Proposal for Slepian-States-based DV- and CV-QKD Schemes Suitable for Implementation in Integrated Photonics Platforms

Ivan B. Djordjevic

University of Arizona, Department of Electrical and Computer Engineering, 1230 E. Speedway Blvd., Tucson, AZ 85721, USA

Manuscript received June 13, 2019. The paper was supported in part by MURI ONR project N00014-13-1-0627 and by NSF.

Abstract: QKD leverages underlying principles of quantum mechanics to realize distribution of keys with verifiable security. Despite appealing features of QKD, there are some fundamental and technical challenges that need to be solved prior to its widespread applications. Firstly, QKD secret-key rate (SKR) is fundamentally limited by channel loss, as dictated by the rate-loss tradeoff. Quantum repeaters would be an ultimate solution to overcome this problem; however, they are well beyond the reach. The second challenge lies in the scalability and cost. Future's QKD systems must be suitable for mass production with low-cost, reliable realignment-free operations, and small power consumption. To solve for these problems in a simultaneous manner, we propose to encode information in the orthogonal Slepian sequences' bases. Such an approach is highly robust against turbulence effects in free-space optical links and dispersion effects/fiber nonlinearities in fiber-optics channels, thereby improving QKD distance. Moreover, exploiting multidimensional encoding space enables high spectral efficiency QKD so that the SKR can be significantly improved. Critically, generation, processing, and detection of Slepian-states can be reliably implemented in an integrated quantum photonics platform, based on both reflective and transmissive waveguide Bragg gratings (WBGs). Proposed reflective/transmissive-WBG-based Slepian-states are applicable to both discrete variable (DV)- and continuous variable (CV)-QKD systems.

Index Terms: Quantum key distribution (QKD), Slepian-states, integrated optics, waveguide Bragg gratings.

1. Introduction

The first quantum key distribution (QKD) scheme was introduced by Bennett and Brassard, who proposed it in 1984 [1],[2], and it is now known as the BB84 protocol. The QKD enables two pre-authenticated parties Alice and Bob, connected by an optical (quantum) link, to generate quantum information-theoretically secure shared secret key. The security of QKD is guaranteed by the quantum mechanics laws. Different photon degrees of freedom, such as polarization, time, frequency, phase, and orbital angular momentum can be employed to implement various QKD protocols. Generally speaking, there are two generic QKD schemes, discrete variable (DV)-QKD and continuous variable (CV)-QKD, depending on strategy applied on Bob's side. In DV-QKD schemes, a single photon detector (SPD) is applied on Bob's side, while in CV-QKD the field quadratures are measured with the help of homodyne/heterodyne detection. The DV-QKD scheme achieves the unconditional security by employing no-cloning theorem and theorem on indistinguishability of arbitrary quantum states. Namely, when Eve interacts with the transmitted quantum states, trying to get information on transmitted bits, she will inadvertently disturb the fidelity of the quantum states that will be detected by Bob. On the other hand, the CV-QKD employs the uncertainty principle claiming that both in-phase and quadrature components of the coherent states cannot be simultaneously measured with the complete precision. We can also classify different QKD schemes as either entanglement assisted (EA) or prepare-and-measure (PM) types.

The research in QKD is getting momentum, in particular after the first satellite-to-ground QKD demonstration [3]. Recently, the QKD over 404 km of ultralow-loss optical fiber is demonstrated; however, with ultralow secret-key rate (SKR) (of $3.2 \cdot 10^{-4}$ b/s) [4]. Given that quantum states cannot be amplified, the fiber attenuation limits the distance. On the other hand, the deadtime (the time over which an SPD remains unresponsive to incoming photons due to long recovery time) of the SPDs, typically in 10-1000 ns range, limits the baud rate and therefore the secure key rate. The CV-QKD schemes, since they employ the homodyne/heterodyne detection, do not exhibit the deadtime limitation problem, however, the typical achievable distances are shorter.

Quantum repeaters would represent an ultimate solution to overcome the channel loss, but they are well beyond the reach of today's available technologies. A near-term solution would to encode quantum information into a Hilbert space with a dimension higher than the mainstream two-dimensional encoding using, e.g., polarization states of photons. A multidimensional (MD) encoding space ensures that random number bits can be delivered upon receiving each single photon, thereby optimizing the photon efficiency for high-rate QKD in the absence of quantum repeaters [5]. Several approaches have recently been pursued to increase the dimension of the encoding space of single photons. These approaches either leverage MD parameters such as time bin, frequency qubits [6], position and linear momentum [7], orbital angular momentum (OAM) [8],[9], or simultaneously utilizing multiple parameters encoded in hyper-entangled states [10]. Unfortunately, OAM modes suffer from phase front distortion [11] and are incompatible with long-haul communications in single-mode fibers. The MD time-bin-encoded QKD can be seamlessly incorporated into standard telecom networks, as experimentally demonstrated in [12], but the time-bin encoding largely sacrifices the spectral efficiency. Indeed, MD time-bin-encoded QKD only enjoys an advantage over two-dimensional protocols in scenarios with either a photon-budget constraint at the source or detector deadtime-limited performance. The second challenge lies in the scalability and cost of QKD. Like the prevailing classical communication systems, future QKD systems must provide mass productivity with low cost, reliable realignment-free operations, and small power consumptions. In this regard, photonic integrated circuits (PICs) would be a promising platform for miniaturized QKD systems, but they do not naturally accommodate the widely used qubits. Specifically, PICs are less effective in processing polarization-encoded information. In addition, the required long integrated delay line at the transmitters and the receivers for time-bin-encoded QKD schemes significantly increase the footprint of PICs for QKD and therefore limit the scalability of such an approach.

