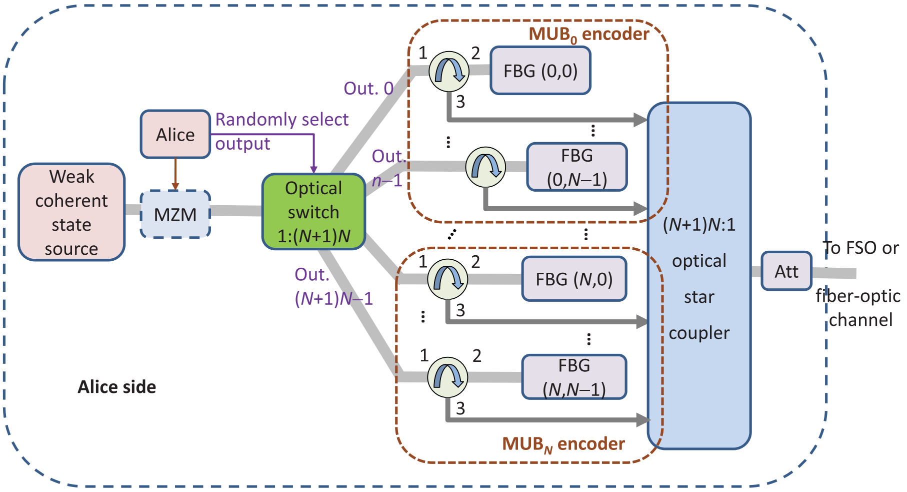
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

FBG-Based Weak Coherent State and Entanglement-Assisted Multidimensional QKD

Volume 10, Number 4, August 2018

Ivan B. Djordjevic



DOI: 10.1109/JPHOT.2018.2860524
1943-0655 © 2018 IEEE

FBG-Based Weak Coherent State and Entanglement-Assisted Multidimensional QKD

Ivan B. Djordjevic

Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ 85721 USA

DOI:10.1109/JPHOT.2018.2860524

Manuscript received June 10, 2018; revised July 23, 2018; accepted July 24, 2018. Date of publication July 26, 2018; date of current version August 10, 2018. This work was supported in part by the MURI Office of Naval Research Project N00014-13-1-0627. (e-mail: ivan@email.arizona.edu).

Abstract: In this paper, we propose several fiber Bragg gratings (FBGs) based on both weak coherent state (WCS) and entanglement-assisted (EA) multidimensional QKD (MQKD) protocols with mutually unbiased bases (MUBs) derived from the complex Hadamard matrices. We also propose how to implement them by using FBGs with orthogonal impulse responses, derived from Slepian sequences. The proposed FBG-based protocols are capable of simultaneously achieving unprecedented spectral efficiency and secret-key rates in long-distance quantum communication. Regarding the WCS protocols, random base selection and FGB-MUB-based protocols are introduced. Regarding EA protocols, we introduce a generic class of FBG-based *N*-dimensional protocols and describe the corresponding FBG-based encoders and decoders. The security analysis of the proposed MQKD protocols is further performed by taking into account FBG fabrication imperfections, modeled by the *L*-neighbor model. It has been shown that the proposed MQKD protocols significantly outperform the conventional two-dimensional QKD protocols, and impose less stringent bandwidth requirements compared to multidimensional time–frequency and time-bin protocols.

Index Terms: Quantum key distribution (QKD), Multidimensional QKD (MQKD), Fiber Bragg gratings (FBGs), Entanglement assisted MQKD protocols, Weak coherent state-based MQKD protocols.

1. Introduction

The quantum information processing has been intensively studied for various applications including quantum computation, quantum sensing, quantum communication, quantum key distribution (QKD, also known as quantum cryptography), and quantum radar applications [1]–[5]. It has been widely recognized that the underlying principles of quantum mechanics can be used to enable QKD with verifiable security. Specifically, the impossibility for an eavesdropper to tap the quantum channel and distinguish among non-orthogonal states without introducing disturbance to the quantum channel ensures that the quantum cryptography system is secure [2]. However, most of these previous research efforts have focused on two-dimensional quantum cryptography, commonly performed by employing the BB84 protocol. Unfortunately, SKRs in two-dimensional (2-D) QKD protocols are very low, and at the same time the distances are rather limited manly due to the presence of channel impairments and device imperfections. Moreover, the device imperfections can be exploited by Eve through quantum non-demolition measurements to compromise the security. To deal with polarization effects the polarization scrambling was proposed in [6], while the measurement-device-independent QKD was proposed in [7]. For some recent research 2-D experiments an interested reader is referred to [8]. It has been also proposed to employ either non-orthogonal quantum states [9] or differential phase-shift keying [10].

Another approach to improve the SKR is by introduction of multidimensional QKD protocols. Several methods have recently been proposed to increase the information content of photons for QKD applications [8]–[26]. These methods rely on encoding information either using time and frequency (known as t-f protocols) [8]–[13], linear momentum [16], [17], orbital angular momentum (OAM) [2], [3], [19]–[23], or using multiple degrees of freedom made available through hyper-entangled states [24], [25]. Single-photon multidimensional QKD (MQKD) has been experimentally demonstrated using OAM [23], as well as exploiting photon position and linear momentum [18]. However, all of these spatially-encoded schemes suffer from phase front distortion due to imperfect generation of the OAM modes. It has been experimentally demonstrated in [26] that the time-bin encoding can be used to improve the SKRs of 2-D protocols. Unfortunately, to increase the dimensionality, the duration of time-bins must be reduced, which significantly increases the bandwidth requirement and sacrifices the spectral efficiency.

