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 is obtained if one uses conventional all-optical passive 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. The performance of the latter system will also be analyzed in the presence of system imperfections.

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

I. INTRODUCTION

QUANTUM communications is entering a new phase in its development that targets new markets and aims 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]. The reach of conventional QKD links is, nevertheless, limited as they rely on low-power signals, e.g., single photons [4]. 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 [5]–[10] and partly modify their setups in order to obtain spectrally efficient high-rate OFDM-QKD schemes.

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 [11], whose security is at risk with the advancement of technology [12]. In that sense, QKD provides a future-proof method of secure communications. The first proposed QKD protocol by Bennett and Brassard in 1984 (BB84) [4] 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], [13]–[15]. One key technique that has simplified the encoding equipment of QKD is the decoy-state protocol [16], which allows one to use laser pulses, rather than ideal single-photon sources. Recent demonstrations cover distances over 250 km [17] 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. 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 [15], [18]. Multiple-access techniques are also needed to enable interference-free access to different quantum users [3], [19]. 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 [15]. 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 [20].

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 signaling to send more key bits per transmitted quantum state [21]. In addition to this, we should think how most efficiently we can use the available bandwidth per allocated wavelength. 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], [22], 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 [5]–[7]. 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 [7]–[10]. 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.

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 caused by the OFDM system. We propose an optimal gating solution to maximize the key rate. Some numerical results are 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 provide the qubits to be transmitted 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.

Different QKD protocols can be used in this OFDM-QKD setup. In this paper, we assume that the QKD encoders perform phase encoding using decoy-state techniques [16]. Based on the phase-encoded BB84 protocol, Alice chooses her phase value $\phi_A$ 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 successive pulses, separated by time $T_d$ and denoted by $r$ and $s$, with a relative phase corresponding to the chosen basis and the transmitted key bit. The time separation, $T_d$, is assumed to be no shorter than the OFDM symbol duration, $T$. The QKD decoding includes Bob’s selection of his measurement basis by choosing the phase $\phi_B$ from $[0, \pi/2]$ 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. The encoders’ outputs are then combined to form the OFDM signal. The signal representing each subchannel, at the output port of the combiner, must meet the requirements for decoy-state QKD protocols. At the

![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.](image)

![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 $\phi_B$. On the Bob’s side, a similar MZI is used to recombine $r$ and $s$ modes, followed by photodetection.](image)
receiver, ODFT is used to demultiplex the subcarriers. To comply with the OFDM orthogonality condition, in Scheme I, the pulse width is assumed to be \( T = 1/\Delta f \), where \( \Delta f \) 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:

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

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 \( \omega_0 \). At the OFDM decoder, the ODFT circuit effectively generates the outputs

\[
y_m(t) = \frac{1}{N} \sum_{n=0}^{N-1} x(t - nT_x)e^{j2\pi mn/N}, \quad m = 0, 1, ..., N - 1,
\]

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

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

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 (3), in the optical domain. In Scheme I, we assume that the ODFT is implemented by a passive structure consisted of \( N - 1 \) MZIs. Figure 5(a) shows an ODFT circuit for \( N = 4 \). This structure imitates the efficient method of realizing DFT, known as fast Fourier transform (FFT), by means of delays and phase shifts. 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, which can be implemented by electro-absorption modulators (EAM), or simply by time-gating the single-photon detectors used in the QKD decoders. 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 \( T_x \). Each short pulse, after splitting, is fed into QKD phase encoders to produce successive pulses \( r \) and \( s \). Each of these pulses will then go through an ODFT circuit generating \( N \) short pulses within an OFDM symbol duration \( T \). We assume that \( r \) and \( s \) pulses are apart by at least a period of \( T \).

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 \( T_x \) 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 \( \omega \) is given by

\[
x(t) = \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} A_k p(t - lT_x)e^{j2\pi kl/N},
\]

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

$$y_m(t) = \frac{1}{N^2} \sum_{n=0}^{N-1} \sum_{k=0}^{N-1} A_k p(t - (n + l)T_c) e^{i2\pi(kl+mn)/N},$$  \hspace{1cm} (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

$$z_m(t) = \sum_{k=0}^{N-1} A_k p(t - (N - 1)T_c) e^{i2\pi kl/N}.$$  \hspace{1cm} (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 \( m \)th 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 OFDM 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 [3], [23].