In this paper, we formulate a new framework to enable long-haul, high-rate, robust, and scalable QKD systems with MD qubits encoded in the orthogonal Slepian sequences' bases. As shown in [13],[14] for a given signal bandwidth and symbol duration, Slepian functions represent the maximum possible number of real-valued orthogonal waveforms, and as such they are excellent candidates to be used in multidimensional signaling. Similarly to classical MD optical communications [15],[16], such an approach is highly robust against turbulence effects in free-space optical (FSO) links [16] and dispersion effects/fiber nonlinearities [15] in fiber-optics channels when either standard single-mode fibers (SMFs) or nonzero-dispersion shifted-fibers (NZ-DSFs) are used in twin-field configuration [17],[18], thereby improving the QKD distance. As an illustration, as shown in [16] the MD communications exhibit better tolerance to turbulence effects in FSO channels and fading effects in wireless channels. Moreover, exploring the MD encoding space enables high spectral efficiency QKD so that the communication SKRs can be substantially improved. Critically, the generation, processing, and detection of Slepian states can be reliably implemented in an integrated quantum photonics platform, based on proposed electronically controlled (EC) reflective/transmissive waveguide Bragg gratings (WBGs). The proposed reflective/transmissive-WBG-based Slepian-states are applicable to both discrete variable (DV)- and continuous variable (CV)-QKD schemes. To summarize, by employing the Slepian states-based QKD both the SKRs can be improved and transmission distance extended. Moreover, the Slepian states-based QKD represents a scalable solution suitable for implementation in PIC platforms. Finally, as it will be shown in numerical results' section, the Slepian states-based MD QKD exhibits a better tolerance to channel impairments' induced errors.

The paper is organized in five sections. After introductory section, in Section 2 Slepian-states-based DV-QKD protocols are described, employing both transmissive and reflective WBGs. Both PM and EA MD QKD schemes are described. Corresponding CV-QKD schemes suitable for implementation in integrated optics are described in Section 3. Some illustrative numerical SKR results are provided in Section 4. Finally, Section 5 provides some relevant concluding remarks.

2. Slepian-states-based DV-QKD Protocols Suitable for Implementation in Integrated Photonics Platforms

To address the key challenges described above, we propose take a reconciled approach to develop new MD protocols and tailored efficient PICs to substantially advance scalable, high-rate, and long-haul QKD systems, as illustrated in Fig. 1, for the weak coherent states-based scenario. By employing the proposed EC-WBGs, to be implemented in nonlinear PICs, we can develop the quantum transmitters and receivers for MD-QKD schemes and beyond. Compared to fiber Bragg gratings (FBGs) proposed in our recent publication [11], EC-WBGs can be mass fabricated in a PIC platform, in lieu of the liquid crystal platform [19], so that quantum information encoded in a large number of mutually unbiased bases (MUBs) can be processed. As such, the scalability is significantly improved while substantially reducing the cost.

Time-bin encoding is an appealing mean for implementing MD-QKD with telecom compatible components, as demonstrated in [12], where a ~ 4 Mbit/s SKR was achieved, in a back-to-back configuration. However, as illustrated in Fig. 2(*left*), an *N*-dimensional either time-bin encoding scheme or time-phase encoding scheme [12] requires *N* time slots with only one time bin, on average, being occupied by a photon, but the rest time slots are left vacuum. Due to the *N*–1 vacuum slots, time-bin-encoded MD-QKD suffers from low spectral efficiency. In fact, the required optical bandwidth is proportional to *N*, as illustrated in Fig. 2(*left*). To tackle the limitation of time-bin encoding we proposed recently introducing orthogonal Slepian sequence states [11],[13], as illustrated in Fig. 2(*right*). In Slepian-encoded MD-quantum state, *every time slot* is encoded with a single-photon level signal. The temporal-spectral profile, described by a state in the Slepian sequence, represents the encoded MD quantum information. Note that different Slepian states are orthogonal so that a Slepian sequence with *N* elements can be used as an encoding basis. Akin to the two-dimensional encoding space, a superposition of Slepian states can form a Slepian state in a conjugate encoding basis. In classical orthogonal frequency division multiplexing (OFDM), orthogonal subcarriers improve the spectral efficiency and reduce inter-symbol interference (ISI) and inter-channel interference. Likewise, MD-quantum communication based on Slepian states is also anticipated to enjoy high spectral efficiency and low crosstalk between multiplexed quantum channels. As illustrated in Fig. 2(*right*), the consumed optical bandwidth (1/*T*) is independent of the system dimensionality *N*. However, the bandwidth required in time-frequency QKD system is proportional to $1/\tau=N/T$.

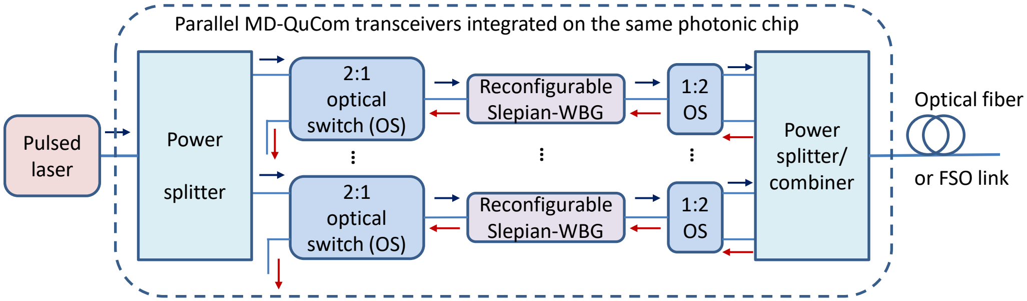


Fig. 1 Illustration of parallel MD-quantum communication (QuCom) transceiver integrated on the same quantum photonic chip. Arrow → (←) denotes the transmitting (receiving) direction.