To address these key challenges for QKD, we propose to employ the fiber Bragg gratings (FBGs) with mutually orthogonal impulse responses, denoted as $\{[\,0\rangle, |1\rangle, \ldots, |N-1\rangle\}$ as the encoding basis for MQKD. Both weak coherent state (WCS) and entanglement assisted MQKD protocols are possible with mutually unbiased bases (MUBs) derived from the complex Hadamard matrices. In the basic configuration, Alice will randomly select any of the base states with the same probability, indicating that $\log_2 N$ bits per photon is transmitted. Alice will also probe the channel for Eve's presence by sending the superposition state $(|0\rangle + |1\rangle + \cdots + |N-1\rangle)/\sqrt{N}$, with optimized probability (to maximize the SKR). Bob will be then, on the other hand, use the set of complex-conjugate FBGs, N circulators, and N single-photon detectors to detect Alice's transmitted state. In the second configuration, MUBs derived from complex Hadamard matrices will be used in well-known WCS MQKD protocol to transmit the raw key. To generate a base within an MUB, a single FBG, with properly weighted superimposed orthogonal impulse responses should be fabricated. To increase the dimensionality of the system, we need just to increase the number of FBGs rather than decreasing the slot duration like in either t-f or time-bin protocols. Finally, FBG-based entanglement assisted (EA) MQKD protocols will be described. Compared to parallel 2-D protocols, in which any crosstalk among parallel channels can increase the probability of photon loss in addition to increase in quantum bit-error rate (QBER), the crosstalk due to imperfectly fabricated FBGs in proposed MQKD protocols will result only in the SKR reduction thanks to multidimensionality of the system. Moreover, multidimensional signaling schemes are known to be more tolerant to atmospheric turbulence effects in free-space optical (FSO) links and fiber nonlinearities and polarization-mode dispersion (PMD) effects in fiber-optics channels [27].

The paper is organized as follows. In Section 2, two FBG-based WCS protocols are proposed. In Section 3, FBG-based entanglement assisted MQKD protocol is described. In Section 4, security analysis of FBG-based entanglement assisted MKQD protocols is provided. In Section 5, we provide relevant concluding remarks.

2. Proposed FBG-Based Weak Coherent State Protocols

In basic FBG-based *random base selection weak coherent state protocol*, we employ FBGs with mutually orthogonal impulse responses, denoted as $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$ as the encoding basis for MQKD, as illustrated in Fig. 1. The Alice encoder is composed of 1:($N+1$) optical switch, $N+1$ circulators, $N+1$ FBGs, and ($N+1$):1 optical star coupler (power combiner). The Mach-Zehnder modulator (MZM) is optional, it is used to perform NRZ to RZ conversion. When the weak coherent state source is based on a pulse laser, the MZM can be omitted. To encode Alice randomly selects the optical switch output, say the n-th output, and the n-th FBG imposes the corresponding impulse response on an attenuated laser pulse, which is passed to the star coupler. With N mutually orthogonal impulse responses imposed on FBGs, Alice can transmit $\log_2 N$ bits per signaling interval.

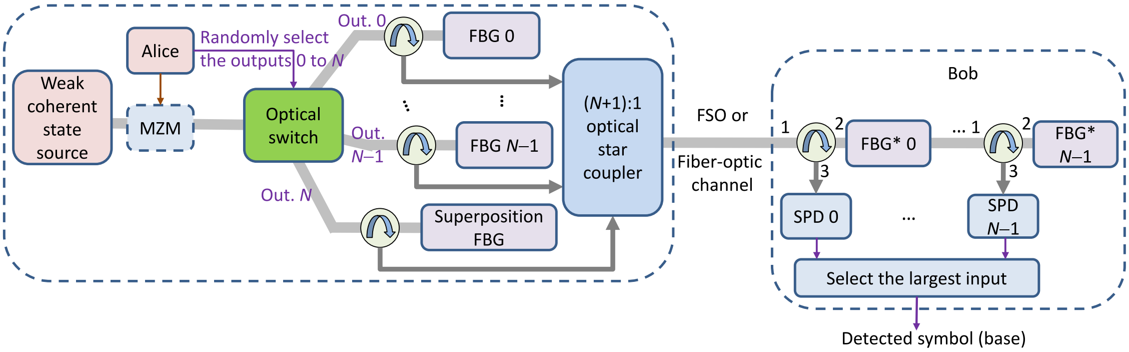


Fig. 1. Architecture implementing the basic FBG-based WCS protocol. FSO: free-space optical, SPD: single photon detector.

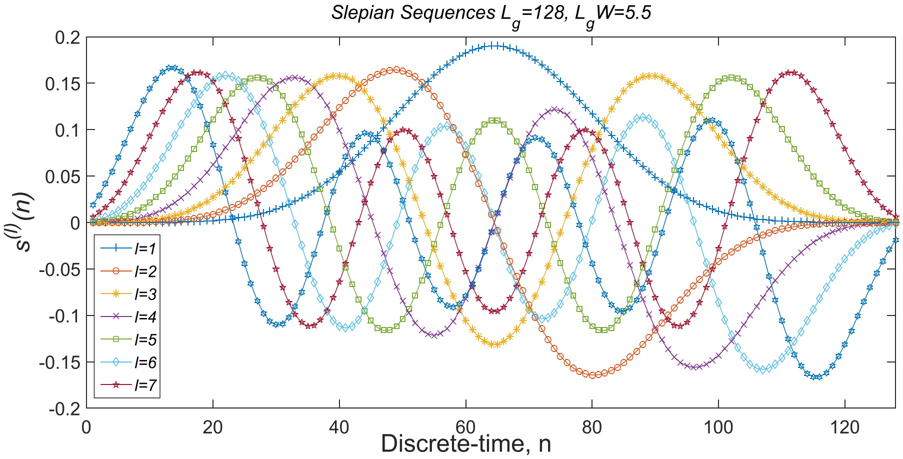


Fig. 2. Slepian sequences of order up to 7 for sequence length of $L_g = 128$ and discrete-time×half-bandwidth product $L_gW = 5.5$.

The superposition FBG is fabricated by writing the resulting impulse response, obtained by superposition of N mutual orthogonal impulse responses, on a single FBG. To probe for Eve's presence Alice selects the (N+1)-th optical switch output and therefore creates the superposition state $(|0\rangle + |1\rangle + \cdots + |N-1\rangle)/\sqrt{N}$. On receiver side, Bob employs a series of complex-conjugate FBGs. The matched complex-conjugate FBG reflects the pulse back, and the single-photon detector (SPD) at port 3 of circulator detects the presence of pulse, and Bob is able to identify the transmitted symbol by employing the select the largest input logic. When Bob detects the photons on majority of SPDs, he will know that this particular symbol should be used to estimate the quantum bit-error rate (QBER), and therefore to detect the presence of Eve. Other configurations employing the same concept are also possible.