The loss-free 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.

III. QUANTUM ANALYSIS

In this section, we analyze the OFDM-QKD systems proposed in Sec. [1] 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. [8] and then we combine the results to find the output operators in QKD decoding modules.

![Fig. 7: (a) Proposed active ODFT Circuit. By employing an optical switch instead of 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.]

A. Scheme I

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

$$\hat{x}(t) = \sum_{k=0}^{N-1} \hat{a}_k e^{i\omega k t}, \hspace{1cm} 0 < t < T,$$

(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 \( \hat{b}_0(t) = \sum_{j=0}^{N-1} \hat{b}_0 e^{j\omega j t}, \hspace{1cm} \hat{b}_1(t) = \sum_{j=0}^{N-1} \hat{b}_1 e^{j\omega j t} \) and \( \hat{b}_2(t) = \sum_{j=0}^{N-1} \hat{b}_2 e^{j\omega j t} \) 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, \( \omega \), the transformation matrices of the three MZIs in Fig. [5] are given by

$$B_{\omega,1} = \frac{1}{2} \begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{-j\omega t} \end{pmatrix} \begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix}$$

(8)

for the MZI on the left,

$$B_{\omega,2} = \frac{1}{2} \begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{-j\omega t} \end{pmatrix} \begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix}$$

(9)

for the one on top right, and

$$B_{\omega,3} = \frac{1}{2} \begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & je^{-j\omega t} \end{pmatrix} \begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix}$$

(10)

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

$$\begin{pmatrix} \hat{a}_k(t) \\ \hat{b}_k(t) \end{pmatrix} = B_{\omega,1} \begin{pmatrix} \hat{a}_k(t) \\ \hat{b}_0(t) \end{pmatrix},$$

(11)
pulses of the OFDM signal overlap. The signal corresponding is only met in a region of width $T$ the above equation. As explained in Sec. II, the orthogonality 

\[
\left( \hat{y}_{0,k}(t) \right) = B_{\omega,k} \left( \hat{d}_k(t) \right), \quad (12)
\]

\[
\left( \hat{y}_{1,k}(t) \right) = B_{\omega,k} \left( \hat{b}_1(t) \right),
\]

\[
\left( \hat{y}_{2,k}(t) \right) = B_{\omega,k} \left( \hat{b}_2(t) \right). \quad (13)
\]

Then, applying the superposition principle, the output operator for output port $m$ in Fig. 5 is given by

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

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 vacuum 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:

\[
\hat{X}_m(t) = \frac{1}{N} \sum_{n=0}^{N-1} \hat{x}(t - nT_c) e^{2\pi i mn/N}, \quad m = 0, \ldots, N-1, \quad (15)
\]

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

\[
\hat{X}_m(t) = \frac{1}{N} \sum_{k=0}^{N-1} \hat{a}_k e^{2\pi i (f_0 + k\Delta f) t} \frac{1}{N} \sum_{n=0}^{N-1} e^{2\pi i (m-k) n/N}. \quad (16)
\]

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

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

where $A$ is either 1 or 1 and $\beta_{1i}$’s are constant coefficients. The operator $\hat{A} \hat{a}_m(t)$ is the evolved version of $\hat{a}_m$ and is given by $\hat{A} \hat{a}_m(t) = \hat{a}_m e^{\imath \omega t}$, 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

\[
\hat{d}_m(t) = \frac{1}{2} \left( e^{i \phi_{1r}} \hat{a}_r^{(m)}(t) + \hat{a}_s^{(m)}(t) \right) + \sum_{i=0}^{N-2} \sum_{n=0}^{N-1} \beta_{1i}^{(s)} \hat{b}_{1i}^{(s)}(t) + \sum_{i=0}^{N-2} \sum_{n=0}^{N-1} \beta_{1i}^{(r)} \hat{b}_{1i}^{(r)}(t), \quad T - T_c < t < T. \quad (18)
\]