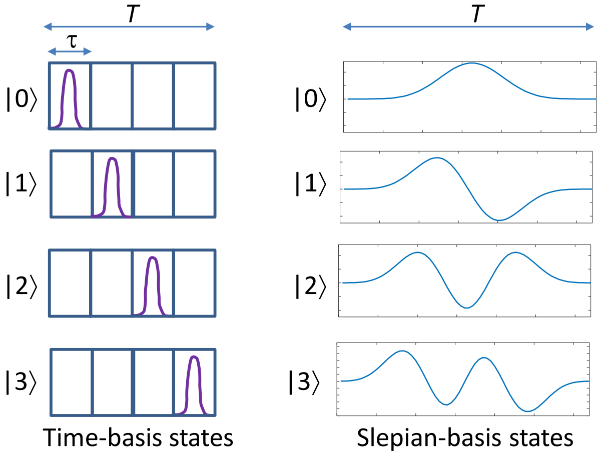
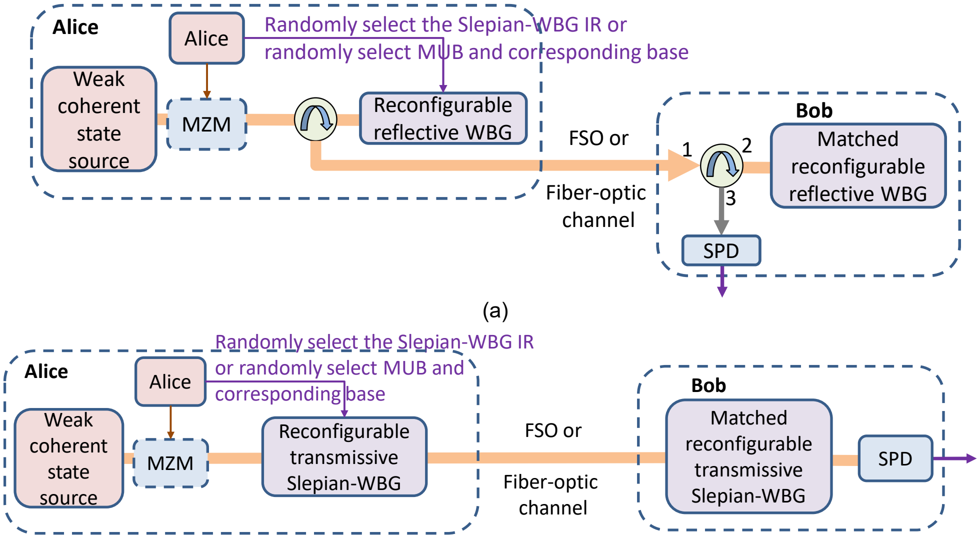


Fig. 2 (Left) Time-basis in 4-D t.f. QKD (*T*: symbol duration, τ: bin duration, $\tau=T/4$). (Right) Slepian- states in 4-D MD-QKD.

Let us first outline the protocol designs for *MD-DV-QKD based on reflective Slepian-WBGs*, which does not require the use of entangled states. In basic WBG-based *random base selection PM protocol*, we employ Slepian-WBGs with mutually orthogonal impulse responses (IRs), denoted as {[0⟩, |1⟩, …, |*N*-1⟩} as the encoding basis for MD-QKD, as illustrated in Fig. 3(a). The Alice encoder is composed of an adaptive, reconfigurable Slepian-WBG implemented in PIC technology and a circulator, with the Mach-Zehnder modulator (MZM) being optional, which is used to perform NRZ to RZ conversion. When the weak coherent state (WCS) source is based on a pulsed laser, the MZM is not required. To encode Alice randomly selects the orthogonal IR to be used, and a genetic algorithm (GA) is used to determine the voltages to be applied on electrodes of WBG-devise shown in Fig. 4 to reconfigure to the desired basis function $|n\rangle$. The surface-profile diffraction grating is used as one of substrates. By filling the grating groves with the dielectric, controlled by electrodes on another substrate, the waveguide is created as explained in [19]. The m-th electrode (m=1,2,..,M) together with grating waveguide below it serves as the m-th segment with refractive index $n(m)$. By properly changing the control voltages, we can tune the overall impulse response to the desired Slepian sequence. In the absence of control voltages, the default grating will represent the central Slepian sequence from the set of Slepian sequences being employed. To speed-up the reconfiguration process, the GA should be run in installation stage only to determine the set of voltages required for each basis function, with corresponding results being stored in a look-up-table (LUT). We propose to employ either aluminum nitride (AlN)- or lithium niobate (LN)-based platform to implement the proposed Slepian-sates-based MD-QKD protocols. Both AlN and LN can be integrated with silicon (Si) platforms [20],[21] and as such are suitable for large-scale integration. With N mutually orthogonal impulse responses imposed on WBGs, Alice can transmit $\log_2 N$ bits per signaling interval. To probe for Eve's presence Alice reconfigures the WBG to generate the superposition state $([0\rangle+|1\rangle+ \ldots + |N\text{-}1\rangle)/\sqrt{N}$. To upgrade system to higher dimensionality we will need to re-run the GA to determine the set of voltages required, and this can be done in initialization stage. Moreover, it is possible to determine the required voltages for different system dimensionalities and store the results for the GA in the LUT. In this case, in operation stage, the system upgrade will mean just reading out data related to voltages at a different address in the LUT.

Given that optical circulators are difficult to implement in integrated optics, we propose to employ the *transmissive Slepian-WBGs* instead, with corresponding scheme being provided in Fig. 3(b). The transmissive FBGs have been already studied for use in picosecond optical signal processing [22], and we believe that fabrication of transmissive WBGs to generate Slepian-states will be possible too.


Alice
Alice
Randomly select the Slepian-WBG IR or
randomly select MUB and corresponding base
Weak coherent state source
MZM
Reconfigurable reflective WBG
FSO or
Fiber-optic channel
Bob
1
2
3
Matched reconfigurable reflective WBG
SPD
Alice
Alice
Randomly select the Slepian-WBG IR
or randomly select MUB and
corresponding base
Weak coherent state source
MZM
Reconfigurable transmissive Slepian-WBG
FSO or
Fiber-optic channel
Bob
Matched reconfigurable transmissive Slepian-WBG
SPD

(a)

(b)

Fig. 3 The reconfigurable Slepian-WBG-based schemes implementing either the random base selection PM protocol or MUB-based protocol for DV-QKD applications based on: (a) reflective Slepian-WBGs and (b) transmissive Slepian-WBGs.

On receiver side, Bob employs another reconfigurable matched transmissive Slepian-WBG, as shown in Fig. 3(b). The non-matched-transmissive-Slepian-WBG reflects the pulse back, while the matched-transmissive-WBG passes the signal and the single-photon detector (SPD) detects the presence of pulse, and Bob is able to identify the transmitted symbol, when Alice used the same basis state $|n\rangle$. Other configurations employing the same concept are also possible. To improve the SKR, we need to employ more advanced protocols. Unfortunately, for advanced protocols the use of circulators in Bob's detector is required, as illustrated in Fig. 5, which is composed of N reflective-WBGs. (Only, the basic random base selection PM protocol does not require the use of circulators.) Bob employs a series of matched reflective-WBGs. The matched reflective-WBG reflects the pulse back, and the corresponding SPD at port 3 of circulator will able to detect the presence of a pulse. Only one SPD will detect the presence of the pulse unless when the signaling interval is used for quantum bit-error rate (QBER) estimation. 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 QBER is lower than the prescribed threshold-QBER-value they continue with the protocol, otherwise, they abort the protocol. Other signaling intervals that are not used for QBER estimations are used for the sifted key. After that, the classical postprocessing steps are applied. The corresponding transmissive WBGs-based scheme will require the employment of the circulators as well.