The mutual orthogonal impulse response for FBG-design can be derived from Slepian sequences [27] as we proposed in [29], [30]. To implement the FBGs with mutual orthogonal impulse responses, with perfect impulse responses, the time-domain based FBG design algorithm should be used [30], [31]. Compared to conventional discrete layer peeling algorithm (DLPA) applied in spectral-domain [29], the time-domain FBG design results in FBGs with perfectly orthogonal impulse responses [30]. As an illustration, in Fig. 2 we provide the Slepian sequences of order up to seven to be used as FBG impulse responses, for sequence length $L_g = 128$ and discrete-time×half-bandwidth product $L_gW = 5.5$. On the hand, in Fig. 3 we provide the impulse response of designed FBG, obtained by employing the time-domain design algorithm, corresponding to the Slepian sequence of order

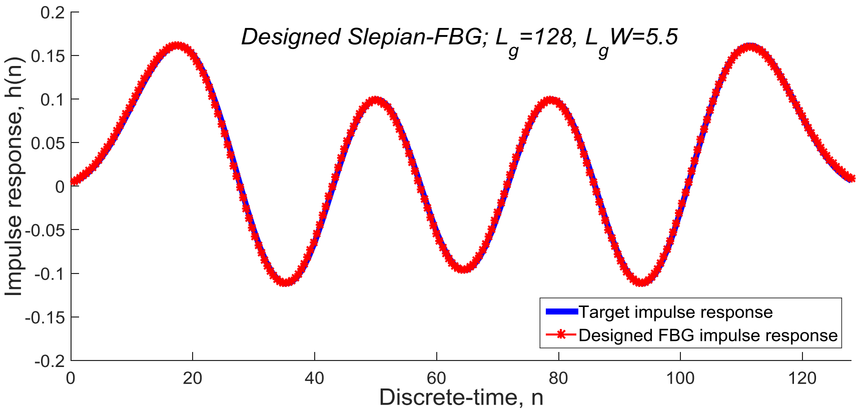


Fig. 3. Impulse responses of the target Slepian sequence of order 7 and designed FBG impulse response employing time-domain design algorithm (for sequence length of $L_g = 128$ and discrete-time×half-bandwidth product $L_gW = 5.5$).

7 (again for sequence length $L_g = 128$ and discrete-time×half-bandwidth product $L_gW = 5.5$), for discrete-time step size $\Delta = 0.1$. The accuracy of determining the parameters of FBG-section is $O(\Delta^3)$ [31], indicating that FBGs can be fabricated with high accuracy using this method. Clearly, an excellent agreement can be found between target and designed FBG impulse responses. The complex-basis functions can also be used as the impulse responses for FBGs.

To summarize, the *FBG-based random base selection WCS* protocol can be described as follows:

1) Alice randomly selects the basis state from the set $\{[0\rangle, |1\rangle, \ldots, |N-1\rangle\}$. Each basis state selection caries $\log_2 N$ bits.
2) With probability $p < 1/2$, Alice sends the superposition state $([0\rangle + |1\rangle + \cdots + |N-1\rangle)/\sqrt{N}$.
3) In sifting procedure, Alice announces the signaling intervals in which she transmitted the superposition states. These are used to check for Eve's presence/activity. If the quantum bit-error rate (QBER) is higher than the prescribed threshold they abort protocol, otherwise, they continue with the protocol. All other signaling intervals contribute to the sifted key.
4) In information reconciliation, which is based on systematic (n, k) nonbinary low-density parity-check (LPDC) coding, Alice encodes her information symbols and sends $(n-k)$ parity symbols over an authenticated classical channel. Bob then runs the sum-product nonbinary LDPC decoding algorithm to correct the errors introduced by channel and Eve. Alternatively, binary LDPC coding can be used instead in coded modulation fashion.
5) The privacy amplification step is implemented through the use of universal hash functions G, which map the set of k-bit strings A to the set of m-bit strings B such that for any distinct $a_1, a_2 \in A$, when g is chosen uniformly at random from G, the probability of having $g(a_1) = g(a_2)$ is at most $1/|B|$. On such a way, Alice and Bob distil from corrected key a smaller set of symbols/bits whose correlation with Eve's string is below a desired threshold.

Another protocol to be described in this section is based on the MUBs derived from the complex Hadamard matrices. As an illustration, in 4-dimensional (4-D) system, assuming that MUB$_0$ is given by $\{(1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1)\}$, the another MUB can be derived from the following normalized complex Hadamard matrices, parametrized by parameter θ:

$$H_4^{(\mathrm{MUB}_1)}(\theta) = \frac{1}{\sqrt{4}} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{j\theta} & -1 & -e^{j\theta} \\ 1 & -1 & 1 & -1 \\ 1 & -e^{j\theta} & -1 & e^{j\theta} \end{bmatrix}. \tag{1}$$

The corresponding MUB$_1$ can be obtained by setting $\theta = 0$ rad in (1), to obtain MUB$_1$ = $\{0.5(1, 1, 1, 1), 0.5(1, 1, -1, -1), 0.5(1, -1, 1, -1), 0.5(1, -1, -1, 1)\}$. On the other hand,

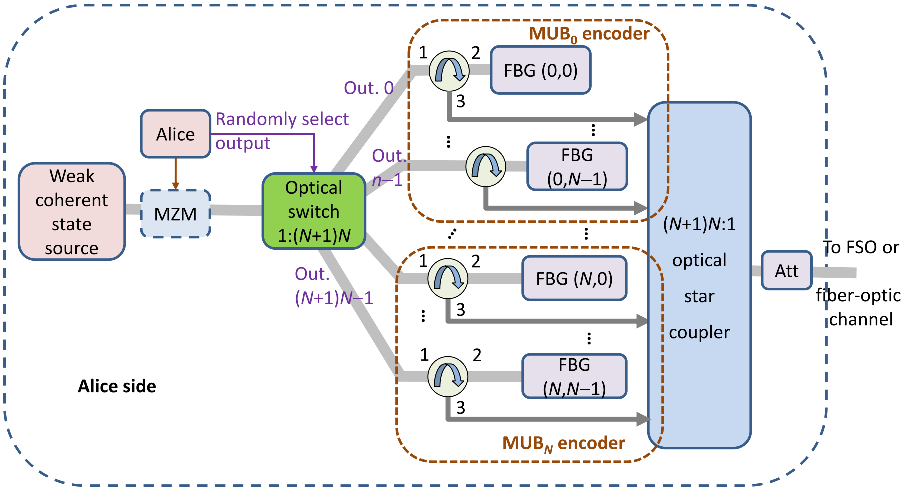


Fig. 4. Alice optical switch-based MUB-FBG encoder for weak coherent state protocols. Att: Attenuator.

