Orthogonal Frequency Division Multiplexed Quantum Key Distribution

Sima Bahrani, *Student Member, IEEE*, Mohsen Razavi, and Jawad A. Salehi, *Fellow, IEEE*

***Abstract*—We propose orthogonal frequency division multiplexing (OFDM), as a spectrally efficient multiplexing technique, for quantum key distribution (QKD) at the core of trusted-node quantum networks. Two main schemes are proposed and analyzed in detail, considering system imperfections, specifically, time misalignment issues. It turns out that while multiple service providers can share the network infrastructure using the proposed multiplexing techniques, no gain in the total secret key generation rate is obtained if one uses conventional passive all-optical OFDM decoders. To achieve a linear increase in the key rate with the number of channels, an alternative active setup for OFDM decoding is proposed, which employs an optical switch instead of conventional passive circuits. We show that by using our proposed decoder the bandwidth utilization is considerably improved as compared to conventional wavelength division multiplexing techniques.**

***Index Terms*—Quantum key distribution, orthogonal frequency division multiplexing, quantum networks**

I. Introduction

QUANTUM communications has entered a new phase in its development targeting new markets and aiming at widespread use and adoption in different scenarios. With the successful demonstration of SECOQC [1] and Tokyo [2] quantum key distribution (QKD) networks, we are now at a stage to develop many-user quantum networks [3]–[6]. The reach of conventional QKD links is, nevertheless, limited as they rely on low-power signals, e.g., single photons [7]. The initial solution perceived for the first generation of quantum networks relies on a *trusted* set of nodes, in a mesh topology, at the core network. Such nodes enable secure key exchange between any two remote users via a cascade of key exchanges between neighboring nodes along the path that connects the two users. In order to support many users at the access nodes, it is necessary to proportionally generate longer secret keys between the internal core nodes of the network. The analogy in classical telecommunications is the ratio between the end-user data rates and the high traffic of data at the backbone of the network. One simple idea to achieve higher key rates is to use multiplexing techniques to generate keys in parallel. In this paper, we employ one of the most advanced classical multiplexing techniques to come up with orthogonal frequency division multiplexed QKD (OFDM-QKD) schemes. We look at existing *all-optical* orthogonal frequency division multiplexing (OFDM) techniques [8]–[13] and partly modify their setups in order to obtain spectrally efficient high-rate OFDM-QKD schemes.

This research was supported in part by the European Community's Seventh Framework Programme Grant Agreement 277110, the UK's Engineering and Physical Sciences Research Council Grant EP/M506953/1, and Iran National Science Foundation (INSF).

S. Bahrani and J. A. Salehi are with the Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran. M. Razavi is with the School of Electronic and Electrical Engineering, University of Leeds, Leeds, LS2 9JT, UK, e-mail: m.razavi@leeds.ac.uk.

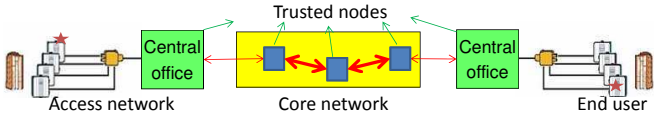

Fig. 1: Trusted-node architecture for emerging quantum networks. The end users may be connected to the core network via passive optical networks. In order to generate a secret key between two end users, one must first generate a key between any two neighboring nodes along their connecting path. The key generated between the end user and its corresponding central office can then be encrypted and securely relayed node by node until it reaches the other party. Note that the internal links (thicker lines) must carry a higher traffic.

QKD enables secure key exchange without relying on computational complexity. This is in contrast with existing techniques for key exchange, e.g., the RSA protocol [14], whose security is at risk with the advancement of technology [15]. In that sense, QKD provides a *future-proof* method of secure communications. The first proposed QKD protocol by Bennett and Brassard in 1984 (BB84) [7] relied on the polarization encoding of single photons. Since then new protocols and encoding schemes have emerged and QKD has seen field demonstrations along with conventional telecom channels [2], [16]–[18]. Recent demonstrations cover distances over 250 km [19] and with nearly 50 users. The next step for QKD development will focus on extending the reach of the system and the number of users QKD networks can support.

Quantum networks are facing several challenges before their full implementation. One key requirement is their integration with existing and future classical optical communication networks [6], [20]. This implies the need for new quantum friendly standards for optical networks. That will include devising proper mechanisms by which weak quantum signals can be separated from classical channels [18], [21]. Multiple-access techniques are also needed to enable interference-free access to different quantum users [3], [22]. Eventually, QKD systems must improve their performance in terms of rate-versus-distance behavior and cost.

One feasible approach to long-distance QKD is based on trusted-node quantum networks. With current technology, we are able to generate secret keys at a rate on the order of Mb/s at 50 km of distance [18]. By cascading several of such links, as shown in Fig. 1, *and* trusting all intermediate nodes, one, in principle, can exchange secret keys at any distance by first generating secret keys between neighboring nodes and then relaying the initial key, in an encrypted way, to the other party. The main requirement for this approach is to trust all nodes in between the two end users. While this assumption may

be acceptable for the first generation of quantum networks, it can be removed in future generations by relying on quantum repeater setups at the core network [23].

In trusted-node networks, the internal nodes in the core network are expected to have a high traffic of key exchange as they are providing service to a large number of end users. It is important then to generate a large number of secret key bits per allocated wavelength to each quantum channel over these core links. One possible approach is to use non-binary signalings to send more key bits per transmitted quantum state [24]. In addition to this, we should think how most efficiently we can use the available bandwidth per allocated wavelength, especially with reference to QKD systems that rely on dense wavelength division multiplexing (DWDM) techniques [6]. Our proposed solution here relies on one of the most spectrally efficient methods in classical communications, i.e., OFDM. OFDM relies on the full orthogonality of its subcarriers to multiplex multiple channels. This full orthogonality is essential in QKD applications [3], [25], in order to minimize the interference from other classical and quantum users. In our case, each subcarrier represents a QKD channel between two core nodes. The total key generation rate between these two nodes is then expected to increase linearly by the number of subcarriers. Moreover, OFDM is compatible with non-binary signaling techniques, and that would enable us to take the maximum benefit from the available bandwidth. Finally, by using a multiplexing technique, multiple service providers can use the capacity of the core network without trusting each other. Note that the OFDM-QKD can be modified to be used as a multiple-access technique in multi-user QKD setups. In this paper, we focus on the multiplexing aspect with the objective of increasing the rate at the core of QKD networks.

Being an optical system, QKD can be merged best with OFDM if all-optical OFDM encoders and decoders are used. Here, we consider two possible implementations for the all-optical OFDM transmitter. In the first approach, the OFDM subcarriers are generated directly by a bank of frequency offset locked laser sources or an optical comb generator [8]–[10]. After encoding the subcarriers, an optical coupler combines them to generate the OFDM signal. The second approach uses the optical inverse discrete Fourier transform (OIDFT) circuit to generate the OFDM signal [10]–[13]. Short pulses are fed into the OIDFT circuit following the QKD encoding stage. Both these approaches rely on real-time optical discrete Fourier transform (ODFT) at their receivers. Conventional passive implementations of ODFT turn out to be too lossy to be useful for our main objective of increasing the rate. In our work, we show how the ODFT circuit can be modified to be effective for QKD applications.

Different QKD protocols can be used in our proposed OFDM-QKD setups. Here, we focus on the decoy-state variant of the BB84 protocol [26]. The decoy-state technique allows us to use *weak* laser pulses, rather than ideal single-photon sources as originally proposed in [7], and that would simplify the encoding equipment of QKD. In order to obtain immunity against the photon-number splitting attacks, in the decoy-state protocol, for every transmitted QKD pulse, the sender has to randomly choose its intensity from a set of available intensities, where one of which corresponds to the main signal, and the rest to decoy states. In practice, it is often sufficient to use only two decoy states [27], although, in this paper, for analytical convenience, we assume infinitely many decoy states are used. Our proposed setups are compatible with other QKD protocols, such as continuous-variable or distributed-phase QKD protocols [28]. The detailed analysis of the latter systems is, however, beyond the scope of this paper.

Both optical OFDM and QKD are advanced technologies. It is interesting to see how drawbacks in one system would translate into the other. While some of the drawbacks with OFDM may directly affect our OFDM-QKD system, there are certain issues that are less of a problem in a QKD setup. For instance, one known OFDM problem in the classical domain is its high peak-to-average power ratio, which makes it susceptible to distortions due to nonlinearity effects [29], [30]. Fortunately, for QKD applications, nonlinearity is not necessarily a major issue because the QKD transmitted signals are low power. Nevertheless, the common OFDM-related imperfections such as time misalignment [31]–[33], phase noise introduced by the lasers [30], [34], [35], and frequency offsets between the transmitter and the receiver carriers (in the case of applying a local oscillator at the receiver) [30], [34] can potentially influence the orthogonality between subchannels, and subsequently affect the performance of OFDM-QKD systems. In this paper, we specifically consider the degrading effects due to time misalignmnet, which is the major source of error in the most promising setup we propose here.

