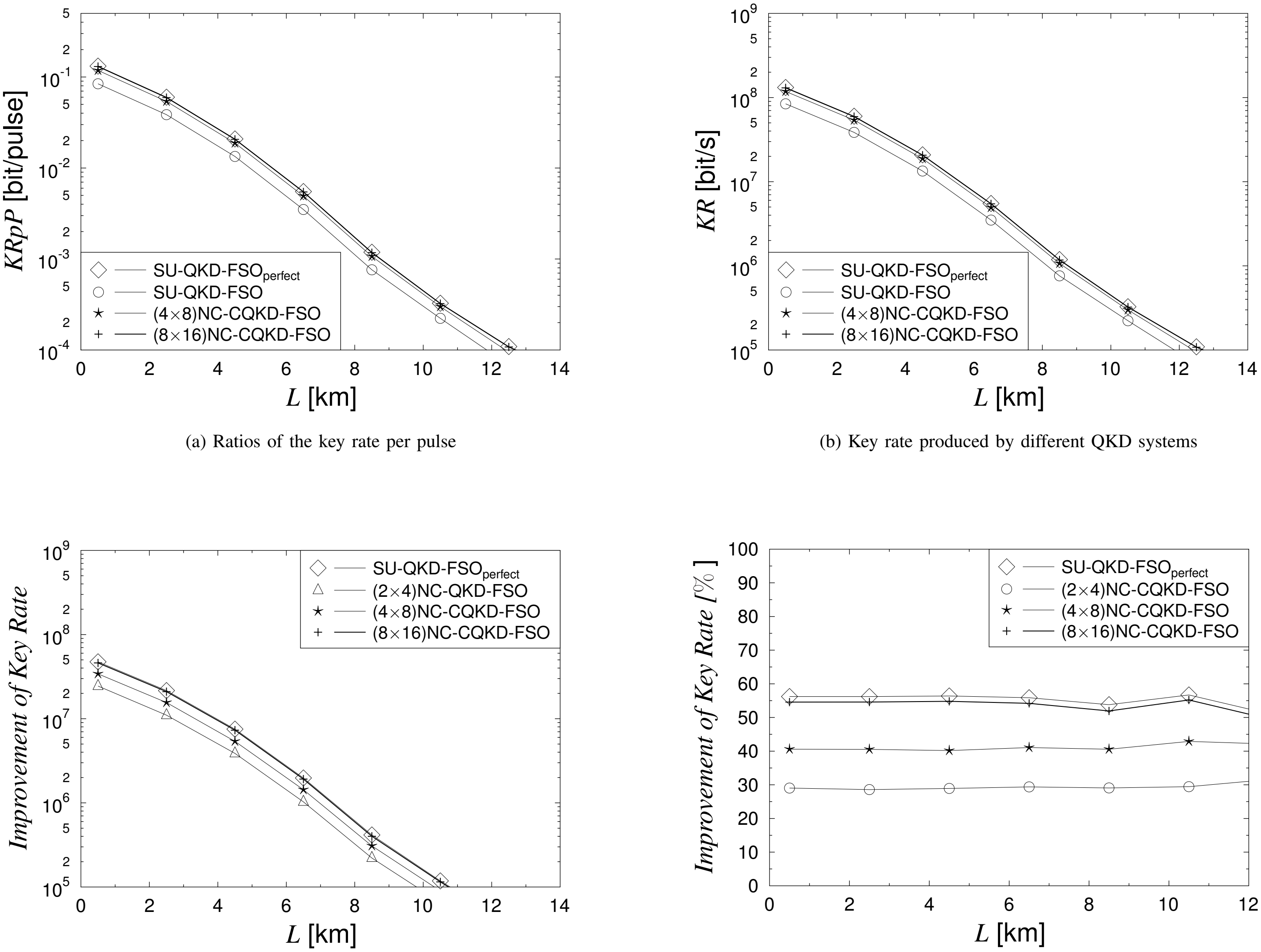
[14] M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, and H. Weinfurter, "Spatial mode side channels in free-space QKD implementations," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, pp. 187–191, May 2015.

[15] J.-P. Bourgoin, B. L. Higgins, N. Gigov, C. Holloway, C. J. Pugh, S. Kaiser, M. Cranmer, and T. Jennewein, "Free-space quantum key distribution to a moving receiver," *Optics Express*, vol. 23, no. 26, pp. 33437–33447, 2015. Times Cited: 00.

[16] M. T. Gruneisen, M. B. Flanagan, B. A. Sickmiller, J. P. Black, K. E. Stoltenberg, and A. W. Duchane, "Modeling daytime sky access for a satellite quantum key distribution downlink," *Optics Express*, vol. 23, no. 18, pp. 23924–23934, 2015. Times Cited: 00.