the MUB$_2$ can be obtained from complex Hadamard matrix given by equation (2) below:

$$H_4^{(MUB_2)} = \frac{1}{\sqrt{4}} \begin{bmatrix} 1 & j & j & -1 \\ 1 & j & -j & 1 \\ 1 & -j & j & 1 \\ 1 & -j & -j & 1 \end{bmatrix}. \tag{2}$$

Therefore, the problem of finding a set of $N+1$ MUBs is equivalent to the problem of finding N mutually unbiased complex Hadamard matrices. Various methods to design complex Hadamard matrices are discussed in [32]. However, the number of MUBs being actually used should be reasonable, given that the probability of Alice and Bob selecting the same MUB is reversely proportional to $N+1$. Moreover, as shown in Sec. 4, the SKR improvement when the number of MUBs is increased from two to $N+1$, for the same dimensionality of QKD system, is not significant. The main improvement in N-D QKD protocols in terms of SKR, compared to 2-D protocols, comes from the increase in dimensionality of the system.

The Alice optical switch-based encoder architecture for proposed *MUB-FBG-based N-dimensional (N-D) protocol* is shown in Fig. 4. This schemes requires the use of [1:$(N+1)N$] optical switch, and $(N+1)N$ FBGs with superimposed impulse responses, such that each superimposed impulse response represents a base within the corresponding MUB. The notation FBG (m, n) is used to impose the n-th base ($n = 0, \ldots, N-1$) within the m-th MUB ($m = 0, \ldots, N$). To encode Alice just randomly selects one optical switch output out of $(N+1)N$ available outputs. On such a way, Alice randomly selects both the MUB and the base within MUB simultaneously. For MUB$_0$, the FBGs denoted with indices $(0, 0), \ldots, (0, N-1)$ are simply FBGs derived from mutually orthogonal Slepian sequences. On the other hand, the MUB$_i$, where $i \neq 0$, can be defined as:

$$MUB_i = \left\{ e^{j\phi_0^{(b)}} \,|0\rangle \otimes \cdots \otimes e^{j\phi_n^{(b)}} \,|n\rangle \otimes \cdots \otimes e^{j\phi_{N-1}^{(b)}} \,|N-1\rangle \right\}_{b=0}^{N-1}, \tag{3}$$

where we use $\otimes$ to denote the tensor product and index b to denote the base within the MUB. Clearly, the base b within MUB$_i$ is implemented by fabricating the FBG with superimposed Slepian sequences with proper phase shifts according to (3). The port 3 outputs of circulators are used as inputs to $(N+1)N$:1 optical star coupler. The attenuator at the output of star coupler is used to ensure the proper normalization.

On receiver side (see Fig. 5), Bob employs 1:$(N+1)$ optical switch to randomly select the measurement MUB, as illustrated in Fig. 5(a). Once the MUB is selected, only complex-conjugate

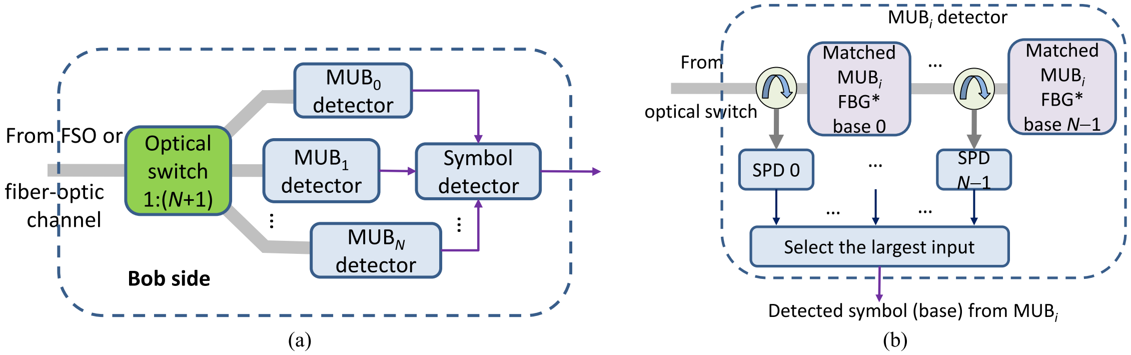


Fig. 5. Bob's decoder architecture for the proposed MUB-FBG-based weak coherent state protocols: (a) Bob's side MUB-FBG decoding scheme, and (b) the configuration of the *i*-th MUB detector. SPD: single photon detector.

matched base FBG will reflect the pulse encoded using the corresponding base FBG on Alice side, other FBGs will be transparent. The reflected pulse will trigger the SPD at corresponding port 3, as shown in Fig. 5(b). Further, select the largest input logic will determine which base within MUB was used on Alice side. After raw key transmission is completed, Alice and Bob announce the MUB being used in every signaling interval, and in sifting phase keep only the symbols at signaling intervals when both used the same MUB. In direct (reverse) information reconciliation Alice (Bob) then performs the systematic (l, k) LDPC coding, in which l–k parity bits are generated and send to Bob (Alice) over the authenticated classical channel. Bob (Alice) then performs the LDPC decoding to correct both the quantum channel and Eve's induced errors. Finally, Alice and Bob then perform the privacy amplification with the help of hash functions, to minimize the cross-correlation with Eve's channel. The simplest, yet efficient, privacy amplification hash functions are based on multiplication by a random element of the Galois field GF(2^l), while preserving the first r bits after multiplication. Algorithms based on the fast Fourier transform can be implemented in an FPGA/ASIC hardware to perform the Galois field multiplications efficiently.

Therefore, the proposed *MUB-FBG-based N-D protocol* can be summarized as follows:

1) Alice randomly selects the MUB form the set of MUBs $\{\text{MUB}_0, \ldots, \text{MUB}_N\}$, followed by random selection of the basis state from selected MUB. Alternatively, Alice randomly selects the FBG, out of $(N+1)N$ available, to be used as the basis state, with the help of an optical switch as shown in Fig. 4. Clearly, with this protocol Alice transmits $\log_2 N$ bits per signaling interval (symbol).
2) Bob randomly selects the MUB to use in the measurement, and employs the MUB detector shown in Fig. 5(b). Selected MUB and corresponding SPD click determine which symbol was transmitted.
3) In sifting procedure, Alice and Bob announce the MUBs being used. They keep only instances when both used the same MUB.
4) Alice selects a subset of symbols, to be used against Eve's presence/activity, and informs Bob about the locations. These are used to estimate the QBER. If the QBER is higher than the threshold, they abort the protocol.
5) The information reconciliation step is similar to that used in FBG-based random base selection WCS protocol.
6) The privacy amplification step is identical to the FBG-based random base selection WCS protocol.