Finally, it is interesting to note that, while one of the key advantages of OFDM in the microwave domain is its reliance on digital signal processing, OFDM-QKD setups may less benefit from this feature. At the receiver side, any measurement on the OFDM signal before the QKD decoders could alter the transmitted states and result in errors. That is why it is important to have a fully optical setup for OFDM decoders. At the transmitter side, an optical OFDM setup would, in principle, allow multiple users to encode their key bits without trusting each other. This cannot necessarily be achieved if we first generate the OFDM signal electronically and then convert it to an optical signal. That said, there will be much room for improvement in future work, while, in this work, we assess the possibility of OFDM-QKD systems.

The rest of the paper is organized as follows. In the next section, we propose two OFDM-QKD schemes and describe their principles of operation. In Sec. III, the proposed OFDM-QKD schemes are analyzed from a quantum mechanical perspective. The analysis of secret key generation rate is presented in Sec. IV, in which we particularly focus on time misalignment issues within the OFDM system. We propose an optimal gating solution to maximize the key rate. Some numerical results are then presented in Sec. V. We conclude the paper in Sec. VI.

II. System Description

In this section, we describe QKD over all-optical OFDM links. Figure 2 shows the overall system structure. The QKD encoders generate the quantum signals, in the form of pulses,

Fig. 2: QKD over an OFDM link. The QKD encoded optical pulses are multiplexed by an all-optical OFDM encoder. At the receiver, the corresponding OFDM decoder followed by QKD decoders are used to generate secret keys.

that carry the information about the encoded key bits in each subchannel. The resulting optical pulses are fed simultaneously into the OFDM encoder to be multiplexed. At the receiver, the OFDM decoder followed by essential QKD decoding modules can be used to complete the QKD protocol. The key part in the OFDM decoder is an ODFT circuit, which effectively separates the subchannels.

In this paper, we assume that the QKD encoders perform phase encoding using decoy-state techniques [26]. Based on the phase-encoded BB84 protocol, Alice chooses her phase value ϕ_A from one of the bases $\{0, \pi\}$ or $\{\pi/2, 3\pi/2\}$. The two phase values in each basis correspond to bits 0 and 1. As shown in Fig. 3, an optical pulse sent by Alice passes through a Mach-Zehnder interferometer (MZI). The output is two non-overlapping successive pulses, denoted by r and s, of duration T with a relative phase corresponding to the chosen basis and the transmitted key bit. The QKD decoding includes Bob's selection of his measurement basis by choosing the phase $\phi_B \in \{0, \pi/2\}$ randomly in one arm of his MZI and the detection of the output signal. In the following, we describe two OFDM-QKD setups based on the proposed schemes for all-optical OFDM.

A. Scheme I

Figure 4 depicts the OFDM-QKD system that relies on directly generated subcarriers. At the transmitter, a bank of frequency offset locked laser diodes generate the input optical pulses to N QKD encoders. These pulses are individually phase randomized, as required by the decoy-state protocol [36], and then go through a bank of encoders as in Fig. 3. Because the information is encoded in the phase difference, these overall random phases do not change the encoded bits. The same holds for the possible phase noise of the lasers so long as their phase is constant during the transmission of each bit. In our forthcoming analysis, we account for possible relative phase distortions between r and s pulses in Fig. 3. The outputs of the QKD encoders are then combined to form the OFDM signal. If we trust all the elements in the Alice box of Fig. 4, we can adjust the transmitted power such that

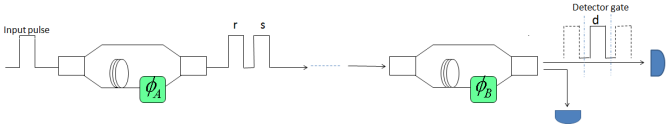

Fig. 3: Phase encoded QKD. Alice encodes her key bits by choosing a phase value $\phi_A \in \{0, \pi/2, \pi, 3\pi/2\}$. Each optical pulse passes through the MZI and produces two output pulses with the relative phase ϕ_A. On the Bob's side, a similar MZI is used to recombine r and s modes, followed by photodetection.

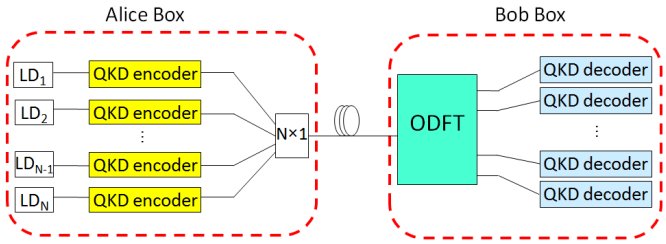

Fig. 4: OFDM-QKD using directly generated subcarriers. The optical pulses, generated by N frequency offset-locked laser diodes, are fed into the QKD encoders. At the receiver, an ODFT circuit is required to separate the subcarriers.

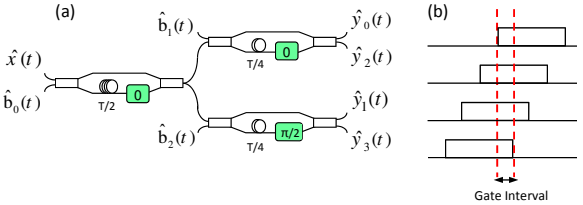

Fig. 5: (a) The passive ODFT circuit for $N = 4$. The circuit consists of three MZIs with corresponding delays and phase shifts. (b) Shifted replicas of the input OFDM signal for $N = 4$. The shift values for $N = 4$ are $\{0, T/4, T/2, 3T/4\}$. The time slot, in which all these copies overlap, is extracted by the time gating operation.

it is at the *output* of the combiner that each subchannel has the right intensity for its corresponding pulse. This will allow us to neglect the losses in the encoder box, as we assume in this paper. At the receiver, ODFT is used to demultiplex the subcarriers. To comply with the OFDM orthogonality condition, in Scheme I, the pulse width is $T = 1/\Delta f$, where Δf is the frequency separation of the subcarriers.

To illustrate the principles of this scheme, consider the classical case, where the OFDM signal is generated by combining classical subchannels as follows:

$$x(t) = \sum_{k=0}^{N-1} a_k e^{j\omega_k t}, \quad 0 < t < T, \tag{1}$$

where a_k is the complex amplitude of the k^{th} subchannel with frequency $\omega_k = \omega_0 + 2\pi k\Delta f$ for a nominal channel frequency ω_0. The ODFT circuit, at the decoder, will then separate different subcarriers and generate the following output signals:

$$y_m(t) = \frac{1}{N}\sum_{n=0}^{N-1} x(t - nT_c)e^{j2\pi nm/N}, \quad m = 0, 1, ..., N-1, \tag{2}$$

where $T_c \triangleq T/N$. With the assumption of $T = 1/\Delta f$, we can conclude from (1) and (2) that

$$y_m(t) = \sum_{k=0}^{N-1} a_k e^{j\omega_k t}\left(\frac{1}{N}\sum_{n=0}^{N-1} e^{j2\pi n(m-k)/N}\right). \tag{3}$$

The term in the brackets is nonzero only if $k = m$, which leads to the m^{th} subcarrier extraction.

Different methods can be used to realize the OFDM decoding, as required by (2), in the optical domain. In Scheme I, we assume that the ODFT is implemented by a passive structure consisted of $N - 1$ MZIs [8]. Figure 5(a) shows an ODFT circuit for $N = 4$. This structure imitates the efficient

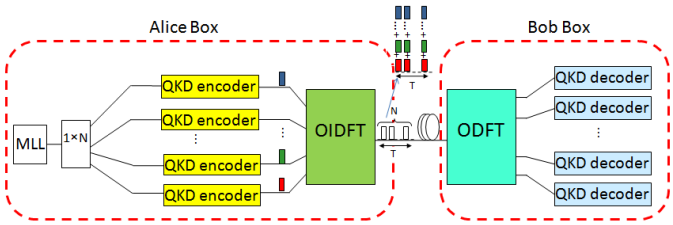

Fig. 6: OFDM-QKD using OIDFT circuit. A train of short pulses generated by an MLL is split into N paths. The OFDM symbol is generated by multiplexing the output pulses of the QKD encoders by the OIDFT circuit. The OFDM symbol consists of a series of pulses, each a superposition of pulses from different inputs. At the receiver, an ODFT circuit demultiplexes the subcarriers.

method of realizing DFT, known as fast Fourier transform (FFT), by means of delays, couplers, and phase shifters. Each output port of the ODFT circuit is a weighted sum of shifted replicas of the input as required by (2). It will then provide us with a real-time DFT operation once all shifted replicas of the input overlap, as shown in Fig. 5(b). That would require a time gating operation [8], [9], which can be implemented by electro-absorption modulators (EAM), or simply by time-gating the single-photon detectors used in the QKD decoders. Time misalignment can then be a major source of error in such a scheme. The quantum operation of the ODFT circuit is discussed in more detail Sec. III.

B. Scheme II

Figure 6 shows an alternative setup for the OFDM-QKD system. Here, the output of a pulsed laser source, e.g., a mode-locked laser (MLL), is split into several paths by an optical splitter. The pulses should be short enough to cover the spectrum of all the subcarriers in the OFDM symbol. Here, we assume that the pulse width is slightly lower than T_c. Similar to Scheme I, each short pulse, after splitting, is fed into QKD encoders to produce successive pulses r and s. Each of these pulses will then go through an OIDFT circuit generating N short pulses within an OFDM symbol duration T. The delay in the MZI of Fig. 3 is assumed to be greater than T.