[17] G. Vallone, D. G. Marangon, M. Canale, I. Savorgnan, D. Bacco, M. Barbieri, S. Calimani, C. Barbieri, N. Laurenti, and P. Villoresi, "Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels," *Physical Review A*, vol. 91, no. 4, 2015.

[18] A. Carrasco-Casado, N. Denisenko, and V. Fernandez, "Correction of



(a) Ratios of the key rate per pulse

(b) Key rate produced by different QKD systems

(c) Improvement of the key rate in bit/s

(d) Improvement of the key rate in %

Fig. 9: Benefits of the NC-CQKD-FSO system over SU-QKD-FSO system in terms of key rate, when applying the average number of $n_S = 1$ photons per pulse, for the outage probability of $P_{SD}^{SU} = 2 \times 10^{-1}$, the generating bit rate $R_b = 2.5 \times 10^9$ of the raw key and other parameters listed in Table IV.

beam wander for a free-space quantum key distribution system operating in urban environment," *Optical Engineering*, vol. 53, no. 8, 2014.

[19] G. Vest, M. Rau, L. Fuchs, G. Corrielli, H. Weier, S. Nauerth, A. Crespi, R. Osellame, and H. Weinfurter, "Design and evaluation of a handheld quantum key distribution sender module," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, pp. 131–137, May 2015.

[20] M. Rau, T. Heindel, S. Unsleber, T. Braun, J. Fischer, S. Frick, S. Nauerth, C. Schneider, G. Vest, S. Reitzenstein, M. Kamp, A. Forchel, S. Hoefling, and H. Weinfurter, "Free space quantum key distribution over 500 meters using electrically driven quantum dot single-photon sources-a proof of principle experiment," *New Journal of Physics*, vol. 16, 2014.

[21] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," *New Journal of Physics*, vol. 4, p. 41, 2002.

[22] K. Shimizu, T. Honjo, M. Fujiwara, T. Ito, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, "Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of tokyo metropolitan area," *Journal of Lightwave Technology*, vol. 32, pp. 141–151, Jan 2014.

[23] J. H. Shapiro, "Near-field turbulence effects on quantum-key distribution," *Phys. Rev. A*, vol. 67, p. 022309, Feb 2003.

[24] M. Gabay and S. Arnon, "Quantum key distribution by a free-space MIMO system," *Journal of Lightwave Technology*, vol. 24, pp. 3114–3120, Aug 2006.

[25] M. Safari and M. Uysal, "Relay-assisted quantum-key distribution over long atmospheric channels," *Journal of Lightwave Technology*, vol. 27, pp. 4508–4515, Oct 2009.

[26] P. V. Trinh, N. T. Dang, and A. T. Pham, "All-optical relaying fso systems using edfa combined with optical hard-limiter over atmospheric turbulence channels," *Journal of Lightwave Technology*, vol. 33, pp. 4132–4144, Oct 2015.

[27] D. Kedar and S. Arnon, "Urban optical wireless communication networks: the main challenges and possible solutions," *IEEE Communications Magazine*, vol. 42, pp. S2–S7, May 2004.

[28] Y. Liu, L. Guo, and X. Wei, "Optimizing backup optical-network-units

selection and backup fibers deployment in survivable hybrid wireless-optical broadband access networks," *Journal of Lightwave Technology*, vol. 30, pp. 1509–1523, May 2012.

[29] H. Chen, Y. Li, S. K. Bose, W. Shao, L. Xiang, Y. Ma, and G. Shen, "Cost-minimized design for twdm-ponbased 5g mobile backhaul networks," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 8, pp. B1–B11, Nov 2016.

[30] M. A. Khalighi and M. Uysal, "Survey on free space optical communication: A communication theory perspective," *IEEE Communications Surveys Tutorials*, vol. 16, pp. 2231–2258, Fourthquarter 2014.

[31] J. L. Rebelatto, B. F. Uchôa-Filho, Y. Li, and B. Vucetic, "Generalized distributed network coding based on nonbinary linear block codes for multi-user cooperative communications," in *2010 IEEE International Symposium on Information Theory (ISIT 2010)*, pp. 943 –947, June 2010.

[32] J. Rebelatto, B. Uchoa Filho, Y. Li, and B. Vucetic, "Multi-user cooperative diversity through network coding based on classical coding theory," *IEEE Transactions on Signal Processing*, vol. 60, pp. 916–926, Feb. 2012.

[33] H. V. Nguyen, S. X. Ng, and L. Hanzo, "Performance bounds of network coding aided cooperative multiuser systems," *Signal Processing Letters, IEEE*, vol. 18, no. 7, pp. 435–438, 2011.

[34] H. V. Nguyen, S. X. Ng, and L. Hanzo, "Irregular convolution and unity-rate coded network-coding for cooperative multi-user communications," *IEEE Transactions on Wireless Communications*, vol. 12, no. 3, pp. 1231–1243, 2013.