B. Scheme II

To start our analysis in this scheme, we denote the annihilation operator corresponding to the spatial mode at the output of $k$th QKD encoder by $\hat{a}_k$. We assume that an ODFT 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

\[
\hat{x}(t) = \frac{1}{N} \sum_{i=0}^{N-1} \hat{c}_i [p(t - iT_c)]. \quad (19)
\]

where $\hat{c}_i = \sum_{k=0}^{N-1} \hat{d}_k e^{2\pi i kN/N}$ is the $p$th temporal mode at the output of the ODFT 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 protocol. 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

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

The coefficient $e^{2\pi i m/N}$ 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

\[
\hat{d}_m(t) = \left[ \frac{1}{2} (e^{i \phi_{1r}} \hat{a}_r^{(m)} + \hat{a}_s^{(m)}) + \sum_{i=0}^{N-2} \sum_{k=0}^{N-1} \beta_{ik}^{(s)} \hat{b}_{ik}^{(s)} + \sum_{i=0}^{N-2} \sum_{k=0}^{N-1} \beta_{ik}^{(r)} \hat{b}_{ik}^{(r)} \right] \times p(t - T + T_c). \quad (21)
\]

Another option for the receiver in this scheme is the structure we proposed in Fig. 7(a). For this active decoder, (21) is multiplied 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 [5].

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 [24], [25]. The average number of photons per QKD channel is given by $\mu$, 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 $\max[0, P(Y_0)]$, where

\[
P(Y_0) = Q_1(1 - h(e_1)) - f Q_2 h(E_p), \quad (22)
\]

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
\[ Q_\mu = 1 - (1 - Y_0)e^{-\eta_\mu}, \quad Q_\eta = (Y_0/2 + e_d(1 - e^{-\eta})) / Q_\mu, \]
where
\[ Y_1 = (1 - \eta)Y_0 + \eta \]
and $Y_0$ is the probability of a single photon state and $Y_0$ is the yield of a single photon state in the case where there is no detectable noise. The parameter $e_d$ represents the additional loss due to the OFDM decoding scheme. For instance, in Scheme I, with gate interval of $T_c$, the parameter $e_d$ equals $1/N$ in the ideal case. For Scheme II, and the active decoder of Fig. 7(a), $e_d$ is ideally one.

We calculate the parameters in (23) by finding the probabilities of interest once the QKD measurement parameters are known. For instance, the measurement operator for the representative photodetector in Fig. 3 is given by
\[ \hat{M} = \int_{\text{gate interval}} d_n(t) \xi_n(t) dt, \]
where $d_n(t)$ represents the dark count of the photodetectors, $\alpha$ is the channel loss factor in dB per unit of length, and $\eta_{\text{ins}}$ represents the additional loss due to the OFDM decoding scheme. For instance, in Scheme I, with gate interval of $T_c$, the parameter $e_d$ equals $1/N$ in the ideal case. For Scheme II, and the active decoder of Fig. 7(a), $e_d$ is ideally one.

We calculate the parameters in (23) by finding the probabilities of interest once the QKD measurement parameters are known. For instance, the measurement operator for the representative photodetector in Fig. 3 is given by
\[ \hat{M} = \int_{\text{gate interval}} d_n(t) \xi_n(t) dt, \]
where $d_n(t)$ represents the dark count of the photodetectors, $\alpha$ is the channel loss factor in dB per unit of length, and $\eta_{\text{ins}}$ represents the additional loss due to the OFDM decoding scheme. For instance, in Scheme I, with gate interval of $T_c$, the parameter $e_d$ equals $1/N$ in the ideal case. For Scheme II, and the active decoder of Fig. 7(a), $e_d$ is ideally one.

We calculate the parameters in (23) by finding the probabilities of interest once the QKD measurement parameters are known. For instance, the measurement operator for the representative photodetector in Fig. 3 is given by
\[ \hat{M} = \int_{\text{gate interval}} d_n(t) \xi_n(t) dt, \]
where $d_n(t)$ represents the dark count of the photodetectors, $\alpha$ is the channel loss factor in dB per unit of length, and $\eta_{\text{ins}}$ represents the additional loss due to the OFDM decoding scheme. For instance, in Scheme I, with gate interval of $T_c$, the parameter $e_d$ equals $1/N$ in the ideal case. For Scheme II, and the active decoder of Fig. 7(a), $e_d$ is ideally one.