Contrary to the t-f protocol, wherein the increase in SKR requires the reduction in bin size and therefore more expensive receiver electronics; in proposed FBG-based QKD schemes we need just to increase the number of FBGs, which are inexpensive to fabricate. Therefore, the proposed FBG-based protocols represent low-cost alternative to enable high-SKR QKD.

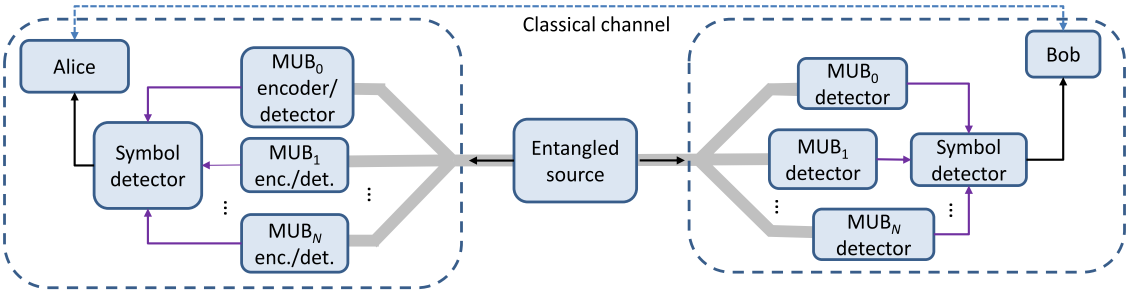


Fig. 6. FBG-based entanglement assisted MQKD system architecture.

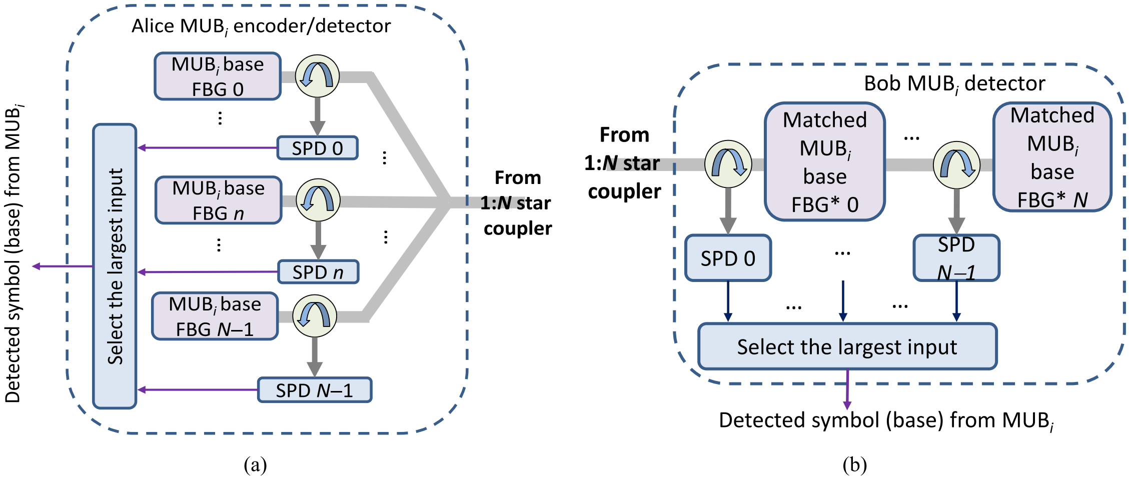


Fig. 7. Configurations of Alice and Bob's MUB encoders/detectors: (a) Alice MUB encoder/detector and (b) Bob's MUB detector.

3. Proposed FBG-Based Entanglement Assisted (EA) MQKD Protocols

In this section, we describe the proposed FBG-based entanglement assisted encoders/decoders architectures for MQKD protocols (see Figs. 6–7). In FBG-based entanglement assisted architecture, shown in Fig. 6, the entangled source generates a pair of strongly correlated photons, based on spontaneous parametric down-conversion process. For instance, for this purpose, the PPLN-based crystal can be used. Alice employs an 1:($N + 1$) optical star so that the MUB is randomly selected. The MUB encoder/detector again employs an N:1 optical star to randomly select a base within the MUB, as illustrated in Fig. 7(a). The base n within MUB is imposed by a properly fabricated FBG, with superimposed impulse response, selected according to the base n of selected MUB. The selected base within MUB is detected by the corresponding SPD and the maximum input selection logic. Therefore, our FBG-based EA MQKD protocols employ the hyper-engagement (see for instance [24] for additional details on hyper-entanglement). On receiver side, Bob employs 1: ($N + 1$) star coupler to randomly select the MUB, and once MUB is selected Bob's employs a series of complex-conjugate base FBGs to determine the base selected by Alice with the help of SPD and the maximum input selector logic, as shown in Fig. 7(b). Alice and Bob then announce the MUBs used in their measurements over the classical channel. Only the instances when both used the same MUBs are kept during the sifting phase, the other items are discarded. After that the information reconciliation and privacy amplification are performed in similar fashion as described in the previous section.

To summarize, the proposed *FBG-based entanglement assisted MQKD protocol* can be described as follows:

1) Alice's photon from the entangled pair randomly choses the output waveguide of 1:$(N+1)$ optical star coupler, and thus randomly selecting the MUB branch. Within the corresponding MUB brunch, the Alice's photon randomly selects the FBG branch, representing the base within the MUB. Clearly, the selection of MUB and corresponding base-FBG is purely random and independent of Alice. Alice by observing SPDs' outputs, by employing the largest input selection logic determines which MUB and corresponding MUB base get selected, and thus determines the symbol carrying $\log_2 N$ bits.
2) Bob's photon from the entangled pair randomly choses the waveguide from 1:$(N+1)$ optical star, and thus (similarly as for Alice side) randomly selecting the MUB branch. The Bob's MUB detector is composed of concatenation of N conjugate-FBGs corresponding to N basis within the MUB. The conjugate-FBG matched to the Alice side's imposed impulse response reflects the photon back, which gets detected by corresponding SPD on circulator port 3. Therefore, MUB branch selection and corresponding SPD click determine which symbol was transmitted.
3) In sifting procedure, Alice and announce the MUBs being used. They keep only instances when both employed the same MUB.
4) Alice selects a subset of symbols, to be used against Eve's presence/activity, and informs Bob about the locations. These are used to estimate the QBER. If the QBER is higher than the threshold, they abort the protocol.
5) Information reconciliation and privacy amplification steps, identical to those used in WCS protocols described in previous section, are then applied.