The required OIDFT can be implemented by a structure similar to the ODFT. For instance, the circuit in Fig. 5(a), for the special case of $N = 4$, can be employed for OIDFT as well. In the case of OIDFT, the input pulses (denoted by y components) enter from the right hand side of Fig. 5(a) and the output will be the signal labeled by $\hat{x}(t)$. Assuming that the y pulses are synchronous, in each OFDM symbol, the output signal x consists of four pulses apart by multiples of T_c within a T-long frame. Each of the latter pulses are a combination of all input pulses, as shown in Fig. 6.

More generally, in the classical case, the generated OFDM amplitude at any carrier frequency ω is given by

$$x(t) = \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} A_k p(t - lT_c) e^{j2\pi kl/N}, \tag{4}$$

where $p(t)$ represents the shape of the initial laser pulse and A_k is the complex amplitude of the k^{th} subchannel. Note that in Fig. 6, subchannels are separated spatially at the input to OIDFT. At the receiver, the ODFT operation in (2) shifts each of the pulses within an OFDM symbol and combines them together to generate

$$y_m(t) = \frac{1}{N^2} \sum_{n=0}^{N-1} \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} a_k p(t - (n + l)T_c) e^{j2\pi(kl+nm)/N}, \tag{5}$$

for $m \in \{0, 1, ..., N-1\}$. In a real-time implementation, only at $n + l = N - 1$, all relevant input pulses are added together at which $y_m(t)$ reduces to

$$z_m(t) = \sum_{k=0}^{N-1} \frac{A_k}{N} p(t - (N-1)T_c) e^{j2\pi k(N-1)/N} \left(\frac{1}{N} \sum_{n=0}^{N-1} e^{j2\pi n(m-k)/N}\right). \tag{6}$$

Here again, the term in the brackets is zero for $k \neq m$, which implies that, up to a known overall phase factor, the original information in A_m can be recovered at the mth output port of the ODFT circuit of Fig. 6.

For the receiver of Scheme II, we have two options. We can either use the passive OFDM decoder used in Scheme I, or, alternatively, the active structure shown in Fig. 7(a). The main advantage of the latter is to remove the inherent loss in the passive OFDM decoder. To better explain the loss effect in the passive decoder, consider a sequence of N pulses at the input $x(t)$ of Fig. 5(a), and let us look at the output signals. In this case, each input pulse has four paths to take, with different delays and phase shifts, to reach to the output ports of Fig. 5(a). In other words, for each input pulse, there will be four output pulses at each of the decoder's four output ports; see Fig. 7(b). Only one out of these four output pulses has the right amount of delay and phase shift to be used for our ODFT operation, and that is why time gating is required. The inevitable drawback of this approach is that the other three pulses, and the power therein, will remain unused and that will contribute to a maximum total efficiency of $1/N$ for a passive decoder as in Fig. 5(a). To overcome this drawback, our proposed OFDM decoder in Fig. 7(a) employs an optical switch along with proper delays, instead of a passive circuit, to perform the serial to parallel conversion. As shown in Fig. 7(c), this way there will be no extra pulses to be discarded, and the ODFT process can be implemented by a passive N-by-N circuit, of a star topology but with phase shifters along each internal path, with no fundamental overall loss [8], [37].

The above feature of the active decoder in Fig. 7(a) makes it a better choice for high-rate QKD links, as we will see in the following sections. The passive decoder schemes can still be used for the sake of sharing the channel resources between multiple service providers. They do not, however, offer any total-rate advantage as compared to a single-carrier system. Note that the OFDM decoder of Fig. 7(a) is mostly compatible with Scheme II, due to its discrete nature, as compared to Scheme I. Nevertheless, one should take note of possible challenges of using the active decoder with Scheme II. While, by using a common pulsed source, Scheme II is more immune to phase noise or frequency offset problems, time misalignment is still a key concern. That is why, in the following sections, we study the impact of such timing errors in our OFDM-QKD setups. Secondly, while the active decoder removes the loss associated with time gating, its optical switch

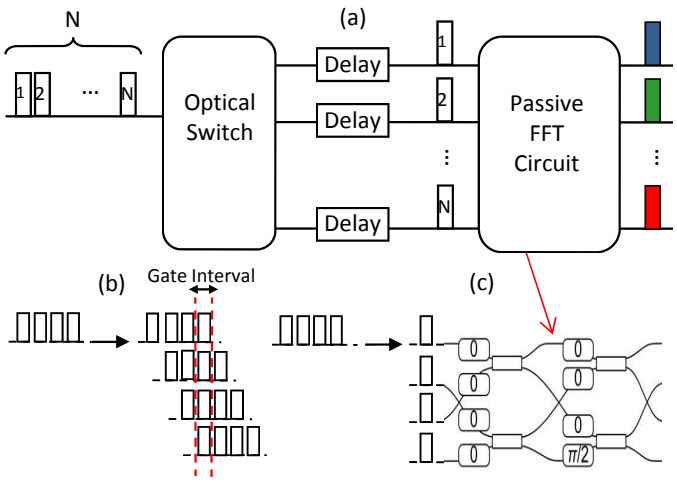

Fig. 7: (a) Proposed *active* ODFT circuit. By employing an optical switch instead of a power splitter, the loss of time gating is eliminated. (b) Passive approach to serial-to-parallel conversion for $N = 4$. Some pulses are generated and then discarded during the time gating process. (c) Active approach to serial-to-parallel conversion for $N = 4$ followed by the FFT circuit [8].

will introduce some additional insertion loss. The latter, within our practical regime of interest, is shown to be less than 2 dB for ultrafast optical switches and will be accounted for in our numerical analysis [38]. Optical switches may also have nonzero extinction ratios, because of which some power leaks to other undesired output ports. This is a minor problem for the decoder of Fig. 7(a), because the input pulses to the switch are non-overlapping in time. By using time gating and proper delay lines, the leaked power to other ports should not appear in the same time slot that time gating is taking place, hence has negligible effect on system performance.

III. Quantum Analysis

In this section, we analyze the OFDM-QKD systems proposed in Sec. II from a quantum mechanical perspective. We choose the Heisenberg picture for our analysis. In two steps, we first concentrate on the operation of the system corresponding to each of the two pulses r and s in Fig. 3, and then we combine the results to find the output operators in QKD decoding modules.

A. Scheme I

In the Heisenberg picture, the output operator of the Alice box in Fig. 4 can be expressed as

$$\hat{x}(t) = \sum_{k=0}^{N-1} \hat{a}_k e^{j\omega_k t}, \quad 0 < t < T, \tag{7}$$

where $\hat{a}_k$ is the annihilation operator corresponding to the mode representing the k^{th} subcarrier. For the rest of this section, we neglect the path loss effect, which will be considered when we calculate the secret key generation rate. We then focus on the receiver setup assuming that at its input the signal $\hat{x}(t)$ is received.

For simplicity, let us first consider the special case of $N = 4$. As shown in Fig. 5, the ODFT circuit, in this case, is implemented by three MZIs. The operators $\hat{b}_0(t) = \sum_{k=0}^{N-1} \hat{b}_{0k} e^{j\omega_k t}$, $\hat{b}_1(t) = \sum_{k=0}^{N-1} \hat{b}_{1k} e^{j\omega_k t}$ and $\hat{b}_2(t) = \sum_{k=0}^{N-1} \hat{b}_{2k} e^{j\omega_k t}$ represent the vacuum fluctuations of the unused ports of the MZIs' beam splitters corresponding to all existing frequency modes of the system. For a center frequency, ω, the transformation matrices of the three MZIs in Fig. 5 are given by

$$B_{\omega,1} = \frac{1}{2}\begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{-j(\omega\frac{T}{2})} \end{pmatrix}\begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix}, \tag{8}$$

for the MZI on the left,

$$B_{\omega,2} = \frac{1}{2}\begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{-j(\omega\frac{T}{4})} \end{pmatrix}\begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix}, \tag{9}$$

for the one on top right, and

$$B_{\omega,3} = \frac{1}{2}\begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & je^{-j(\omega\frac{T}{4})} \end{pmatrix}\begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix}, \tag{10}$$

for the one on bottom right of Fig. 5(a). Applying the above transformations to mode k, we obtain

$$\begin{pmatrix} \hat{a}'_k(t) \\ \hat{b}'_k(t) \end{pmatrix} = B_{\omega_k,1}\begin{pmatrix} \hat{a}_k(t) \\ \hat{b}_{0k}(t) \end{pmatrix}, \tag{11}$$

$$\begin{pmatrix} \hat{y}_{0,k}(t) \\ \hat{y}_{1,k}(t) \end{pmatrix} = B_{\omega_k,2}\begin{pmatrix} \hat{a}'_k(t) \\ \hat{b}_{1k}(t) \end{pmatrix}, \tag{12}$$

$$\begin{pmatrix} \hat{y}_{2,k}(t) \\ \hat{y}_{3,k}(t) \end{pmatrix} = B_{\omega_k,3}\begin{pmatrix} \hat{b}'_k(t) \\ \hat{b}_{2k}(t) \end{pmatrix}. \tag{13}$$