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, $Y_1 = (1 - \eta)Y_0 + \eta$ is the yield of a single photon state and $Y_0$ is the probability of any detector click without having any transmitted photons from the corresponding QKD encoder. Furthermore, $e_d$ represents the probability of phase stability errors and the total transmissivity of the link is given by
\[ \eta = \eta_0 \eta_\mu \eta_{\text{ins}} 10^{-\alpha L/10}, \]
where $\eta_0$ is the quantum efficiency of the photodetectors, $\alpha$ is the channel loss factor in dB per unit of length and $\eta_{\text{ins}}$ represents any additional insertion loss in the link. Here, $\eta_\mu$ represents the additional loss due to the OFDM decoding scheme. For instance, in Scheme I, with gate interval of $T_c$, the parameter $\eta_\mu$ equals $1/N$ in the ideal case. For Scheme II, and the active decoder of Fig. 7(a), $\eta_\mu$ is ideally one.

We calculate the parameters in (23) by finding the probabilities of interest once the QKD measurement parameters are known. For instance, the measurement operator for the representative photodetector in Fig. 3 is given by
\[ \hat{M} = \int_{\text{gate interval}} d_n(t) \xi_n(t) dt, \]
where $d_n(t)$ represents the dark count of the photodetectors, $\alpha$ is the channel loss factor in dB per unit of length, and $\eta_{\text{ins}}$ represents the additional loss due to the OFDM decoding scheme. For instance, in Scheme I, with gate interval of $T_c$, the parameter $\eta_\mu$ equals $1/N$ in the ideal case. For Scheme II, and the active decoder of Fig. 7(a), $\eta_\mu$ is ideally one.

From the above equations, we can see that the key rate is given by
\[ R = \frac{1}{T_c} \left[ 2 \left( 1 - Q_\mu - Q_\eta \right) \right], \]
where $Q_\mu = 1 - (1 - Y_0)e^{-\eta_\mu}$ and $Q_\eta = (Y_0/2 + e_d(1 - e^{-\eta})) / Q_\mu$.

In order to analyze the secret key generation rate of the proposed schemes in more detail, one should consider the influence of major impairments in the system, which may degrade system performance. Here, we specifically consider time misalignment issues, which are known to be critical in all-optical OFDM systems [27], [28]. 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 $p_{\text{crosstalk}}$, which adds to the background noise, and, second, they slightly reduce the transmissivity factor $\eta_\mu$. One can reduce the crosstalk noise by reducing the width of the gate interval, but, by doing so, $\eta_\mu$ 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 $R_{\text{OFDM}}$ is maximized, where
\[ R_{\text{OFDM}} = \max[NP(Y_{\text{OFDM}}/T_c, 0)], \]
where $Y_{\text{OFDM}} = 1 - (1 - (\rho_{\text{dc}} + p_{\text{crosstalk}}))^2$.

In this section, we investigate the performance of the proposed OFDM-QKD schemes by considering the following three cases: Scheme I, Scheme II with a passive OFDM decoder, 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. The nominal values used for OFDM-QKD system parameters are listed in Table I. These parameters are chosen to meet certain practical considerations. With the chosen OFDM symbol duration, the subchannel frequency separation, $\Delta_f$, has to be 10 GHz, which has been used in several all-optical OFDM experiments [7], [29]. The pulse width, $T_p$, in Scheme II should be less than $T_c = T/N$. Here, we assume that the ratio $\delta/T_p$ in this scheme is equal to 0.05.

Figure 8 depicts the optimal gate width normalized by $T_c$ for different values of $N$ versus a normalized measure of misalignment $E[|\tau_k|]/T$. It can be seen that, for Scheme I the optimal gate width decreases once the time misalignment becomes larger. For Scheme II, the initial optimal gate width is equal to $T_p$. With the increase of time misalignment, this parameter increases to $T_c$ and then decreases. This is mainly because for small time misalignments, $p_{\text{crosstalk}}$ is approximately zero, but the optimal gate width should be increased from $T_p$ to prevent $\eta_\mu$ from unnecessary degradation. The optimal gate width is also a function of $N$, and except for small time misalignments in Scheme II, it goes down with $N$. In fact for large values of $N$, where, $T_c$ becomes proportionally small, it may not be possible to find an optimal gate as the cross talk noise covers the entire pulse width.