4. Security Issues

Here we are interested in the security against attacks in which the Eve's interaction is independent identically distributed (i.i.d.), and these attacks are known as the collective attacks. Practical keys are of finite length, and we need to assume the EA protocols' stages are imperfect, subject to certain failure probability [2], [3]. To deal with such scenarios, the concept of ε-security is introduced by Renner [33]. We say that the key *Key* is *ε-secure* with respect to an eavesdropper E if the trace distance between the joint state of *Key* and Eve E, denotes as $\rho_{Key,E}$, and joint state of completely mixed state (CMS) and Eve's state, denoted as $\rho_{CMS,E}$, is smaller than or equal to ε. In other words, we can write:

$$Tr\left(\rho_{Key,E},\rho_{CMS,E}\right)=\frac{1}{2}\left\|\rho_{Key,E}-\rho_{CMS,E}\right\|\leq\varepsilon. \tag{4}$$

Since each step can fail with certain probability, the security of the final key ε can be represented as a summation of securities for error correction (EC) ε_{EC}, privacy amplification (PA) ε_{PA}, and parameter estimation (PE) ε_{PE} steps; as well as the Renyi entropies estimates failure probability [33], denoted as ε_R. In other words, we can write $\varepsilon=\varepsilon_{EC}+\varepsilon_{PA}+\varepsilon_{PE}+\varepsilon_R$. Based on Renner's security theory for quantum cryptography with finite resources [33], [34], the bound for secure finite key secure rate is given by [2], [3], [34]:

$$R_K=(k/K)\max\left\{S(A|E)-S(A|B)-(1/k)ld(2/\varepsilon_{EC})-(2/k)ld(2/\varepsilon_{PA})-(2N\ +\ 3)\left[ld\left(2/\varepsilon_R\right)/k\right]^{1/2}\right\}, \tag{5}$$

where we use $S(\cdot|\cdot)$ to denote the von Neumann conditional entropy, $\mathrm{ld}(x)$ to denote $\log_2(\mathrm{x})$, while $S(A|E)$ is determined by $\mathrm{ld}(N)-I_E$, with I_E being the Eve's information. The fraction k/K represents the portion of the sequence of length $k<K$ actually used for the key, the remaining bits are used for parameters' estimation. The maximization in equation (5) is performed with respect to unknown parameters as explained in [2], [3]. To determine Eve's information we assume that the probability for Alice and Bob outcomes to differ by d mod N, when MUB i and base b within that MUB is selected, denoted by $q_{ib}(d)$, can be described L-neighbor model [3]. Namely, when FBGs are derived from Slepian sequences, different impulse responses will exhibit different number of crossing of time

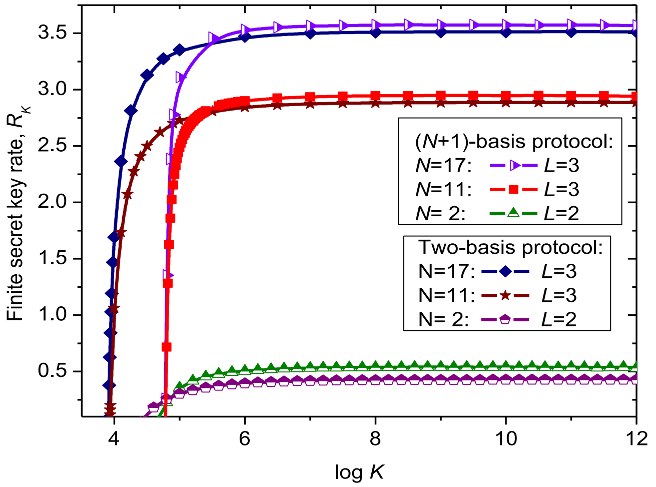


Fig. 8. Secrete finite key fraction rate R_K vs. the sequence length K for imperfectly fabricated FBGs, represented by L-neighbor model, assuming that different steps in the protocols are imperfect ($\varepsilon_{EC} = 10^{-9}, \varepsilon = 10^{-5}, 1 - q = 0.95$).

axis, indicating that a Slepian sequence with a given number of crossings can be mistaken for Slepian sequences with closet numbers of crossings.

As an illustration, the 5-neighour transition matrix for 7-dimensional system is given by:

$$\Pi = \begin{bmatrix} 1-q & q/4 & q/4 & 0 & 0 & q/4 & q/4 \\ q/4 & 1-q & q/4 & q/4 & 0 & 0 & q/4 \\ q/4 & q/4 & 1-q & q/4 & q/4 & 0 & 0 \\ 0 & q/4 & q/4 & 1-q & q/4 & q/4 & 0 \\ 0 & 0 & q/4 & q/4 & 1-q & q/4 & q/4 \\ q/4 & 0 & 0 & q/4 & q/4 & 1-q & q/4 \\ q/4 & q/4 & 0 & 0 & q/4 & q/4 & 1-q \end{bmatrix}. \tag{6}$$

In the absence of fabrication imperfections, the transition matrix will be diagonal.

Results of simulations are summarized in Fig. 8, for different dimensionalities of the FBG-based EA MQKD protocols ($N = 11$ and $N = 17$). We assume that tolerable error correction rate is $\varepsilon_{EC} = 10^{-9}$, while that the total tolerable error rate is $\varepsilon = 10^{-5}$. The parameters ε_{PA} and ε_{PE} are chosen on such a way to maximize the secret finite key fraction rate R_K, while the Renyi parameter ε_R is determined by $\varepsilon_R = \varepsilon - (\varepsilon_{EC} + \varepsilon_{PA} + \varepsilon_{PE})$. Finally, the probability for Alice and Bob outcomes to agree is set to $1 - q = 0.95$. The imperfect fabrication of FBGs, resulting in crosstalk among FBG impulse responses, is modelled by employing 3-neighbor model, in which the observed impulse response is affected by two closet neighbors (in terms of number of time-axis-crossings in impulse response). Clearly, both ($N + 1$)-base and two-base protocols for $N = 11$ and 17 significantly outperform two and three-based protocols for 2-D QKD. For sufficiently long sequences, ($N + 1$)-base protocol outperforms two-base protocol. The two-base protocol shows better robustness for insufficient sequence length K.