The output operator for output port m in Fig. 5 is then given by

$$\hat{y}_m(t) = \sum_{k=0}^{3} \hat{y}_{m,k}(t), \quad m = 0, 1, 2, 3. \tag{14}$$

Note that the above operations are all linear. Based on the superposition principle, we can split each output $\hat{y}_m(t)$ to two parts. The first part is the output obtained by neglecting the vaccum operators, and the other part is a linear combination of all vacuum operators. More generally, it can be concluded that the output of such an ODFT circuit, neglecting the vacuum operators, can be expressed as a function of $\hat{x}(t)$, as follows:

$$\hat{X}_m(t) = \frac{1}{N}\sum_{n=0}^{N-1} \hat{x}(t - nT_c)e^{j2\pi nm/N}, \quad m = 0, \ldots, N-1, \tag{15}$$

which is similar in form to (2) for the classical case. Substituting (7) into (15) and applying the orthogonality condition, $\Delta f = \frac{1}{T}$, we obtain

$$\hat{X}_m(t) = \sum_{k=0}^{N-1} \hat{a}_k e^{j2\pi(f_0+k\Delta f)t}\left(\frac{1}{N}\sum_{n=0}^{N-1} e^{j2\pi n(m-k)/N}\right). \tag{16}$$

Note that the term in the brackets is nonzero only if $k = m$. We then obtain

$$\hat{y}_m(t) = A\hat{a}_m(t) + \sum_{i=0}^{N-2}\sum_{k=0}^{N-1} \beta_{ik}\hat{b}_{ik}(t), \quad m = 0, \ldots, N-1, \tag{17}$$

where A is either 1 or j and β_{ik}'s are constant coefficients. The operator $\hat{a}_m(t)$ is the evolved version of $\hat{a}_m$ and is given by $\hat{a}_m(t) = \hat{a}_m e^{j\omega_m t}$, and similarly for the vacuum operators in the above equation. As explained in Sec. II, the orthogonality is only met in a region of width T/N, where all of the shifted

copies of the OFDM signal overlap. The signal corresponding to this overlapping time slot will eventually be detected by the photodetectors in the receiver module.

With the phase encoding QKD protocol, the two successive pulses r and s for channel m, represented by $\hat{a}_r^{(m)}$ and $\hat{a}_s^{(m)}$, respectively, will be recombined at the receiver's MZI in Fig. 3. The output operator corresponding to the recombined pulse d in Fig. 3 for the m^{th} output is then given by

$$\hat{d}_m(t) = \frac{j}{2}(e^{j\phi_B^{(m)}}\hat{a}_r^{(m)}(t) + \hat{a}_s^{(m)}(t)) + \sum_{i=0}^{N-2}\sum_{k=0}^{N-1}\beta_r^{(ik)}\hat{b}_r^{(ik)}(t) + \sum_{i=0}^{N-2}\sum_{k=0}^{N-1}\beta_s^{(ik)}\hat{b}_s^{(ik)}(t), \qquad T - T_c < t < T. \quad (18)$$

B. Scheme II

To start our analysis in this scheme, we denote the annihilation operator corresponding to the spatial mode at the output of the k^{th} QKD encoder by $\hat{a}_k$. We assume that an OIDFT circuit similar to the one depicted in Fig. 5(a) for $N = 4$, yet in the reverse direction, is used at the transmitter. Then, we can obtain the output operator of the Alice box by applying the transformation matrix of each MZI. It can be concluded that the output operator of the Alice box is given by

$$\hat{x}(t) = \frac{1}{N}\sum_{l=0}^{N-1}\hat{c}_l p(t - lT_c), \quad (19)$$

where $\hat{c}_l = \sum_{k=0}^{N-1}\hat{a}_k e^{j2\pi kl/N}$ is the l^{th} temporal mode at the output of the OIDFT circuit. Note that the coefficient $1/N$ in (19) is not necessarily a source of loss, so long as the average number of photons per pulse at the output of the transmitter meets the requirements of the decoy-state protcol. That is we can compensate for the internal loss at the transmitter by tuning the intensity of the incoming light. In our following analysis, this factor $1/N$ has been neglected. With a passive OFDM decoder similar to that of Scheme I at the receiver, the analysis presented in the previous subsection can be useful here as well, except that here we deal with temporal modes. Substituting (19) in (15) and simplifying the equations at $n + l = N - 1$, we can express each output of the ODFT circuit as

$$\hat{y}_m(t) = [\hat{a}_m e^{j2\pi m(N-1)/N} + \sum_{i=0}^{N-2}\sum_{k=0}^{N-1}\beta_{ik}\hat{b}_{ik}] \times p(t - T + T_c), \quad m = 0, \ldots, N-1. \quad (20)$$

The coefficient $e^{j2\pi m(N-1)/N}$ is a constant phase term that can be absorbed in $\hat{a}_m$ in the above equation.

Finally, the output operator obtained by the recombination of the pulses r and s by means of the receiver's MZI, $\hat{d}_m(t)$, is given by

$$\hat{d}_m(t) = [\frac{j}{2}(e^{j\phi_B^{(m)}}\hat{a}_r^{(m)} + \hat{a}_s^{(m)}) + \sum_{i=0}^{N-2}\sum_{k=0}^{N-1}\beta_r^{(ik)}\hat{b}_r^{(ik)} + \sum_{i=0}^{N-2}\sum_{k=0}^{N-1}\beta_s^{(ik)}\hat{b}_s^{(ik)}] \times p(t - T + T_c). \quad (21)$$

Another option for the receiver in this scheme is the structure we proposed in Fig. 7(a). For this active decoder, (21) is multipled by an additional factor $\sqrt{N}$. Furthermore, no vacuum components would appear because the beam splitters in the FFT circuit do not have any unused ports [8].

IV. Key Rate Analysis

This section presents an analysis of the secret key generation rate for the proposed OFDM-QKD schemes. We assume that the efficient decoy-state BB84 protocol is employed in the QKD setup [39], [40]. The average number of photons per QKD channel is given by μ, for the main signal state, and it is calculated at the output of the Alice box. The secret key generation rate per transmitted pulse, in the limit of an infinitely long key, is lower bounded by $\max[0, P(\mathrm{Y}_0)]$, where

$$P(\mathrm{Y}_0) = Q_1(1 - h(e_1)) - f Q_\mu h(E_\mu), \quad (22)$$

and $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy function with f being the error correction inefficiency. The overall gain, the QBER, the gain of a single photon state and the error rate of a single photon state are, respectively, given by [3]

$$Q_\mu = 1 - (1 - \mathrm{Y}_0)e^{-\eta\mu}, E_\mu = (\mathrm{Y}_0/2 + e_d(1 - e^{-\eta\mu}))/Q_\mu, \quad Q_1 = \mathrm{Y}_1\mu e^{-\eta\mu}, e_1 = (\mathrm{Y}_0/2 + e_d\eta)/\mathrm{Y}_1. \quad (23)$$

Equations (22)-(23) provide an estimate to the generated key rate when infinitely many decoy states are in use and no eavesdropper is present. In the above equations, $\mathrm{Y}_1 = (1-\eta)\mathrm{Y}_0 + \eta$ is the yield of a single photon state and Y_0 is the probability of any detector clicks without having any transmitted photons from the corresponding QKD encoder. Furthermore, e_d represents the probability of phase stability errors, between r and s pulses, and the total transmissivity of the link is given by

$$\eta = \eta_g\eta_d\eta_{\mathrm{ins}}10^{-\alpha L/10}, \quad (24)$$

where η_d is the quantum efficiency of the photodetectors, α is the channel loss factor in dB per unit of length and η_{ins} represents any additional insertion loss in the link. Here, η_g represents the additional loss due to the OFDM decoding scheme. For instance, in Scheme I, with gate interval of T_c, the parameter η_g equals $1/N$ in the ideal case. For Scheme II, and the active decoder of Fig. 7(a), η_g is ideally one.

We calculate the parameters in (23) by finding the probabilities of interest once the QKD measurements are done. For instance, the measurement operator for the representative photodetector in Fig. 3 is given by

$$\hat{M} = \int_{gate\ inteval}\hat{d}_m^\dagger(t)\hat{d}_m(t)dt, \quad (25)$$

from which one can obtain key rate parameters. In the analysis of the key generation rate, the terms containing vacuum states will not contribute to the key rate parameters, and that simplifies the calculations.

In order to analyze the secret key generation rate of the proposed schemes in more detail, one should consider the influence of imperfections in the system, which may degrade

TABLE I: Nominal values for system parameters

Parameter	Value
Average number of photons per signal pulse	0.48
Quantum Efficiency	0.3
Total insertion and path loss, $\eta_{\text{ins}}10^{-\alpha L/10}$	10 dB
Receiver dark count rate, γ_{dc}	1E-7 ns^{-1}
Error correction inefficiency, f	1.22
Phase stability error, e_d	0.005
Laser pulse repetition interval, T_s	210 ps
OFDM symbol duration, T	100 ps
Number of subcarriers, N	4, 8, 16

system performance. As explained before, we specifically consider time misalignment issues, which are known to be critical in all-optical OFDM systems. In OFDM, the time alignment of the optical subchannels is critical, due to its effect on their orthogonality. Furthermore, the time gating at the receiver should be synchronized with the transmitted pulses to extract the correct time slot. In our OFDM-QKD setups, nonidentical QKD encoders or some errors in time-gating synchronization may introduce time misalignment.