Figure 9 shows the effect of time misalignment on the total secret key generation rate, $R_{\text{OFDM}}$, of Scheme I and its optimized gate version. We used the optimal gate narrowing values in Fig. 8 in the latter case. It can be seen that by optimizing the gate interval the secret key rate significantly improves. It will, however, never surpass the performance of a single-carrier link 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 $p_{\text{crosstalk}}$ and $\eta_\mu$. 

V. NUMERICAL RESULTS
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 $E[|r_k|]/T$. Here again, applying the optimal gate interval results in an enhancement in the secret key rate. Yet, no improvement 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.

For the parameter values considered here, for $N = 16$, and at a normalized average time misalignment of 0.02, we are doing almost 8 times better than the single carrier link. That would demonstrate the prospect of using OFDM techniques at the core of QKD networks. On the other hand, considering the relative improvement achieved by applying optimal gate interval, it can be concluded that the active OFDM decoder

| Parameter                              | Value          |
|----------------------------------------|----------------|
| Average number of photons per signal pulse | 0.48           |
| Quantum Efficiency                     | 0.3            |
| Total insertion and path loss, $\eta_p 10^{-\delta L/10}$ | 10 dB          |
| Receiver dark count rate, $\gamma_{dc}$ | 1E-7 ns$^{-1}$ |
| Error correction inefficiency, $f$     | 1.22           |
| Phase stability error, $\epsilon_d$    | 0.033          |
| Laser pulse repetition interval, $T_p$  | 210 ps         |
| OFDM symbol duration, $T$              | 100 ps         |
| Number of subcarriers, $N$             | 4, 8, 16       |
VI. CONCLUSIONS

In this paper, 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 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 is 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 \([30]\). We showed that, using our proposed active decoders, OFDM-QKD could 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 \( \tau_k \), \( 0 < |\tau_k| < T_c \), 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 pulse of the \( k \)th subcarrier in the presence of the time misalignment \( \tau_k \). As can be seen in the figure, the shifted copies do not overlap completely in the gate interval, which leads to different summation results in two distinct time intervals, as follows:

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

\[
 t \in (T - T_c + \tau_k, T) \Rightarrow \hat{X}_m(t) = \begin{cases} 
 0 & k \neq m \\
 a_m(t) & k = m 
 \end{cases} \tag{29}
\]

As a consequence, equation (18) is modified to

\[
 \hat{a}_m(t) = \frac{1}{N} \sum_{k = -N/2}^{N/2} e^{i\phi_k} \hat{a}_m(t)_{k \in [T - T_c, T - T_c + \tau_k]} + e^{i\phi_k} \hat{a}_m(t)_{k \in [T - T_c + \tau_k, T]} + \frac{1}{N} \sum_{k = m} e^{i\phi_k} \hat{a}_m(t)_{k \in [T - T_c + \tau_k, T]} \tag{30}
\]

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 \( \hat{g}_k(t) = \frac{1}{N} (e^{i\phi_k} a_0(t) + \hat{a}_0(t)) \) with initial state \( |\alpha\rangle \langle \alpha| e^{i\phi_k} \rangle \), we can write

\[
 \langle \hat{g}_k^\dagger \hat{g}_k \rangle = \frac{2\mu}{N^2} (1 + \cos(\phi_0 - \phi_k)) \frac{T_c}{T}. \tag{31}
\]

Here, \( \mu = |\alpha|^2 \) and \( \phi_k \) 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 \( \phi_k - \phi_0 \), which results in

\[
 E_{\phi_0 - \phi_k}(\langle \hat{g}_k^\dagger \hat{g}_k \rangle) = \frac{1}{2} E_{\phi_0 - \phi_k}(\langle \hat{g}_k^\dagger \hat{g}_k \rangle)_{\text{basis} = \{0, \pi\}} + \frac{1}{2} E_{\phi_0 - \phi_k}(\langle \hat{g}_k^\dagger \hat{g}_k \rangle)_{\text{basis} = \{\pi/2, 3\pi/2\}} = \frac{2\mu T_c}{N^2 T} \tag{32}
\]