[35] J. P. (auth.), *Quantum Mechanics for Pedestrians 1: Fundamentals*. Undergraduate Lecture Notes in Physics, Springer International Publishing, 1 ed., 2014.

[36] A. Zeilinger, "Experiment and the foundations of quantum physics," *Rev. Mod. Phys.*, vol. 71, pp. S288–S297, Mar 1999.

[37] G. Cariolaro, *Signals and Communication Technology: Quantum Communications*. International Publishing Switzerland: Springer, 2015.

[38] L. Oesterling, D. Hayford, and G. Friend, "Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information," in *IEEE Conference on Technologies for Homeland Security (HST) 2012*, pp. 156–161, Nov 2012.

[39] N. L. Piparo and M. Razavi, "Long-distance trust-free quantum key distribution," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, pp. 123–130, May 2015.

[40] J. H. Shapiro, "Normal-mode approach to wave propagation in the turbulent atmosphere," *Appl. Opt.*, vol. 13, pp. 2614–2619, Nov 1974.

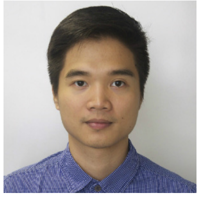
[41] G. R. M. S. S. L. Karp, S., *Optical channels: fibers, clouds, water and the atmosphere*. Plenum Press, 1988.

[42] W. Zhang, S. Hranilovic, and C. Shi, "Soft-switching hybrid fso/rf links using short-length raptor codes: design and implementation," *IEEE Journal on Selected Areas in Communications*, vol. 27, pp. 1698–1708, December 2009.

[43] H. V. Nguyen, C. Xu, S. X. Ng, and L. Hanzo, "Near-Capacity Wireless System Design Principles," *IEEE Communications Surveys Tutorials*, vol. 17, pp. 1806–1833, Fourthquarter 2015.

[44] D.Tse and P. Viswanath, *Fundamentals of Wireless Communications*. Englewood Cliffs, NJ, USA: Cambridge: Cambridge University Press, 2005.

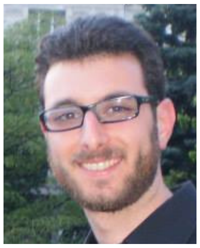
Hung Viet Nguyen received the B.Eng. degree in Electronics & Telecommunications from Hanoi University of Science and Technology (HUST), Hanoi, Vietnam, in 1999, the M.Eng. in Telecommunications from Asian Institute of Technology (AIT), Bangkok, Thailand, in 2002 and the Ph.D. degree in wireless communications from the University of Southampton, Southampton, U.K., in 2013. Since 1999 he has been a lecturer at the Post & Telecommunications Institute of Technology (PTIT), Vietnam. He is involved in the OPTIMIX and CONCERTO European projects. He is currently a postdoctoral researcher at Southampton Wireless (SW) group, University of Southampton, UK. His research interests include cooperative communications, channel coding, network coding and quantum communications.



Phuc V. Trinh received the B.E. degree in Electronics and Telecommunications from the Posts and Telecommunications Institute of Technology, Hanoi, Vietnam in 2013, and the M.Sc. degree in Computer Science and Engineering from the University of Aizu (UoA), Aizuwakamatsu, Japan, in 2015. He is currently working toward the Ph.D. degree in Computer Science and Engineering at UoA. His study in Japan is fully funded by a Japanese government scholarship (MonbuKagaku-sho). He was the recipient of several awards, including the IEEE Sendai Sections Student Award (2014), the UoA Presidents Award (2015), the IEEE VTS Japan Chapter Young Researchers Encouragement Award (2015), the IEEE ComSoc Sendai Chapter Student Excellent Researcher Award (2015), and the Second prize of IEEE Region 10 (Asia-Pacific) Distinguished Student Paper Award (2016). His current research interests are in the area of optical wireless communications, including modulation techniques, coding, system modeling and simulation, and performance analysis. He is a student member of IEEE and IEICE.

Anh T. Pham received the B.E. and M.E. degrees, both in Electronics Engineering from the Hanoi University of Technology, Vietnam in 1997 and 2000, respectively, and the Ph.D. degree in Information and Mathematical Sciences from Saitama University, Japan in 2005. From 1998 to 2002, he was with the NTT Corp. in Vietnam. Since April 2005, he has been on the faculty at the University of Aizu, where he is currently Professor and Head of Computer Communications Laboratory with the Division of Computer Engineering. Dr. Pham's research interests are in the broad areas of communication theory and networking with a particular emphasis on modeling, design and performance evaluation of wired/wireless communication systems and networks. He has authored/co-authored more than 150 peer-reviewed papers on these topics. Dr. Pham is senior member of IEEE. He is also member of IEICE and OSA.