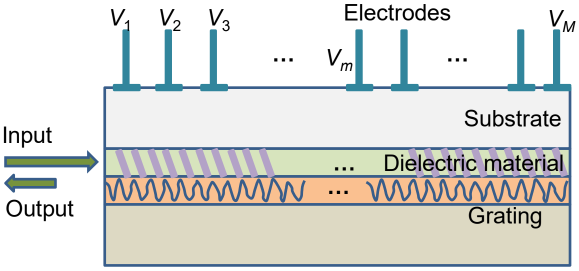


Fig. 4 Implementation of reflective Slepian-WBG (modified from [19]).

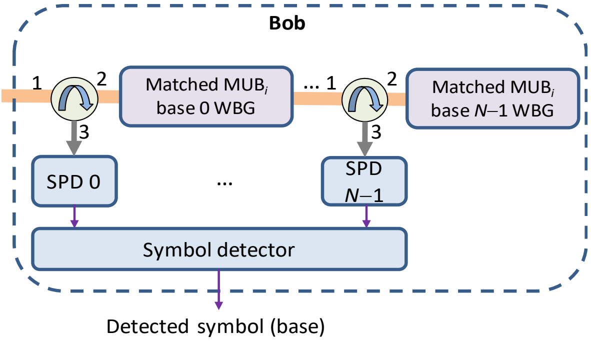


Fig. 5 Bob's reconfigurable reflective Slepian-WBGs-based detector to be used instead of Bob's receiver shown in Fig. 3(a) or as the-i-th MUB detector (for DV-QKD).

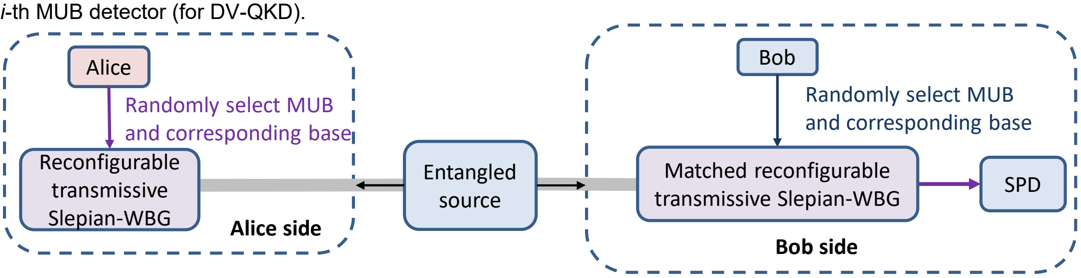

Alice
Randomly select MUB and corresponding base
Reconfigurable transmissive Slepian-WBG
Alice side
Entangled source
Bob
Randomly select MUB and corresponding base
Matched reconfigurable transmissive Slepian-WBG
SPD
Bob side

Fig. 6 The proposed scheme for reconfigurable transmissive-WBG-MUB-based entanglement assisted DV-QKD protocol.

Another protocol described in this section is based on the properly selected MUBs. As an illustration, in 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 selected as 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)}, derived from the theory of the complex Hadamard matrices [11],[23]. To implement this DV-QKD protocol, the reflective-WBG-schemes shown in Figs. 3(a) and 5 are applicable. Namely, Alice first randomly selects which MUB to use following by the random selection of the base within the MUB, and after that she adjusts the voltages to impose the needed superposition state. In initialization stage, the GA has been run to determine the voltages needed to select each base within a given MUB, and the corresponding results are stored in LUT. In operation stage, selected MUB and its corresponding base are used to determine the address in LUT where the voltages' values are stored, which are further used to reconfigure the WBG to the required superposition state. Given that the reconfiguration process is electro-optical, it can be done in order of ns. On receiver side, Bob randomly selects the measurement MUB to be used and reconfigures the corresponding matched WBGs shown in Fig. 5 to match the states that corresponds to the MUB. The matched base WBG will reflect the pulse encoded using the corresponding base WBG on Alice's side, while other WBGs are transparent. The reflected pulse will trigger the SPD at corresponding port 3 (see Fig. 5). The SPD detecting the pulse will determine the base used by Alice for the same MUB. A special case with two MUBs represents a generalization of the time-bin-encoded protocol. However, in Slepian-states-encoded protocol, the increase in the dimension does not increase the overall required bandwidth, as shown in Fig. 2(*right*). In the time-bin-encoded protocol, on the other hand, the increase in dimensionality means that more narrow time-bins are required, which increases the bandwidth and reduces the spectral efficiency. In fully MD-QKD protocols, the SKR is a logarithmic function of the system dimensionality. To improve further the SKR, we propose to employ the parallel MD-QKD protocols, in which several MD-QKD schemes are operated independently and in parallel, in similar fashion as shown in Fig. 1.

Now we describe WBG-based *EA MD-QKD protocols*, with proposed corresponding scheme being provided in Fig. 6. The entangled source generates a pair of strongly correlated photons, employing the spontaneous parametric down-conversion process based on the integrated customized nonlinear waveguides. Alice randomly selects the MUB and the corresponding base within MUB to be imposed by reconfiguring the WBG as described above. On the other hand, Bob randomly selects the MUB and corresponding base to be used in the measurement on his qubit, by properly adjusting the voltages for matched transmissive-WBG-operation. When Bob selected the same MUB and the same base within MUB the corresponding photon pulse will be passed through the matched transmissive Slepian-WBG and be detected by an SPD. For non-matched case, the WBG will reflect the pulse back, and the pulse will not be detected. To improve SKR Bob's receiver can be replaced by corresponding reflective-WBGs-based receiver provided in Fig. 5; however, this scheme requires the employment of circulators.