In our work, we have found the key generation rate of our proposed OFDM-QKD schemes in the presence of time misalignment issues. It turns out that they cause two problems. First, they generate some inter-channel crosstalk, denoted by p_{xtalk}, which adds to the background noise, and, second, they slightly reduce the transmissivity factor η_g. One can reduce the crosstalk noise by reducing the width of the gate interval, but, by doing so, η_g would further be reduced, as we have to leave out some of the desired signal components as well. That would imply the existence of an optimal gate width at which the total secret key rate R_{OFDM} is maximized, where

$$R_{\text{OFDM}} = \max[NP(\text{Y}_{\text{OFDM}})/T_s, 0], \tag{26}$$

and

$$\text{Y}_{\text{OFDM}} = 1 - (1 - (p_{\text{dc}} + p_{\text{xtalk}}))^2. \tag{27}$$

Here, T_s represents the repetition period of the QKD protocol and $p_{\text{dc}} = \gamma_{\text{dc}}T_g$, where γ_{dc} and T_g are the photodetectors' dark count rate and the gate interval, respectively. In Appendix A, we have derived all the required terms for calculating the above key rate as a function of the average time misalignment $\text{E}\{|\tau_k|\}$, where τ_k's are i.i.d random variables representing the time misalignment of the kth channel with respect to the gate interval, and $\delta \triangleq (T_c - T_p)/2$, where T_p is the pulse width in Scheme II. In the following, we present some of our numerical findings for a selected set of parameter values.

V. Numerical Results

In this section, we investigate the performance of the proposed OFDM-QKD schemes by considering the following cases: Scheme I and Scheme II with passive OFDM decoders, and Scheme II with the active OFDM decoder of Fig. 7(a). In order to evaluate the effect of time misalignment on the performance of each case, each subcarrier is assumed to have a time misalignment with uniform distribution, $\tau_k \sim \text{U}(-a, a)$, where $a < T_c$ is an arbitrary constant. We then find the optimal gate width that maximizes the key rate. The nominal values used for the system parameters are listed in Table I. These parameters are chosen in accordance to practical considerations. With the chosen OFDM symbol duration, the subchannel frequency separation, Δf, has to be 10 GHz, which has been used in several all-optical OFDM experiments [10], [41]. The pulse width, T_p, in Scheme II should be less than $T_c = T/N$. Here, we assume that the ratio δ/T_p in this scheme is equal to 0.04.

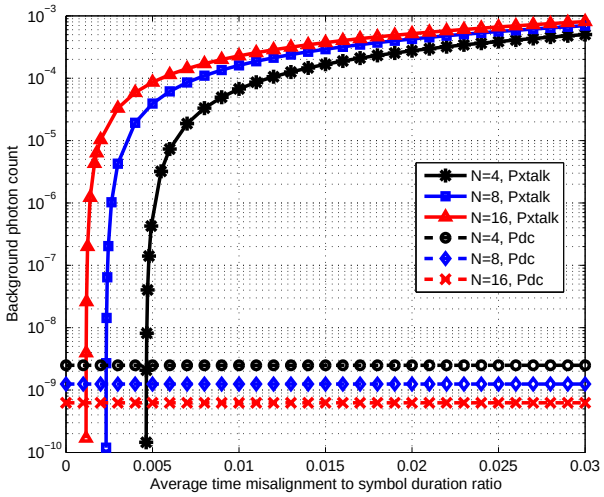

Fig. 8: Background photon count probability components p_{dc} and p_{xtalk} versus $\text{E}\{|\tau_k|\}/T$ for Scheme II with active OFDM decoder, for different values of N.

In order to see the importance of the time misalignment issue, we first look at its induced cross talk contribution as compared to the dark count component. Figure 8 compares the two elements of the background noise, i.e., p_{dc} and p_{xtalk}, versus a normalized measure of misalignment, $\text{E}\{|\tau_k|\}/T$, in the special case of Scheme II with active decoders. A similar overall behavior is observed for other schemes as well. It is clear that while the cross talk is negligible for low values of time misalignment, it becomes the major source of noise in our OFDM-QKD setups. We next consider the effect of time misalignment on each of the proposed setups.

Figure 9 shows the effect of time misalignment on the total secret key generation rate, R_{OFDM}, of Scheme I with and without optimal time gating. In the latter case, the gate width is a constant T_c. It can be seen that by optimizing the gate interval the secret key rate significantly improves. It will, however, barely surpass the performance of a single-carrier link, shown on top of Fig. 9, run at the same clock rate as the OFDM system. The main reason for this is the loss factor N due to the time gating, which results in a reduced key rate per carrier. Moreover, Fig. 9 shows that a system with a larger number of subcarriers, N, is more susceptible to time misalignment errors. This has to do with the interplay between p_{xtalk} and η_g, where the latter turns out to be the dominant factor. In short, no rate advantage is obtained by Scheme I. It, nevertheless, can be used as a multiplexing tool for sharing the infrastructure between multiple service providers.

Next, Fig. 10 shows the total secret key rate of Scheme II with passive OFDM decoder versus $\text{E}\{|\tau_k|\}/T$. Here again,

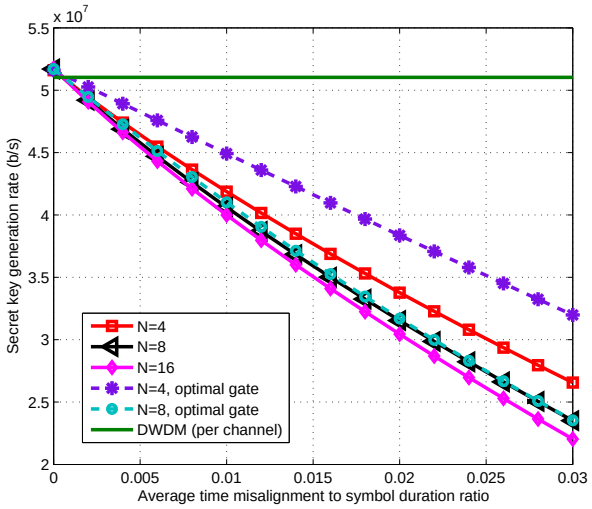

Fig. 9: Secret key generation rate versus $\mathrm{E}\{|\tau_k|\}/T$ for Scheme I and its optimal gate version, for different values of N.

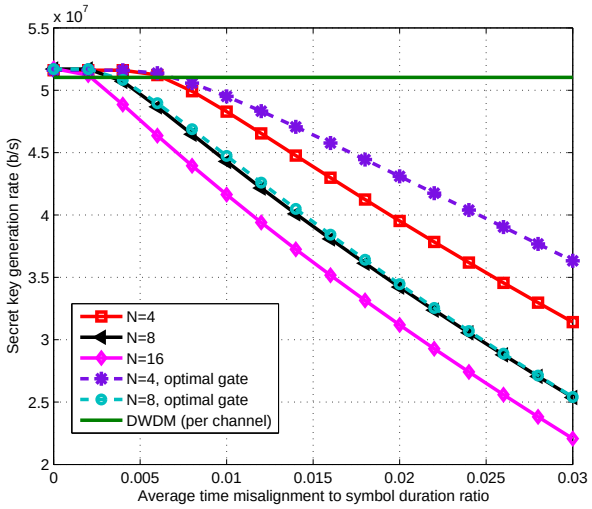

Fig. 10: Secret key generation rate versus $\mathrm{E}\{|\tau_k|\}/T$ for Scheme II with passive OFDM decoder and its optimal gate version, for different values of N. The parameter δ/T_p is chosen to be 0.04.

applying the optimal gate interval results in an enhancement in the secret key rate. Yet, no improvement, as compared to the DWDM-QKD system, is observed in the overall key rate by increasing N, which is mainly due to the inherent loss in the passive structure of the OFDM decoder.

The secret key generation rate of Scheme II with the proposed active OFDM decoder is depicted in Fig. 11. It can be seen that by multiplexing more subchannels in the system the secret key rate increases. This increase is initially linear with the number of subchannels, but once the time misalignment kicks in the key rate also correspondingly drops. Nevertheless, it always stays above that of the single DWDM-QKD channel depicted in the bottom of the figure. In fairness to the DWDM system, we have accounted for 2 dB of additional insertion loss for the optical switch in the OFDM-QKD system. The DWDM curve uses 100-ps-long pulses. Under these conditions, for $N = 16$, and at a normalized average time misalignment of 0.02, we are doing almost 6 times better than the single carrier link. That would demonstrate the prospect of using OFDM techniques at the core of QKD networks.