Zunaira Babar received her B.Eng. degree in electrical engineering from the National University of Science & Technology (NUST), Islamabad, Pakistan, in 2008, and the M.Sc. degree (Distinction) and the Ph.D degree in wireless communications from the University of Southampton, UK, in 2011 and 2015, respectively. Her research interests include quantum error correction codes, channel coding, coded modulation, iterative detection and cooperative communications.



Dimitrios Alanis (S'13) received the M.Eng. degree in Electrical and Computer Engineering from the Aristotle University of Thessaloniki in 2011 and the M.Sc. and PhD degrees in Wireless Communications from the University of Southampton in 2012 and 2017, respectively. He is currently working as a Research Fellow in Southampton Wireless (SW) group, School of Electronics and Computer Science of the University of Southampton, UK. His research interests include quantum computation and quantum information theory, quantum search algorithms, cooperative communications, resource allocation for self-organizing networks, bio-inspired optimization algorithms and classical and quantum game theory.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2017.2712288, IEEE Access

Panagiotis Botsinis (S'12-M'16) received the M.Eng. degree from the School of Electrical and Computer Engineering of the National Technical University of Athens (NTUA), Greece, in 2010, as well as the M.Sc. degree with distinction and the Ph.D. degree in Wireless Communications from the University of Southampton, UK, in 2011 and 2015, respectively. He is currently working as a Research Fellow in the Southampton Wireless group at the School of Electronics and Computer Science of the University of Southampton, UK. Since October 2010, he has been a member of the Technical Chamber of Greece. His research interests include quantum-assisted communications, quantum computation, iterative detection, OFDM, MIMO, multiple access systems, coded modulation, channel coding, cooperative communications, as well as combinatorial optimization.

Daryus Chandra (S'15) received the M.Eng. degree in electrical engineering from Universitas Gadjah Mada, Indonesia, in 2014. He is currently pursuing the Ph.D. degree with the Southampton Wireless Group, School of Electronics and Computer Science, University of Southampton, UK. He is a recipient of scholarship award from the Indonesia Endowment Fund for Education (Lembaga Pengelola Dana Pendidikan, LPDP). His research interests include classical and quantum error correction codes, quantum information, and quantum communications.

Soon Xin Ng (S'99-M'03-SM'08) received the B.Eng. degree (First class) in electronic engineering and the Ph.D. degree in telecommunications from the University of Southampton, Southampton, U.K., in 1999 and 2002, respectively. From 2003 to 2006, he was a postdoctoral research fellow working on collaborative European research projects known as SCOUT, NEWCOM and PHOENIX. Since August 2006, he has been a member of academic staff in the School of Electronics and Computer Science, University of Southampton. He is involved in the OPTIMIX and CONCERTO European projects as well as the IU-ATC and UC4G projects. He is currently an Associate Professor in telecommunications at the University of Southampton. His research interests include adaptive coded modulation, coded modulation, channel coding, space-time coding, joint source and channel coding, iterative detection, OFDM, MIMO, cooperative communications, distributed coding, quantum error correction codes and joint wireless-and-optical-fibre communications. He has published over 200 papers and co-authored two John Wiley/IEEE Press books in this field. He is a Senior Member of the IEEE, a Chartered Engineer and a Fellow of the Higher Education Academy in the UK.

Lajos Hanzo (M'91-SM'92-F'04) received his degree in electronics in 1976 and his doctorate in 1983. In 2009 he was awarded the honorary doctorate "Doctor Honoris Causa" by the Technical University of Budapest. During his 38-year career in telecommunications he has held various research and academic posts in Hungary, Germany and the UK. Since 1986 he has been with the School of Electronics and Computer Science, University of Southampton, UK, where he holds the chair in telecommunications. He has successfully supervised about 100 PhD students, co-authored 20 John Wiley/IEEE Press books on mobile radio communications totalling in excess of 10 000 pages, published 1400+ research entries at IEEE Xplore, acted both as TPC and General Chair of IEEE conferences, presented keynote lectures and has been awarded a number of distinctions. Currently he is directing a 100-strong academic research team, working on a range of research projects in the field of wireless multimedia communications sponsored by industry, the Engineering and Physical Sciences Research Council (EPSRC) UK, the European Research Councils Advanced Fellow Grant and the Royal Societys Wolfson Research Merit Award. He is an enthusiastic supporter of industrial and academic liaison and he offers a range of industrial courses. Lajos is a Fellow of the Royal Academy of Engineering, of the Institution of Engineering and Technology, and of the European Association for Signal Processing. He is also a Governor of the IEEE VTS. During 2008–2012 he was the Editor-in-Chief of the IEEE Press and a Chaired Professor also at Tsinghua University, Beijing. He has 30 000+ citations. For further information on research in progress and associated publications please refer to http://www.wireless.ecs.soton.ac.uk.