3. Multidimensional Slepian-states-based CV-QKD Suitable for Implementation in Integrated Photonics Platforms

Regarding the *MD-CV-QKD protocols*, there are two options. The first option is to employ Slepian-states as a new degree of freedom to implement parallel CV-QKD schemes, which is illustrated in Fig. 7, for the discrete modulation CV-QKD case. (Only the details to the single polarization state and single wavelength are shown to facilitate the explanations.) In this case we multiplex *K* independent conventional 2-D CV-QKD schemes. The second option would be to employ Slepian functions in both electrical and optical domains, in similar fashion as it was done in classical MD optical communications [14]. In this case, we need 2*L* Slepian sequences in electrical domain, *L* per each quadrature channel and the system dimensionality increases to 2*LK*. The corresponding 2-D I/Q modulators in Fig. 7 need to be replaced by 2*L*-dimensional modulators. On receiver side, we would need additional 2*L*-dimensional demodulators, after coherent detection takes place. To simplify explanations, let us now provide additional details of the first scheme only. On Alice side, the laser beam signal is split with the help of 1:*K* star coupler into *K* beams that are used as input of corresponding I/Q modulators. The RF inputs represent *K* parallel RF-assisted M-ary PSK (M-PSK)/quadrature amplitude modulation (QAM) signals, generated with the help of arbitrary waveform generators (AWGs) or digital-to-analog converters (DACs), which are then imposed on different transmissive WBGs with orthogonal impulse responses derived from Slepian sequences. For the RF assisted CV-QKD details, an interested reader is referred to Fig. 8 below. On receiver side, Bob employs 1:*K* star coupler to split the received signal, and in each branch the projection along the matched Slepian basis function is obtained with the help of the matched transmissive WBG filter. So, the outputs of matched transmissive WBGs represent *K* demultiplexed signals. The *k*-th (*k*=1,2,…,*K*) matched WBG output signal undergoes the heterodyne detection, and in the phase noise cancellation (PNC) stage the laser phase noise component and frequency offset get cancelled. Following the down-conversation process in each branch, the resulting baseband signals represented detected (I,Q) signals corresponding to different Slepian-states. Then the classical postprocessing has been applied on the whole raw key, while the corresponding SKR can be calculated as:

$$SKR = R_{\mathrm{raw}}\left[1-\mathrm{leakage}_{\mathrm{ECC}}\left(q\right)\right]-\sum\nolimits_{k} R_{\mathrm{raw}}^{(k)} I_{E}^{(k)},\; R_{\mathrm{raw}} = \sum\nolimits_{k} R_{\mathrm{raw}}^{(k)}, \tag{1}$$

where $I_{E}^{(k)}$ is the mutual information Eve was able to acquire related to the *k*-th Slepian basis function, and $R_{\mathrm{raw}}^{(k)}$ is the raw data rate between Alice and Bob related to the *k*-th Slepian-state. We use leakage$_{\mathrm{ECC}}$(q) to denote the leakage of information due to error correction coding (ECC) under assumption that overall quantum BER was q.

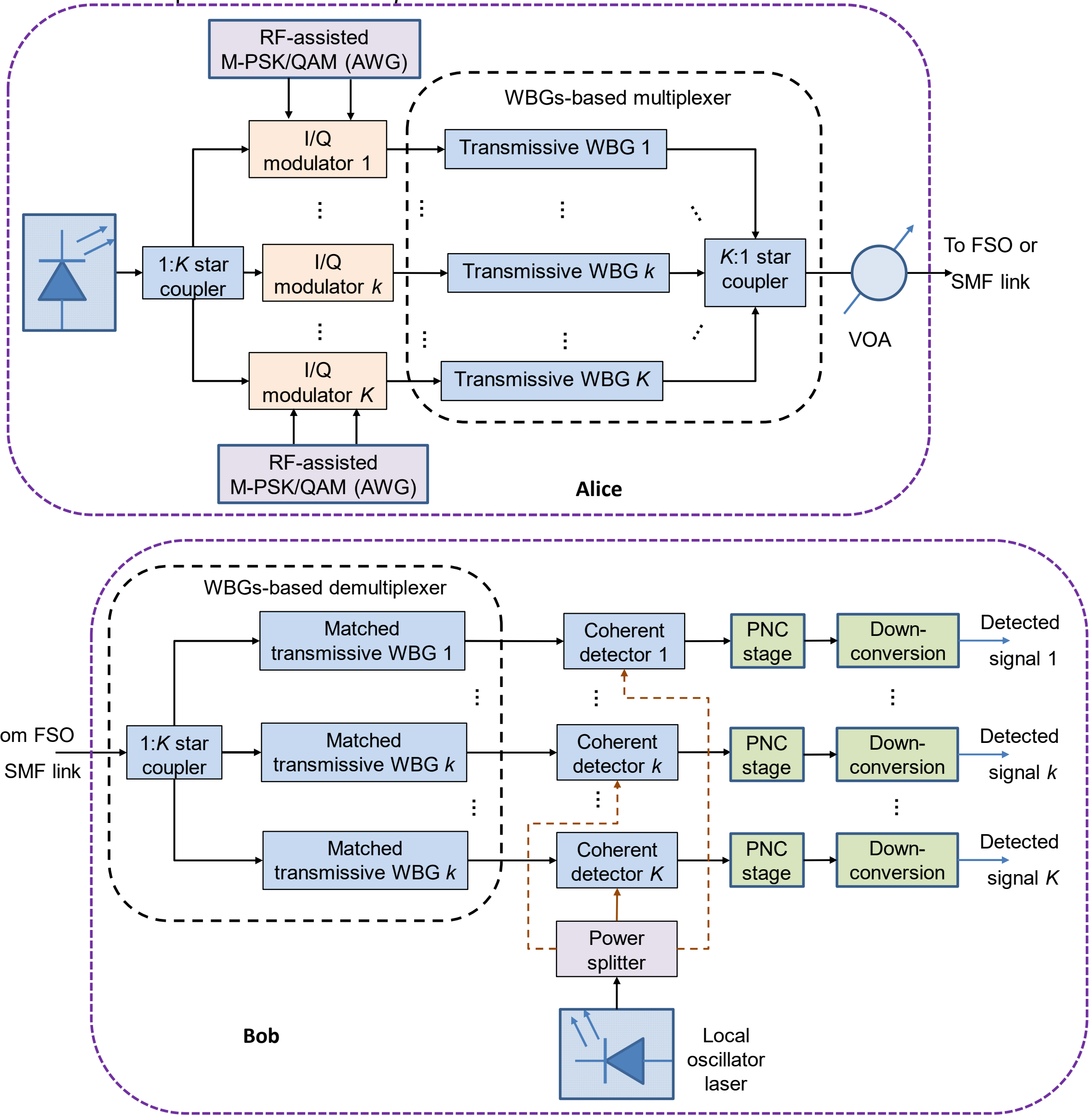


Fig. 7 Proposed scheme for parallel WBGs-based RF-assisted CV-QKD protocol: (top) Alice's transmitter and (bottom) Bob's receiver.