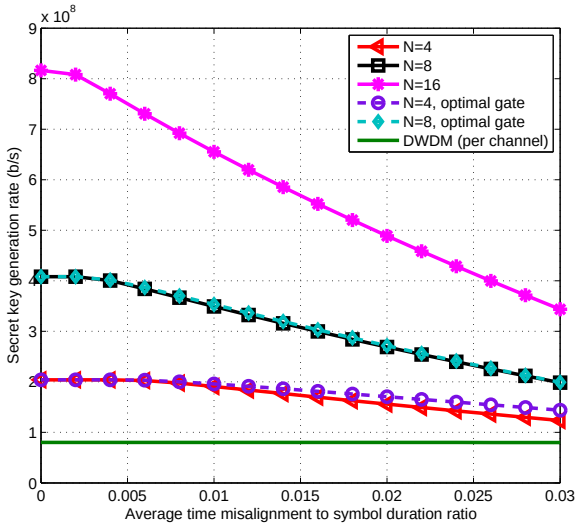

Fig. 11: Secret key generation rate versus $\mathrm{E}\{|\tau_k|\}/T$ for Scheme II with active OFDM decoder and its optimal gate version, for different values of N. The parameter δ/T_p is chosen to be 0.04.

In addition to the total key rate, we also look at the spectral efficiency of each scheme, S, defined by the ratio of the secret key generation rate and the allocated bandwidth. In the case of a DWDM link with channel spacing of 50 GHz, in Fig. 11, $S = 0.16\%$. For the OFDM-QKD systems, assuming that the allocated bandwidth is given by N/T, S has a peak value of 0.5%, which is three times higher than that of the DWDM system. Once time misalignment kicks in, the OFDM-QKD systems with lower values of N are favored as they are less susceptible to such errors. Overall, it can be seen that by multiplexing 4–8 OFDM subcarriers, one can outperform DWDM-QKD systems both in terms of the total key rate and the spectral efficiency in practical regimes of operation [32].

VI. Conclusions

We proposed a spectrally efficient approach to multiplexing QKD channels, namely, OFDM-QKD. Based on the principles of all-optical OFDM in classical communications, several OFDM-QKD schemes were considered. These schemes were analyzed in detail, in terms of their secret key generation rate, considering time-alignment imperfections, which are critical in all-optical OFDM systems. It was shown that such time misalignment issues would introduce a crosstalk noise with a degrading effect on the key rate, similar to that of background noise. We showed that by reducing the gate interval to an optimal value this problem could be alleviated to a large extent. Most importantly, we showed that the existing passive structures for the OFDM decoder would provide no gain in their multiplexing, in terms of the total achievable key rate. We proposed an active OFDM decoder, which, by using an optical switch, followed by proper delays and a passive FFT circuit,

could eliminate the inherent loss in passive decoders. We remark that, in the case of active decoders, ultrafast switches with a transition time on the order of picoseconds may be required. This is due to the short time separation of pulses within an OFDM symbol [38], [42]. This may add to the cost and complexity of the system. Nevertheless, we showed that, using our proposed active decoders, we could outperform the alternative DWDM-QKD systems in terms of the total key rate and spectral efficiency. This implies that OFDM-QKD can provide a high-rate spectrally efficient method of key exchange at the core of trusted-node QKD networks.

Appendix A
OFDM-QKD with misalignment errors

In this appendix, we analyze the operation of our proposed OFDM-QKD setups in the presence of time misalignment.

A. Scheme I

We start our analysis by assuming that each subcarrier has a time misalignment τ_k, $0 < |\tau_k| < T_c$, with respect to the time gating interval. Without loss of generality, we assume that $0 \leq \tau_k < T_c$ (both cases of $\tau_k > 0$ and $\tau_k < 0$ have the same effect). Figure 12(a) shows the shifted copies of the k^{th} subcarrier pulse in the presence of time misalignment τ_k. As can be seen in the figure, the shifted copies does not overlap completely in the gate interval, which leads to different summation results in two distinct time intervals, as follows:

$$t \in (T-T_c, T-T_c+\tau_k) \Rightarrow \hat{X}_m(t) = \begin{cases} \frac{1}{N}\hat{a}_k(t) & k \neq m \\ \frac{N-1}{N}\hat{a}_m(t) & k = m \end{cases} \quad (28)$$

$$t \in (T-T_c+\tau_k, T) \Rightarrow \hat{X}_m(t) = \begin{cases} 0 & k \neq m \\ \hat{a}_m(t) & k = m \end{cases}. \quad (29)$$

As a consequence, equation (18) is modified to

$$\hat{d}_m(t) = \frac{j}{2}\{\frac{N-1}{N}(e^{j\phi_B^{(m)}}\hat{a}_r^{(m)}(t) + \hat{a}_s^{(m)}(t))|_{t\in(T-T_c,T-T_c+\tau_m)} + (e^{j\phi_B^{(m)}}\hat{a}_r^{(m)}(t) + \hat{a}_s^{(m)}(t))|_{t\in(T-T_c+\tau_m,T)} + \frac{1}{N}\sum_{k\neq m}(e^{j\phi_B^{(k)}}\hat{a}_r^{(k)}(t) + \hat{a}_s^{(k)}(t))|_{t\in(T-T_c,T-T_c+\tau_k)}\}, \quad (30)$$

with the third term representing the inter-subcarrier crosstalk on the m^{th} subcarrier. Here, we neglected the vacuum operators due to their elimination once we apply the measurement operator. The background count due to this crosstalk may influence the performance of the system, as we will show in the following.

Defining $\hat{g}_k(t) \triangleq \frac{1}{N}(e^{j\phi_B^{(k)}}\hat{a}_r^{(k)}(t) + \hat{a}_s^{(k)}(t))$ with initial state $|\alpha\rangle_r|\alpha e^{j\phi_A^{(k)}}\rangle_s$, we can write

$$\langle\hat{g}_k^\dagger\hat{g}_k\rangle = \frac{2\mu}{N^2}(1 + cos(\phi_A^{(k)} - \phi_B^k))\frac{\tau_k}{T}. \quad (31)$$

Here, $\mu = |\alpha|^2$ and $\phi_A^{(k)}$ is the relative phase produced by the QKD encoder of the k^{th} subcarrier. We then calculate the expected value of (31) as a function of $(\phi_A^{(k)} - \phi_B^{(k)})$, which results in

$$\mathrm{E}_{(\phi_A^{(k)}-\phi_B^k)}\{\langle\hat{g}_k^\dagger\hat{g}_k\rangle\} = \frac{1}{2}\mathrm{E}_{(\phi_A^{(k)}-\phi_B^{(k)})}\{\langle\hat{g}_k^\dagger\hat{g}_k\rangle|basis = \{0,\pi\}\} + \frac{1}{2}\mathrm{E}_{(\phi_A^{(k)}-\phi_B^{(k)})}\{\langle\hat{g}_k^\dagger\hat{g}_k\rangle|basis = \{\pi/2, 3\pi/2\}\} = \frac{2\mu\tau_k}{N^2T}. \quad (32)$$

Note that cross terms between any two different subcarriers also appear in the $\langle\hat{d}_m^\dagger\hat{d}_m\rangle$. Here, we assume that the laser sources have independent phases. In this case, the phase difference corresponding to any cross term has uniform distribution on the interval $[-\pi, \pi]$. These terms are then eliminated due to their zero expected values. At this point, we generalize our result to include the case $-T_c \leq \tau_k < 0$. Hence, equation (32) can be rewritten as

$$\mathrm{E}_{(\phi_A^{(k)}-\phi_B^k)}\{\langle\hat{g}_k^\dagger\hat{g}_k\rangle\} = \frac{2\mu|\tau_k|}{N^2T}. \quad (33)$$

In the last step, the partial crosstalks due to each subcarrier are added to obtain the total crosstalk background count on the m^{th} subcarrier, denoted by $p_{\mathrm{xtalk}}^{(m)}$, as follows:

$$p_{\mathrm{xtalk}}^{(m)} = \eta'\frac{2\mu}{N^2T}\sum_{k\neq m}\mathrm{E}\{|\tau_k|\}, \quad (34)$$

where η' is the transmissivity of the link, excluding the loss of time gating. Under the assumption that $|\tau_k|$'s are i.i.d random variables, $p_{\mathrm{xtalk}}^{(m)}$ is independent of the subcarrier index. So, we can express the crosstalk background count per subcarrier as

$$p_{\mathrm{xtalk}} = \eta'\frac{2\mu(N-1)\mathrm{E}\{|\tau_k|\}}{N^2T}. \quad (35)$$

Such time misalignments change the loss factor in the time gating operation, η_g, due to the additional loss occurring in the interval $(T-T_c, T-T_c+\tau_m)$ in (30). η_g is then given by

$$\eta_g = \frac{1}{N} - (\frac{\mathrm{E}\{|\tau_k|\}}{T})(1 - (\frac{N-1}{N})^2). \quad (36)$$

Now, let us reduce the gate interval by b from each side to reduce the crosstalk effect. It can be concluded from Fig. 12(a) that $p_{\mathrm{xtalk}} = \mathrm{E}\{A\}$, where A is obtained by

$$A = \begin{cases} \eta'\frac{2\mu(N-1)}{N^2T}(|\tau_k| - b) & |\tau_k| \geq b \\ 0 & |\tau_k| \leq b \end{cases} \quad (37)$$

and p_{xtalk} can be expressed as

$$p_{\mathrm{xtalk}} = \eta'\frac{2\mu(N-1)}{N^2T}p(|\tau_k| \geq b)(\mathrm{E}\{|\tau_k|||\tau_k| \geq b\} - b). \quad (38)$$

Furtheremore, $\eta_g = \mathrm{E}\{B\}$, where

$$B = \begin{cases} \frac{1}{N} - \frac{2b}{T} - \frac{1}{T}(1 - (\frac{N-1}{N})^2)((|\tau_k| - b) & |\tau_k| \geq b \\ 0 & 0 \leq |\tau_k| \leq b \end{cases} \quad (39)$$

and

$$\eta_g = \frac{1}{N} - \frac{2b}{T} - \frac{1}{T}(1 - (\frac{N-1}{N})^2)p(|\tau_k| \geq b)(\mathrm{E}\{|\tau_k|||\tau_k| \geq b\} - b). \quad (40)$$

B. Scheme II

As explained in Sec. II, two receiver structures can be applied for this scheme: the passive OFDM decoder used in Scheme I, and the active OFDM decoder, which exploits an optical switch. In this subsection, we derive the crosstalk background count for both receiver structures.