Note that cross terms between any two different subcarriers also appear in the \( \langle \hat{a}_m^\dagger \hat{a}_n \rangle \). 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

\[
 E_{\phi_0 - \phi_k}(\langle \hat{g}_k^\dagger \hat{g}_k \rangle) = \frac{2\mu |\tau_k|}{N^2 T}. \tag{33}
\]

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 \( p_{\text{xtalk}}^{(m)} \), as follows:

\[
 p_{\text{xtalk}}^{(m)} = \eta' \frac{2\mu}{N^2 T} \sum_{k \neq m} E(|\tau_k|), \tag{34}
\]

where \( \eta' \) 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, \( p_{\text{xtalk}}^{(m)} \) is independent of the subcarrier index. So, we can express the crosstalk background count per subcarrier as

\[
 p_{\text{xtalk}} = \eta' \frac{2\mu(N - 1) E(|\tau_k|)}{N^2 T}. \tag{35}
\]

Such time misalignments change the loss factor in the time gating operation, \( \eta_k \), due to the additional loss which occurs in the interval \( (T - T_c, T - T_c + \tau_m) \) in (30). Hence, \( \eta_k \) is given by

\[
 \eta_k = \frac{1}{N} - \frac{E(|\tau_k|)}{T} (1 - \frac{N - 1}{N}). \tag{36}
\]

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 \( p_{\text{xtalk}} = E(A) \), where \( A \) is obtained by

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

and \( p_{\text{xtalk}} \) can be expressed as

\[
 p_{\text{xtalk}} = \eta' \frac{2\mu(N - 1)}{N^2 T} p(|\tau_k| \geq b)E(|\tau_k||\tau_k| \geq b) - b. \tag{38}
\]
Furtheremore, \( \eta_g = E[B] \), where
\[
B = \begin{cases} 
\frac{1}{N} - \frac{2b}{T} - \frac{1}{N}((1 - \frac{N-1}{N})^2)(|\tau_k| - b) & |\tau_k| \geq b \\
0 & 0 \leq |\tau_k| \leq b 
\end{cases}
\]
and
\[
\eta_g = \frac{1}{N} - \frac{2b}{T} - \frac{1}{N}((1 - \frac{N-1}{N})^2)p(|\tau_k| \geq b)(E[|r_k||r_k| \geq b] - b).
\]
(40)

B. Scheme II

As explained in Sec. [11] 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 \( \tau_k \), \( 0 < |\tau_k| < T_c \), with respect to the time gating interval for each tributary. Figure 12(b) 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 \( 0 < \tau_k < T_c \) is given by
\[
0 < \tau_k < \delta \Rightarrow \hat{d}_m(t) = \frac{j}{2}(e^{j\omega_0m} \hat{a}_m(t) + \hat{a}_m^{(m)}(t))
\]
\[
\delta < \tau_k < T_c \Rightarrow \hat{d}_m(t) = \frac{j}{2} \left( \frac{1}{N} - \frac{2b}{T} \right)((1 - \frac{N-1}{N})^2)(|\tau_k| - b)\hat{a}_m(t) + \frac{1}{N} \sum_{k \neq m} (e^{j\omega_0m} \hat{a}_m(t) + \hat{a}_m^{(m)}(t)) \right)_{|\tau_k| \geq b} + \frac{1}{N} \sum_{k \neq m} (e^{j\omega_0m} \hat{a}_m(t) + \hat{a}_m^{(m)}(t)) \right)_{|\tau_k| < b}
\]
(41)
where \( \delta = (T_c - T_p)/2 \). From this equation we can conclude that in the case of \( \delta \leq |\tau_k| < T_c \), 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
\[
p_{\text{stalk}} = \frac{28(N-1)}{NT_p}p(|\tau_k| \geq \delta)(E[|r_k||r_k| > \delta] - \delta).
\]
(42)

Furthermore, the degrading effect of time misalignment on \( \eta_g \) modifies this parameter to
\[
\eta_g = \frac{1}{N} - \frac{2b}{T} - \frac{1}{N}((1 - \frac{N-1}{N})^2)p(|\tau_k| \geq \delta)(E[|r_k||r_k| > \delta] - \delta).
\]
(43)