To study the FBG fabrication imperfections influence on SKRs, in Fig. 9 we provide SKR results for various probabilities that Alice and Bob's outcomes do not differ, $1 - q$. As expected, when impulse response of fabricated FBG differs more from target impulse response, the parameter $1 - q$ decreases, and corresponding SKRs decrease as well. This effect reduces the SKR for 2-D protocols as well. Moreover, the SKRs for 2-D protocols, for finite resources' analysis, decrease much faster with $1 - q$ probability decrease compared to N-D protocols, indicating that N-D protocols are much more tolerant to fabrication imperfections.

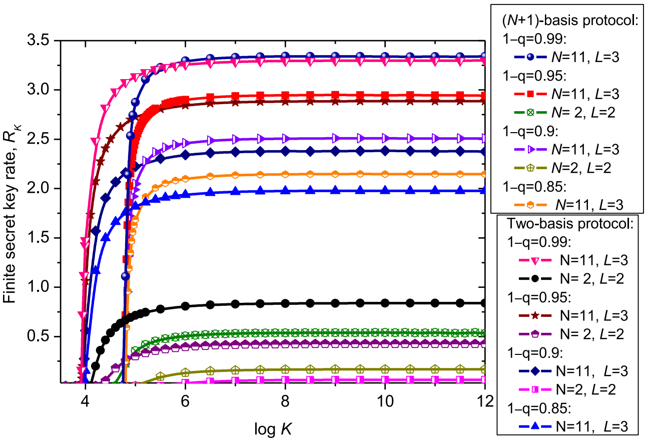


Fig. 9. Secrete finite key fraction rate R_K vs. the sequence length K for imperfectly fabricated FBGs, represented by L-neighbor model, for different $(1 - q)$ parameters; assuming that protocol steps are imperfect ($\varepsilon_{EC} = 10^{-9}$, $\varepsilon = 10^{-5}$).

On the other hand, compared to BB84 protocol, which is sensitive to PMD, polarization dependent loss (PDL), chromatic dispersion, and other propagation effects over SMF, which reduce the SKR and limit transmission distance; the FBG-based protocols are polarization insensitive, and therefore, they are not affected by PMD and PDL effects. Moreover, given the double-orthogonality principle of Slepian sequences, since Slepian sequences stay orthogonal outside of symbol duration [27], [35], Slepian-FBG-based QKD protocols are less sensitive to chromatic dispersion effects. To improve the tolerance to channel impairments and real-life imperfections in 2-D QKD protocols, the decoy state protocols have been proposed [36]. However, given the high immunity to channel impairments and imperfections of N-D systems compared to 2-D system [35], the use of decoy state protocols is not needed for sufficiently high dimensionally of the N-D QKD system.

5. Concluding Remarks

To solve for low SKR problem of 2-D QKD protocols, we have proposed several FBG-based WCS and entanglement assisted MQKD protocols. In these protocols, to increase the dimensionality of the system we need just to increase the number of FBGs, while in t-f and time-bin protocols we need to decrease the bin duration resulting in much more stringent bandwidth requirement and more expensive electronics. Someone may argue that the parallel QKD systems can be used instead of MQKD protocols. Unfortunately, in such systems the probability of photon loss, QBER, and SKR get simultaneously affected. Moreover, given that multidimensional signals have been shown to be more tolerant to channel impairments, such as turbulence effects in FSO links and fiber nonlinearities/PMD/PDL effects in SMF links [27], [35]; the proposed MQKD protocols are more tolerant to protocol imperfections compared to parallel 2-D QKD protocols. Regarding OAM-based QKD protocols, the imperfectly generated OAM modes increase the crosstalk among basis functions. Moreover, during propagation over atmospheric turbulence channel, the turbulence introduces the distortion of the wavefront increasing the crosstalk among OAM modes [37]. Therefore, OAM based QKD protocols are also inferior compared to the proposed FBG-based MQKD protocols.

Two classes of WCS protocols have been proposed, the basic random base selection protocol and MUB-based protocol. The corresponding Alice encoder and Bob's decoder MQKD configurations have been proposed as well. Regarding the entanglement assisted protocols, the generic *N*-dimensional FBG-MUB-based class of MQKD protocols has been introduced, and corresponding hardware architecture has been proposed. The MUBs for MQKD protocols have been derived from complex Hadamard matrices. The proposed low-cost FBG-based MQKD protocols can simultaneously increase the spectral efficiency and SKR for long-distance QKD applications.

References

[1] I. B. Djordjevic, *Quantum Information Processing and Quantum Error Correction: An Engineering Approach*. Boston, MA, USA: Academic, Apr. 2012.

[2] I. B. Djordjevic, “Multidimensional QKD based on combined orbital and spin angular momenta of photon,” *IEEE Photon. J.*, vol. 5, no. 6, Dec. 2013, Art. no. 7600112.

[3] I. B. Djordjevic, “Integrated optics modules based proposal for quantum information processing, teleportation, QKD, and quantum error correction employing photon angular momentum,” *IEEE Photon. J.*, vol. 8, no. 1, Feb. 2016, Art. no. 6600212.

[4] Z. Qu and I. B. Djordjevic, “Four-dimensionally multiplexed eight-state continuous-variable quantum key distribution over turbulent channels,” *IEEE Photon. J.*, vol. 9, no. 6, Dec. 2017, Art. no. 7600408.

[5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Rev. Mod. Phys.*, vol. 81, p. 1301, 2009.

[6] S. Wang *et al.*, “Practical gigahertz quantum key distribution robust against channel disturbance,” *Opt. Lett.*, vol. 43, no. 9, pp. 2030–2033, 2018.

[7] C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, “Measurement-device-independent quantum key distribution robust against environmental disturbances,” *Optica*, vol. 4, pp. 1016–1023, 2017.