For completeness of presentation, we describe the generalized RF-assisted CV-QKD applicable to any two-dimensional signal constellation, including M-PSK and QAM signals. Moreover, in [24],[25] M-PSK scheme was described only. To facilitate explanations, only the details related to the signal polarization state and single Slepian-state are shown. On Alice side, the discrete modulated (M-PSK/QAM) signals, are first imposed on the RF subcarrier and are then converted to optical domain with the help of an optical I/Q modulator and sent to Bob over either fiber-optics or free-space optical (FSO) link. On receiver side, Bob employs the heterodyne coherent detector together with a PNC stage to control the level of excess noise. The PNC stage first squares the reconstructed in-phase and quadrature signals and after that either adds or subtracts them depending on the optical hybrid type. The PNC stage further performs bandpass filtering to remove DC component and double-frequency term, followed by the down-conversion, implemented with the help of multipliers and low-pass filters (LPFs). Given that PNC stage cancels the phase noise and frequency offset fluctuations, it exhibits better tolerance to the excess noise compared to traditional CV-QKD schemes.

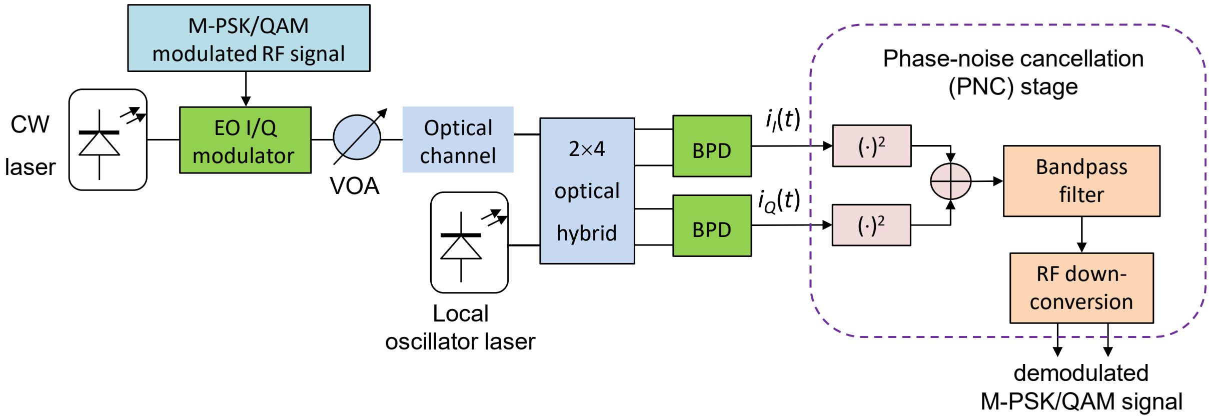


Fig. 8 Generalized RF-assisted CV-QKD scheme applicable to both M-ary PSK and QAM signals (only details related to single polarization state and single Slepian-state are shown). VOA: variable optical attenuator, BPD: balanced photodetector.

4. Illustrative Secret-Key Rates Results

To illustrate high potential of the proposed Slepian-sates-based QKD protocols, in Figs. 9 and 10 we provide the SKR results per single Slepian-state and single wavelength for both DV- and CV-QKD protocols for different SMF distances. We assume that both DV- and CV-QKD schemes employ full parallelization to maximize the SKRs. In simulations, we assume that recently fabricated ultra-low-loss fiber with attenuation coefficient of 0.1419 dB/km at 1560 nm is used [26]. For DV-QKD protocols, see Fig. 9, we assume that detector efficiency of η=0.2, the visibility of V=0.99, the dark counts' probability of p_d=10^{-6}, the dead time τ_d is set to 10 ns, while the mean photon number is chosen to be the optimum (maximizing the SKR).

Regarding the CV-QKD protocols, we assume that heterodyne detection is used for both Gaussian modulation (GM) and discrete modulation (DM) and RF-assisted discrete modulation with 8-states as described in [25]. In Fig. 9(a), we perform comparison for the same reconciliation efficiency of β=0.9. We further assumed that Alice employs collective attack, and that detector efficiency is 0.9. The baud rate for CV-QKD is set to 10 GBd, while RF subcarrier for DM is set to 10 GHz. The excess noise ε and the electrical noise v_{el} variances (expressed in shot noise units) are used as parameters. For distance of 200 km, when the decoy state protocol is employed, we can achieve SKR of 2.09 kb/s (per single Slepian-state and single wavelength). By employing 10 Slepian-states and 10 wavelengths, we can achieve total SKR of 0.209 Mb/s. On the other hand, by employing GM (for ε=10^{-3} and v_{el}=10^{-2}) for the same distance we can achieve 3.6 Mb/s per single Slepian-state and single wavelength. By employing both polarization states, 10 Slepian-sates, and 10 wavelength channels the total SKR of 720 Mb/s is achievable, which would represent the record SKR for distance of 200 km. Unfortunately, such high reconciliation efficiency with GM is rather difficult to achieve with practical error correction schemes [27]. One of the key advantages of DM over GM is in availability of high reconciliation efficiency schemes, in particular those ones based on LDPC coding [28]. Namely, the reconciliation efficiency for DM schemes β_{DM} is much higher than reconciliation efficiency for GM protocols β_{GM}, in other words β_{DM}>>β_{GM} [29]. Another interesting observation comes from the information theory, where we learned that in very low signal-to-noise ratio (SNR) regime the Shannon's channel capacity can be achieved with small signal constellation sizes [28]-[30]. Given that QKD schemes typically operate in low SNR regime, DM protocols can outperform corresponding GM protocols thanks to much better reconciliation efficiency, as illustrated in Fig. 10(b). Moreover, by employing the RF-assisted CV-QKD scheme proposed in [24],[25], which is insensitive to the laser phase noise and frequency offset, the DM protocols with much lower excess noise can be employed, thus further outperforming GM protocols of bad reconciliation efficiency. In Fig. 10(b) we provide SKR vs. transmission distance for both DM and GM protocols assuming typical practical reconciliation efficiencies. The electrical noise variance is set to v_{el}=0.01, detector efficiency is η=0.85, and excess noise variance is set to ε=10^{-3}. Evidently, the DM protocols outperform the GM protocols for typical reconciliation efficiency values, in terms of SKR vs. distance dependence.