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 \( p_{\text{stalk}} = E[A] \), where
\[
A = \begin{cases} 
\eta_g \frac{28(N-1)}{NT_p}p(|\tau_k| \geq b) & |\tau_k| \geq b + \delta \\
0 & 0 \leq |\tau_k| \leq b + \delta
\end{cases}
\]
(44)
Hence, \( p_{\text{stalk}} \) can be written as
\[
p_{\text{stalk}} = \eta_g \frac{28(N-1)}{NT_p}p(|\tau_k| \geq b + \delta)(E[|r_k||r_k| > b + \delta - (b + \delta)).
\]
(45)
The loss factor \( \eta_g \) is also obtained by \( E[B] \), where \( B \) is given by
\[
B = \begin{cases} 
\frac{1}{N} - \frac{2b}{T} - \frac{1}{N}((1 - \frac{N-1}{N})^2)(|\tau_k| - b) & |\tau_k| \geq b + \delta \\
0 & 0 \leq |\tau_k| \leq b + \delta
\end{cases}
\]
(46)
where \( u(.) \) is the step function. Hence, \( \eta_g \) can be expressed as
\[
\eta_g = \frac{1}{N} - \frac{2b}{T} - \frac{1}{N}((1 - \frac{N-1}{N})^2)p(|\tau_k| \geq b + \delta) + \frac{1}{NT_p}(1 - \frac{N-1}{N})^2p(|\tau_k| \geq \delta)(E[|r_k||r_k| > \delta]) + \frac{b - \delta}{NT_p}p(|\tau_k| \geq \delta) + \frac{1}{NT_p}(p(|\tau_k| \geq |b - \delta|) - \frac{1}{NT_p}(p(|\tau_k| > b + \delta)(E[|r_k||r_k| > b + \delta]) - \frac{b}{NT_p}p(|\tau_k| \geq |b - \delta|)(E[|r_k||r_k| > b + \delta]) - \frac{2(b - \delta)}{NT_p}p(|\tau_k| < b - \delta)u(b - \delta)
\]
(47)
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 \( \tau_k \), \( 0 < |\tau_k| < T_c \), with respect to the switching time. Due to the elimination of the loss incurred by passive serial to parallel conversion, equation (41) is modified by a multiplicative factor \( \sqrt{N} \). Hence, the parameters \( p_{\text{stalk}} \) and \( \eta_g \) are, respectively, given by (42) and (43), 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 KQD 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] 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.
[5] D. Hilkerkuss, 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.
[6] D. Hilkerkuss, R. Schnagrow, T. Schellingeret 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.
[7] 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.

[8] 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.

[9] M. Razavi, 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] K. A. Patel et al., “Cocurrence of high-bit-rate quantum key distribution and optical fiber,” *Phys. Rev. X*, vol. 2, pp. 041010, Nov. 2012.

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

[17] 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.

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

[19] 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 (IW CIT)*, Tehran, Iran, 2013, pp. 1–7.

[20] N. Lo Piparo and M. Razavi, “Long-distance trust-free quantum key distribution on optical fiber,” *Phys. Rev. X*, vol. 2, p. 041010, Nov. 2012.

[21] L. Sheridan and V. Scarani, “Security proof for quantum key distribution,” *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 1–7, Jan. 2005.

[22] M. E. Marhic, “Discrete Fourier transforms by single-mode star networks,” *Opt. Lett.*, vol. 12, no. 1, pp. 63–65, Jan 1987.

[23] 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.

[24] 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.

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

[26] 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. 21350–21361, 2009.

[27] M. Ali and X. Wang, “Effects of symbol time misalignment and frequency offset on performance of realistic all-optical odfm system,” in *Fast Fourier Transform and Its Applications*. IEEE Press, 1985, pp. 267–278.

[28] A. J. Lowery and L. Du, “All-optical ofdm transmitter design using awgs and low-bandwidth modulators,” *Optics express*, vol. 19, no. 17, pp. 15696–15704, 2011.

[29] A. Bogoni, X. Wu, S. R. Nuccio, J. Wang, Z. Bakhitiari, and A. E. Willner, “Photonic 640-gb/s reconfigurable odfm add-drop multiplexer based on pump depletion in a single pphn waveguide,” in *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 18, no. 2, pp. 709–716, 2012.