First, we consider Scheme II with a passive OFDM decoder. We assume a time misalignment τ_k, $0 < |\tau_k| < T_c$, with respect to the time gating interval for each tributary. Figure 12(b)

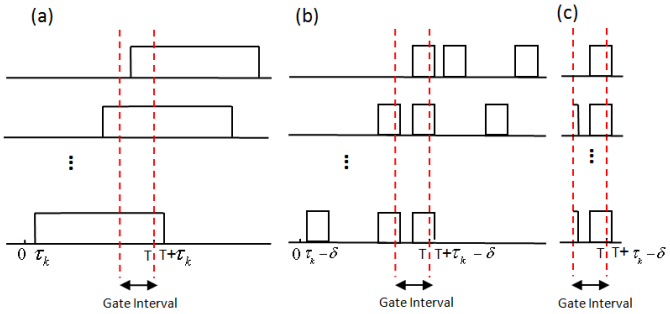

Fig. 12: Shifted copies of the signal corresponding to k^{th} tributary in the presence of the time misalignment τ_k, for (a) Scheme I, (b) Scheme II with passive OFDM decoder, (c) Scheme II with active OFDM decoder.

depicts the replicas of the pulse series corresponding to the k^{th} tributary. We denote the width of each pulse by T_p. Following the same steps as in the previous subsection, we conclude that the output operator, $\hat{d}_m(t)$, for $0 < \tau_k < \delta$ is given by

$$\hat{d}_m(t) = \frac{j}{2}(e^{j\phi_B^{(m)}}\hat{a}_r^{(m)}(t) + \hat{a}_s^{(m)}(t)), \tag{41}$$

and for $\delta < \tau_k < T_c$ we have

$$\begin{aligned}\hat{d}_m(t) &= \frac{j}{2}\{\frac{N-1}{N}(e^{j\phi_B^{(m)}}\hat{a}_r^{(m)}(t) + \hat{a}_s^{(m)}(t))|_{t\in(T-T_c,T-T_c+\tau_m-\delta)} \\ &+ (e^{j\phi_B^{(m)}}\hat{a}_r^{(m)}(t) + \hat{a}_s^{(m)}(t))|_{t\in(T-T_c+\tau_m+\delta,T)} \\ &+ \frac{1}{N}\sum_{k\neq m}(e^{j\phi_B^{(m)}}\hat{a}_r^{(k)}(t) + \hat{a}_s^{(k)}(t))|_{t\in(T-T_c,T-T_c+\tau_k-\delta)}\},\end{aligned} \tag{42}$$

where $\delta = (T_c - T_p)/2$. From this equation we can conclude that in the case of $\delta < |\tau_k| < T_c$, an inter-subcarrier crosstalk is introduced. We can then derive the background count of such crosstalk by applying the same strategy as in the previous subsection. The final result can be expressed as

$$p_{\text{xtalk}} = \eta' \frac{2\mu(N-1)}{N^3 T_p} p(|\tau_k| \geq \delta)(\mathrm{E}\{|\tau_k|||\tau_k| > \delta\} - \delta). \tag{43}$$

Furthermore, the degrading effect of time misalignment on η_g modifies this parameter to

$$\eta_g = \frac{1}{N} - (\frac{1}{NT_p})(1 - (\frac{N-1}{N})^2)p(|\tau_k| \geq \delta)(\mathrm{E}\{|\tau_k|||\tau_k| > \delta\} - \delta). \tag{44}$$

Now, we consider the narrowed gate case. If the gate interval is decreased by b from each side, we can conclude from Fig. 12(b) that $p_{\text{xtalk}} = \mathrm{E}\{A\}$, where

$$A = \begin{cases} \eta' \frac{2\mu(N-1)}{N^3 T_p}(|\tau_k| - b - \delta) & |\tau_k| \geq b + \delta \\ 0 & |\tau_k| \leq b + \delta \end{cases} \tag{45}$$

Hence, p_{xtalk} can be written as

$$p_{\text{xtalk}} = \eta' \frac{2\mu(N-1)}{N^3 T_p} p(|\tau_k| \geq b+\delta)(\mathrm{E}\{|\tau_k|||\tau_k| \geq b+\delta\} - (b+\delta)). \tag{46}$$

The loss factor η_g is also obtained by $\mathrm{E}\{B\}$, where B is given by

$$B = \begin{cases} \frac{1}{N} - \frac{2b}{NT_p} - \frac{1}{NT_p}(1 - (\frac{N-1}{N})^2)((|\tau_k| - (b+\delta)) & |\tau_k| \geq b + \delta \\ \frac{1}{N} - \frac{|\tau_k|+b-\delta}{NT_p} & |b-\delta| \leq |\tau_k| \leq b + \delta \\ \frac{1}{N} - \frac{2(b-\delta)}{NT_p}u(b-\delta) & 0 \leq |\tau_k| \leq |b-\delta| \end{cases} \tag{47}$$

where $u(.)$ is the step function. Hence, η_g can be expressed as

$$\begin{aligned}\eta_g = \frac{1}{N} &- \{(\frac{2b}{NT_p} - \frac{(b+\delta)}{NT_p}(1 - (\frac{N-1}{N})^2))p(|\tau_k| \geq b+\delta) + \\ &\frac{1}{NT_p}(1 - (\frac{N-1}{N})^2)p(|\tau_k| \geq b+\delta)(\mathrm{E}\{|\tau_k|||\tau_k| \geq b+\delta\}) + \\ &\frac{(b-\delta)}{NT_p}p(|b-\delta| \leq |\tau_k| \leq b+\delta)) + \frac{1}{NT_p}(p(|\tau_k| \geq |b-\delta|) \\ &(\mathrm{E}\{|\tau_k|||\tau_k| \geq |b-\delta|\}) - p(|\tau_k| \geq b+\delta)(\mathrm{E}\{|\tau_k|||\tau_k| \geq b+\delta\})) \\ &-\frac{2(b-\delta)}{NT_p}p(|\tau_k| < b-\delta)u(b-\delta)\}\end{aligned} \tag{48}$$

Next, we discuss the time misalignment issue in Scheme II with an active OFDM decoder. Figure 12(c) shows the pulse series of the k^{th} tributary in the presence of time misalignment τ_k, $0 < |\tau_k| < T_c$, with respect to the switching time. Due to the elimination of the loss incurred by passive serial to parallel conversion, equations (41) and (42) are modified by a multiplicative factor $\sqrt{N}$. Hence, the parameters p_{xtalk} and η_g are, respectively, given by (43) and (44), multiplied by N.

References

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

[2] M. Sasaki *et al.*, "Field test of quantum key distribution in the Tokyo QKD Network," *Opt. Exp.*, vol. 19, no. 11, pp. 10 387–10 409, 2011.

[3] M. Razavi, "Multiple-access quantum key distribution networks," *IEEE Trans. Commun.*, vol. 60, no. 10, pp. 3071–3079, 2012.

[4] P. D. Townsend, "Quantum cryptography on multiuser optical fibre networks," *Nature*, vol. 385, no. 6611, pp. 47–49, 1997.

[5] K.-I. Kitayama, M. Sasaki, S. Araki, M. Tsubokawa, A. Tomita, K. Inoue, K. Harasawa, Y. Nagasako, and A. Takada, "Security in photonic networks: threats and security enhancement," *Journal of Lightwave Technology*, vol. 29, no. 21, pp. 3210–3222, 2011.

[6] A. Ciurana, J. Martínez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden, and V. Martin, "Quantum metropolitan optical network based on wavelength division multiplexing," *Optics express*, vol. 22, no. 2, pp. 1576–1593, 2014.

[7] 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.

[8] D. Hillerkuss, M. Winter, M. Teschke *et al.*, "Simple all-optical FFT scheme enabling Tbit/s real-time signal processing," *Optics express*, vol. 18, no. 9, pp. 9324–9340, 2010.

[9] D. Hillerkuss, R. Schmogrow, T. Schellinger *et al.*, "26 Tbit/s line-rate super-channel transmission utilizing all-optical fast Fourier transform processing," *Nature Photonics*, vol. 5, no. 6, pp. 364–371, 2011.

[10] Z. Wang, K. S. Kravtsov, Y.-K. Huang, and P. R. Prucnal, "Optical FFT/IFFT circuit realization using arrayed waveguide gratings and the applications in all-optical OFDM system," *Optics express*, vol. 19, no. 5, pp. 4501–4512, 2011.