With DM protocol, the SKR of 1 Mb/s is achievable for distance of 197 km. By employing 10 Slepian-states, two polarization states, and 10 wavelengths we can achieve the SKR of 200 Mb/s by employing the DM-based CV-QKD, with practical reconciliation efficiency.

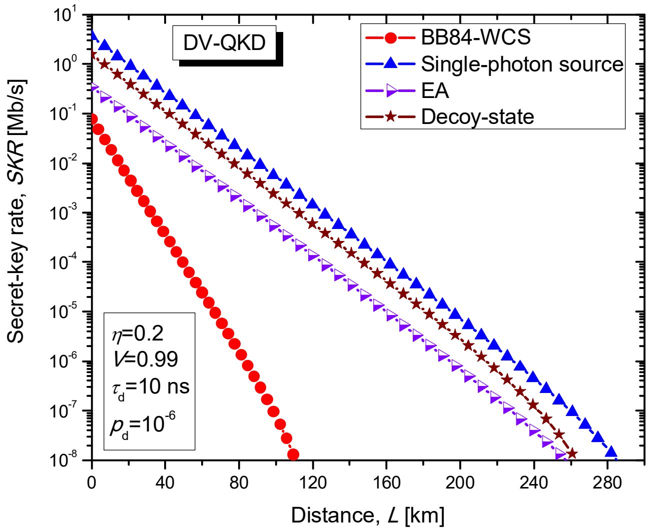
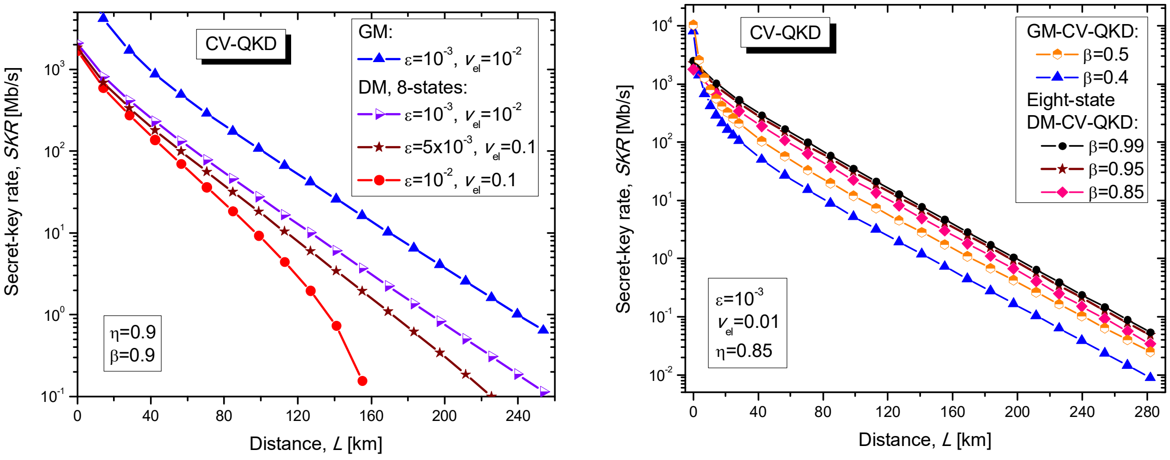


Fig. 9 DV-QKD secret-key rates per single wavelength and single Slepian-sate vs. distance.



(a)

(b)

Fig. 10 CV-QKD SKRs per single wavelength and single Slepian-sate vs. distance: (a) DM vs. GM for the same reconciliation efficiency and (b) for typical reconciliation efficiencies.

To demonstrate better tolerance to channel impairments of proposed MD-DV-QKD against that of 2-D protocols, in Fig. 11 we provide the secrecy fraction (normalized SKR) plots for different QKD dimensionalities by employing the generalized depolarization model. In this model, the probability that Alice and Bob outcomes differ by $n \in \{0,1,\ldots,N-1\}$, denoted as $q_{AB}(n)$ is determined by:

$$q_{AB}(n) = \begin{cases} 1-q, & n=0 \\ q/(N-1), & n \neq 0 \end{cases}. \tag{2}$$

Clearly, this model is a generalization of classical N-ary symmetric channel model, and parameter q denotes the probability that Alice and Bob outcomes are different. This parameter is easy to measure in both FSO and fiber-optics links. From Fig. 11, we can conclude that the proposed MD QKD protocols are much more robust to both channel and Eve's introduced errors compared to two-basis and three-basis 2-D protocols. Further, we conclude that (N+1)-basis protocols are more robust compared to two-basis protocols for the same system dimensionality.

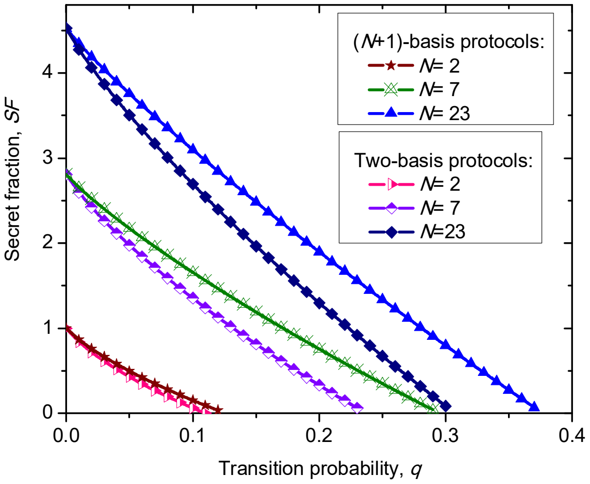


Fig. 11 Secret key fraction vs. transition probability, when system dimensionality *N* is used as a parameter.