[8] S. Wang *et al.*, “Field and long-term demonstration of a wide area quantum key distribution network,” *Opt. Exp.*, vol. 22, pp. 21739–21756, 2014.

[9] T. Sasaki, Y. Yamamoto, and M. Koashi M, “Practical quantum key distribution protocol without monitoring signal disturbance,” *Nature*, vol. 509, no. 7501, pp. 475–478, May 22, 2014.

[10] Z. Zhang, X. Yuan, Z. Cao, and X. Ma, “Practical round-robin differential-phase-shift quantum key distribution,” *New J. Phys.*, vol. 19, p. 033013, 2017.

[11] H. de Riedmatten, I. Marcikic, V. Scarani, W. Tittel, H. Zbinden, and N. Gisin, “Tailoring photonic entanglement in high-dimensional Hilbert spaces,” *Phys. Rev. A*, vol. 69, p. 050304, 2004.

[12] R. T. Thew, A. Acín, H. Zbinden, and N. Gisin, “Bell-type test of energy-time entangled qutrits,” *Phys. Rev. Lett.*, vol. 93, p. 010503, 2004.

[13] S. Wang *et al.*, “Proof-of-principle experimental realization of a qubit-like qudit-based quantum key distribution scheme,” *Quantum Sci. Technol.*, vol. 3, no. 2, 2018, Art. no. 025006.

[14] S. Wang *et al.*, “Experimental demonstration of a quantum key distribution without signal disturbance monitoring,” *Nature Photon.*, vol. 9, pp. 832–836, 2015.

[15] Z.-Q. Yin *et al.*, “Improved security bound for the round-robin-differential-phase-shift quantum key distribution,” *Nature Commun.*, vol. 9, 2018, Art. no. 457.

[16] M. N. O’Sullivan-Hale, I. A. Khan, R. W. Boyd, and J. C. Howell, “Pixel entanglement: Experimental realization of optically entangled $d = 3$ and $d = 6$ qudits,” *Phys. Rev. Lett.*, vol. 94, p. 220501, 2005.

[17] L. Neves, G. Lima, J. G. A. Gómez, C. H. Monken, C. Saavedra, and S. Pádua, “Generation of entangled states of qudits using twin photons,” *Phys. Rev. Lett.*, vol. 94, p. 100501, 2005.

[18] S. P.Walborn, D. S. Lemelle, M. P. Almeida, and P. H. S. Ribeiro, “Quantum key distribution with higher-order alphabets using spatially encoded qudits,” *Phys. Rev. Lett.*, vol. 96, p. 090501, 2006.

[19] A. Vaziri, G. Weihs, and A. Zeilinger, “Experimental two-photon, three-dimensional entanglement for quantum communication,” *Phys. Rev. Lett.*, vol. 89, p. 240401, 2002.

[20] N. K. Langford *et al.*, “Measuring entangled qutrits and their use for quantum bit commitment,” *Phys. Rev. Lett.*, vol. 93, p. 053601, 2004.

[21] G. Molina-Terriza, A. Vaziri, J. Reháček, Z. Hradil, and A. Zeilinger, “Triggered qutrits for quantum communication protocols,” *Phys. Rev. Lett.*, vol. 92, p. 167903, 2004.

[22] S. Groblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, “Experimental quantum cryptography with qutrits,” *New J. Phys.*, vol. 8, p. 75, 2006.

[23] M. T. Gruneosen *et al.*, “Holographic generation of complex fields with spatial light modulators: application to quantum key distribution,” *Appl. Opt.*, vol. 47, no. 4, pp. A32–A42, 2008.

[24] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, “Generation of hyperentangled photon pairs,” *Phys. Rev. Lett.*, vol. 95, p. 260501, 2005.

[25] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, “Beating the channel capacity limit for linear photonic superdense coding,” *Nature Phys.*, vol. 4, pp. 282–286, 2008.

[26] N. T. Islam, C.C.W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, “Provably secure and high-rate quantum key distribution with time-bin qudits,” *Sci. Adv.*, vol. 3, p. e1701491, 2017.

[27] I. B. Djordjevic, *Advanced Optical and Wireless Communications Systems*. Basel Switzerland: Springer International Publishing, Dec. 2017.

[28] D. Slepian, “Prolate spheroidal wave functions, Fourier analysis and uncertainty V: The discrete case,” *Bell Syst. Tech. J.*, vol. 57, no. 5, pp. 1373–1381, 1978.

[29] I. B. Djordjevic, A. H. Saleh, and F. Küppers, “Design of DPSS based fiber Bragg gratings and their application in all-optical encryption, OCDMA, optical steganography, and orthogonal-division multiplexing,” *Opt. Exp.*, vol. 22, no. 9, pp. 10882–10897, May 5, 2014.

[30] I. B. Djordjevic, S. Zhang, and T. Wang, “Optically encrypted multidimensional coded modulation for multi-Pb/s optical transport,” in *Proc. IEEE Photon. Conf.*, 2016, pp. 57—58, Paper MB3.6.

[31] L. Dong and S. Fortier, “Formulation of time-domain algorithm for fiber Bragg grating simulation and reconstruction,” *IEEE J. Quantum Electron.*, vol. 40, no. 8, pp. 1087–1098, Aug. 2004.

[32] W. Tadej and K. Zyczkowski, “A concise guide to complex Hadamard matrices,” *Open Syst. Inf. Dyn.*, vol. 13, pp. 133–177, 2006.

[33] R. Renner, “Security of quantum key distribution,” Ph.D. dissertation, Dept. Comput. Sci., Swiss Fed. Inst. Technol., Zurich, Switzerland, Sep. 2005.

[34] V. Scarani and R. Renner, “Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing,” *Phys. Rev. Lett.*, vol. 100, no. 20, May 22, 2008, Art. no. 200501.

[35] I. B. Djordjevic, “On advanced FEC and coded modulation for ultra-high-speed optical transmission,” *IEEE Commun. Surv. Tuts.*, vol. 18, no. 3, pp. 1920–1951, Aug. 19, 2016.

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

[37] I. B. Djordjevic and Z. Qu, “Coded orbital angular momentum modulation and multiplexing enabling ultra-high-speed free-space optical transmission,” in *Optical Wireless Communications—An Emerging Technology*, M. Uysal *et al.*, Eds. New York, NY, USA: Springer, 2016, pp. 363–385.