[11] S. Shimizu, G. Cincotti, and N. Wada, "Demonstration and performance investigation of all-optical OFDM systems based on arrayed waveguide gratings," *Optics express*, vol. 20, no. 26, pp. B525–B534, 2012.

[12] J. Schröder, L. B. Du, J. Carpenter, B. J. Eggleton, and A. J. Lowery, "All-optical OFDM with cyclic prefix insertion using flexible wavelength selective switch optical processing," *Journal of Lightwave Technology*, vol. 32, no. 4, pp. 752–759, 2014.

[13] H. Chen, M. Chen, and S. Xie, "All-optical sampling orthogonal frequency-division multiplexing scheme for high-speed transmission system," *Lightwave Technology, Journal of*, vol. 27, no. 21, pp. 4848–4854, 2009.

[14] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[15] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. IEEE Comp. Soc. Press, 1994, p. 124.

[16] D. Stucki *et al.*, "Long-term performance of the swissquantum quantum key distribution network in a field environment," *New Journal of Physics*, vol. 13, no. 12, p. 3001, 2011.
[17] W. Chen *et al.*, "Field experiment on a star type metropolitan quantum key distribution network," *IEEE Photon. Technol. Lett.*, vol. 21, no. 9, pp. 575–577, May 2009.
[18] K. A. Patel *et al.*, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Phys. Rev. X*, vol. 2, p. 041010, Nov. 2012.
[19] S. Wang *et al.*, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," *Opt. Lett.*, vol. 37, no. 6, pp. 1008–1010, March 2012.
[20] W. Maeda, A. Tanaka, S. Takahashi, A. Tajima, and A. Tomita, "Technologies for quantum key distribution networks integrated with optical communication networks," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 15, no. 6, pp. 1591–1601, 2009.
[21] I. Choi, R. J. Young, and P. D. Townsend, "Quantum information to the home," *New J. Phys.*, vol. 13, p. 063039, June 2011.
[22] M. Razavi, N. Lo Piparo, C. Panayi, and D. E. Bruschi, "Architectural considerations in hybrid quantum-classical networks (invited paper)," in *Iran Workshop on Communication and Information Theory (IWCIT)*, Tehran, Iran, 2013, pp. 1–7.
[23] N. Lo Piparo and M. Razavi, "Long-distance trust-free quantum key distribution," *J. Select. Topics Quantum Electron.*, vol. 21, p. 6600508, May 2015.
[24] L. Sheridan and V. Scarani, "Security proof for quantum key distribution using qudit systems," *Physical Review A*, vol. 82, no. 3, p. 030301, 2010.
[25] M. Razavi, "Multiple-access quantum-classical networks," in *Conf. Proc. Quantum Commun. Meas. Comput.*, vol. 1363. Am. Inst. Phys., 2011, pp. 39–42.
[26] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.* , vol. 94, p. 230504, June 2005.
[27] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, p. 012326, July 2005.
[28] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sep 2009.
[29] J. Armstrong, "OFDM for optical communications," *Lightwave Technology, Journal of*, vol. 27, no. 3, pp. 189–204, 2009.
[30] W. Shieh and I. Djordjevic, *OFDM for optical communications*. Academic Press, 2009.
[31] S. Chandrasekhar and X. Liu, "Experimental investigation on the performance of closely spaced multi-carrier PDM-QPSK with digital coherent detection," *Optics express*, vol. 17, no. 24, pp. 21 350–21 361, 2009.
[32] M. Ali, B. Dai, and X. Wang, "16-QAM all-optical OFDM system performance evaluation with time and frequency offsets," *Microwave and Optical Technology Letters*, vol. 57, no. 7, pp. 1593–1597, 2015.
[33] M. Ali, B. Dai, and X. Wang, "Time and frequency synchronisation in all-optical orthogonal frequency division multiplexing systems," *IET Communications*, vol. 9, no. 5, pp. 630–637, 2015.
[34] T. Pollet, M. Van Bladel, and M. Moeneclaey, "BER sensitivity of OFDM systems to carrier frequency offset and Wiener phase noise," *Communications, IEEE Transactions on*, vol. 43, no. 2/3/4, pp. 191–193, 1995.
[35] G. Colavolpe, T. Foggi, E. Forestieri, and M. Secondini, "Impact of phase noise and compensation techniques in coherent optical systems," *Lightwave Technology, Journal of*, vol. 29, no. 18, pp. 2790–2800, 2011.
[36] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Source attack of decoy-state quantum key distribution using phase information," *Phys. Rev. A*, vol. 88, p. 022308, Aug 2013.
[37] M. E. Marhic, "Discrete Fourier transforms by single-mode star networks," *Opt. Lett.*, vol. 12, no. 1, pp. 63–65, Jan 1987.
[38] A. Bogoni, X. Wu, S. R. Nuccio, J. Wang, Z. Bakhtiari, and A. E. Willner, "Photonic 640-Gb/s reconfigurable OTDM add–drop multiplexer based on pump depletion in a single PPLN waveguide," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 18, no. 2, pp. 709–716, 2012.
[39] 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.
[40] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, "Memory-assisted measurement-device-independent quantum key distribution," *New Journal of Physics*, vol. 16, no. 4, p. 043005, 2014.
[41] A. J. Lowery and L. Du, "All-optical OFDM transmitter design using awgrs and low-bandwidth modulators," *Optics express*, vol. 19, no. 17, pp. 15 696–15 704, 2011.
[42] H.-F. Chou, J. E. Bowers, and D. J. Blumenthal, "Compact 160-Gb/s add-drop multiplexing with a 40-Gb/s base-rate," in *Optical Fiber Communication Conference*. Optical Society of America, 2004, p. PD28.

Sima Bahrani received B.Sc. and M.Sc. degrees in Electrical Engineering from Shiraz University, Shiraz, Iran. From 2012, she is with Optical Networks Research Laboratory (ONRL), at Sharif University of Technology, Tehran, Iran, where she is currently pursuing her Ph.D. degree in Electrical Engineering. Her research interests include all-optical OFDM, Quantum communications, and Quantum cryptography.

Mohsen Razavi received his B.Sc. and M.Sc. degrees (with honors) in Electrical Engineering from Sharif University of Technology, Tehran, Iran, in 1998 and 2000, respectively. From August 1999 to June 2001, he was a member of research staff at the Iran Telecommunications Research Center, Tehran, Iran, working on all-optical CDMA networks. He joined the Research Laboratory of Electronics, at the Massachusetts Institute of Technology (MIT), in 2001 to pursue his Ph.D. degree in Electrical Engineering and Computer Science, which he completed in 2006. He continued his work at MIT as a Post-doctoral Associate during Fall 2006, before joining the Institute for Quantum Computing at the University of Waterloo as a Post-doctoral Fellow in January 2007. He is currently an Associate Professor at the School of Electronic and Electrical Engineering at the University of Leeds. His research interests include a variety of problems in quantum cryptography, quantum optics, and quantum communications networks.

Jawad A. Salehi (M84SM07F10) received his B.S. degree from the University of California, Irvine, in 1979, and the M.S. and Ph.D. degrees from the University of Southern California, Los Angeles, in 1980 and 1984, respectively, all in electrical engineering. He is currently a Full Professor with the Optical Networks Research Laboratory (ONRL), Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran, where he is also the Co-founder of the Advanced Communications Research Institute (ACRI). From 1981 to 1984, he was a full-time Research Assistant at the Communication Science Institute, University of Southern California. From 1984 to 1993, he was a Member of Technical Staff of the Applied Research Area, Bell Communications Research (Bellcore), Morristown, NJ. During 1990, he was with the Laboratory of Information and Decision Systems, Massachusetts Institute of Technology (MIT), Cambridge, as a Visiting Research Scientist. From 1999 to 2001, he was the Head of the Mobile Communications Systems Group and the Co-director of the Advanced and Wideband Code-Division Multiple Access (CDMA) Laboratory, Iran Telecom Research Center (ITRC), Tehran. From 2003 to 2006, he was the Director of the National Center of Excellence in Communications Science, Department of Electrical Engineering, SUT. He holds 12 U.S. patents on optical CDMA. His current research interests include optical multiaccess networks, optical orthogonal codes (OOC), fiber-optic CDMA, femtosecond or ultrashort light pulse CDMA, spread-time CDMA, holographic CDMA, wireless indoor optical CDMA, all-optical synchronization, and applications of erbium-doped fiber amplifiers in optical systems. Prof. Salehi has been an Associate Editor for Optical CDMA of the IEEE TRANSACTIONS ON COMMUNICATIONS since May 2001. In September 2005, he was elected as the Interim Chair of the IEEE Iran Section. He was the recipient of several awards including Bellcores Award of Excellence, the Nationwide Outstanding Research Award from the Ministry of Science, Research, and Technology in 2003, and the Nations Highly Cited Researcher Award in 2004. In 2007, he received the Khwarazmi International Prize, first rank, in fundamental research and also the Outstanding Inventor Award (Gold medal) from the World Intellectual Property Organization (WIPO), Geneva, Switzerland. In 2010, he was promoted to IEEE Fellow for contributions to the fundamental principles in optical code division multiple access. He is among the 250 pre-eminent and most influential researchers worldwide in the Institute for Scientific Information.