5. Concluding Remarks

To simultaneously increase the SKR and extend the transmission distance, we have proposed to employ the Slepian-sates-based DV- and CV-QKD schemes. We have also proposed how to implement these schemes in an integrated quantum photonics platform, based on either transmissive or reflective waveguide Bragg gratings. The proposed multidimensional DV- and CV-QKD schemes are suitable for implementation in both aluminum nitride- and lithium niobate-based platforms. Regarding multidimensional DV-QKD, both prepare-and-measure and entanglement assisted schemes have been proposed. Regarding CV-QKD, Slepian-states have been employed as a degree of freedom to increase SKR through the concept of parallelization.

By simulations, for typical practical parameters, we have shown that low-cost RF-assisted 8-state discrete modulation, employing 10 Slepian-states, two polarization states, and 10 wavelengths, can be used to achieve record total SKR of 200 Mbs over 197 km of ultra-low-loss fiber.

References

[1] C. H. Bennet, G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” in Proc. *IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, pp. 175-179, 1984.

[2] C. H. Bennett, “Quantum cryptography: uncertainty in the service of privacy,” *Science*, vol. 257, pp. 752-753, 1992.

[3] S.-K. Liao, *et al*., “Satellite-to-ground quantum key distribution,” *Nature*, vol. 549, pp. 43–47, 2017.

[4] H.-L. Yin, *et al*., “Measurement-device-independent quantum key distribution over a 404 km optical fiber,” *Phys. Rev. Lett.*, vol. 117, p. 190501, 2 November 2016.

[5] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. van Meter, M. D. Lukin, “Quantum repeater with encoding,” *Phys. Rev. A*, vol. 79, p. 032325, 2009.

[6] 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.

[7] 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.

[8] S.-M. Zhao, *et al.*, “A large-alphabet quantum key distribution protocol using orbital angular momentum entanglement,” *Chin. Phys. Lett.*, vol. 30, no. 6, p. 060305, 2013.

[9] I. B. Djordjevic, “Multidimensional QKD based on combined orbital and spin angular momenta of photon,” *IEEE Photonics Journal*, vol. 5, no. 6, p. 7600112, 2013.

[10] 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.

[11] I. B. Djordjevic, “FBG-based Weak Coherent State and Entanglement Assisted Multidimensional QKD,” *IEEE Photonics Journal*, vol. 10, no. 4, p. 7600512, 2018.

[12] 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.

[13] D. Slepian, "Prolate spheroidal wave functions, Fourier analysis and uncertainty V, The discrete case," *Bell System Tech. J.*, vol. 57, no. 5, pp. 1373-1381, 1978.

[14] I. B. Djordjevic, M. Cvijetic, and C. Lin, "Multidimensional Signaling and Coding Enabling Multi-Tb/s Optical Transport and Networking," *IEEE Sig. Proc. Mag.*, vol. 31, no. 2, pp. 104-117, Mar. 2014.

[15] Y. Zhang, M. Arabaci, I. B. Djordjevic, "Evaluation of four-dimensional nonbinary LDPC-coded modulation for next-generation long-haul optical transport networks," *Optics Express*, vol. 20, no. 8, pp. 9296-9301, 04/09/2012.

[16] I. B. Djordjevic, "OAM-based Hybrid Free-Space Optical-Terahertz Multidimensional Coded Modulation and Physical-Layer Security," *IEEE Photonics Journal*, vol. 9, no. 4, p. 7905712, Aug. 2017.

[17] M. Lucamarini, Z. L. Yuan, J. F. Dynes, A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, pp. 400–403, 2018.

[18] X. Ma, P. Zeng, H. Zhou, "Phase-Matching Quantum Key Distribution," *Phys. Rev. X*, vol. 8. P. 031043, 2018.

[19] C. Wu, M. G. Raymer, "Efficient picosecond pulse shaping by programmable Bragg gratings," *IEEE J. Quantum Electron.*, vol. 42, no. 9, pp. 873-884, 2006.

[20] C. Xiong, W. H. P. Pernice, X. Sun, C. Schuck, K. Y. Fong, H. X. Tang, "Aluminum nitride as a new material for chip-scale optomechanics and nonlinear optics," *New Journal of Physics*, vol. 14, p. 095014, Sept. 2012.

[21] A. Guarino, G. Poberaj, D. Rezzonico, R. Degl'Innocenti, P. Günter, "Electro-optically tunable microring resonators in lithium niobate," *Nature Photonics*, vol. 1, no. 7, p. 407-410, July 2007.

[22] M. R. Fernández-Ruiz, M. Li, M. Dastmalchi, A. Carballar, S. LaRochelle, J. Azaña, "Picosecond optical signal processing based on transmissive fiber Bragg gratings," *Opt. Lett.*, vol. 38, pp. 1247-1249, 2013.

[23] W. Tadej, K. Zyczkowski, "A concise guide to complex Hadamard matrices," *Open Sys. & Information Dyn.*, vol. 13, pp. 133–177, 2006.

[24] Z. Qu, I. B. Djordjevic, M. A. Neifeld, "RF-subcarrier-assisted Four-state Continuous-variable QKD Based on Coherent Detection," *Optics Letters*, vol. 41, no. 23, pp. 5507-5510, Dec. 1, 2016.

[25] Z. Qu, I. B. Djordjevic, "Four-dimensionally multiplexed eight-state continuous-variable quantum key distribution over turbulent channels," *IEEE Photonics Journal*, vol. 9, no. 6, p. 7600408, Dec. 2017.

[26] Y. Tamura, H. Sakuma, K. Morita, M. Suzuki, Y. Yamamoto, K. Shimada, Y. Honma, K. Sohma, T. Fujii, and T. Hasegawa, "The First 0.14-dB/km Loss Optical Fiber and its Impact on Submarine Transmission," *J. Lightwave Technol.*, vol. 36, pp. 44-49, 2018.

[27] J. Lodewyck, *et al.*, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Phys. Rev. A*, vol. 76, p. 042305, 2007.

[28] I. B. Djordjevic, "On Advanced FEC and Coded Modulation for Ultra-High-Speed Optical Transmission," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 3, pp. 1920-1951, 2016.

[29] A. Leverrier A, P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation," *Phys. Rev. Lett.*, vol. 102, p. 180504, 2009.

[30] T. M. Cover TM, J. A. Thomas, *Elements of Information Theory*. John Wile & Sons, New York-Chichester-Brisbane-Toronto-Singapore, 1991.