Slepian-States-based DV- and CV-QKD Schemes Suitable for Implementation in Integrated Optics

Ivan B Djordjevic
University of Arizona, ECE Dept., 1230 E Speedway Blvd, Tucson, AZ 85721 - USA
e-mail: ivan@email.arizona.edu

ABSTRACT

To solve for low secret-key-rate (SKR) and short-distance problems of QKD in a simultaneous manner, we propose to encode information in orthogonal Slepian sequences' bases. Employment of multidimensional encoding-space enables high-spectral-efficiency-QKD so that SKR can be significantly improved. Generation, processing, and detection of Slepian-states for proposed QKD-protocols can be reliably implemented in an integrated optics platform, based on waveguide Bragg gratings.

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

1. INTRODUCTION

The research in QKD is getting momentum, in particular, after the first satellite-to-ground QKD demonstration. Recently, the QKD over 404 km of ultralow-loss optical fiber is demonstrated; however, with ultralow secure key rate ($3.2 \cdot 10^{-4}$ b/s). Given that quantum states cannot be amplified, the fiber attention limits the distance. On the other hand, the deadtime of the single-photon detectors (SPDs) employed in discrete variable (DV)-QKD, typically in 10-1000 ns range, limits the baud rate and therefore the secret-key rate (SKR). The continuous variable (CV)-QKD schemes, since they employ the homodyne/heterodyne detection, do not exhibit the deadtime limitation problem. 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 multiple information bits can be delivered upon receiving each single photon [1], thereby optimizing the photon efficiency for high-rate QKD in the absence of quantum repeaters. 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, position and linear momentum, orbital angular momentum (OAM), or simultaneously utilizing multiple parameters encoded in hyper-entangled states. The MD time-bin-encoded QKD can be seamlessly incorporated into standard telecom networks, as experimentally demonstrated in [2], but the time-bin encoding largely sacrifices the spectral efficiency. 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 limit the scalability.

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. Such an approach is highly robust against turbulence effects in free-space optical (FSO) links and dispersion effects/fiber nonlinearities in fiber-optics channels, thereby improving the QKD distance. Moreover, the MD encoding space enables high spectral efficiency QKD so that 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 the proposed electronically controlled waveguide Bragg gratings (EC-WBGs).

2. SLEPIAN-STATES-BASED QKD PROTOCOLS SUITABLE FOR INTEGRATED OPTICS

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 (WCS)-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 [1], EC-WBGs can be mass fabricated in a PIC platform, in lieu of the liquid crystal platform [3], so that quantum information encoded in a large number of 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 [2], 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-frequency (t.f.) encoding requires N time slots with only one time bin, on average, being occupied by a photon, but the rest time slots are left vacuum. 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 [1], 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 mutually orthogonal so that a Slepian sequence with N elements can be used as an encoding basis. The MD-quantum communication based on Slepian states is 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 on the system dimensionality N. However, the bandwidth required in time-frequency QKD system is proportional to $1/\tau=N/T$.

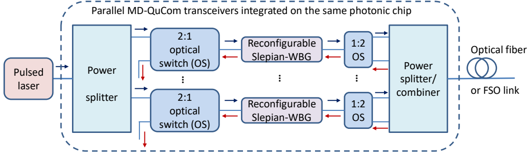

Figure 1. Illustration of parallel MD-quantum communication (QuCom) transceiver integrated on the same quantum photonic chip. Arrow → (←) denotes the transmitting (receiving) direction.

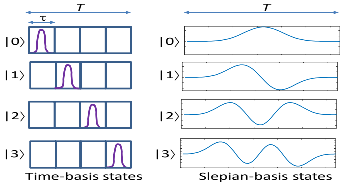

Figure 2. (Left) Time-basis in 4-D t.f. QKD (T: symbol duration, τ: bin duration, τ=T/4). (Right) Slepian- states in 4-D MD-QKD.

Given the space limitations, we only describe the *MD-DV-QKD based on Slepian-WBGs* that does not require the use of entangled states. In basic WBG-based *random base selection prepare-and-measure (PM) protocol*, illustrated in Fig. 3, we employ Slepian-WBGs with mutually orthogonal impulse responses, denoted as $\{[0\rangle, |1\rangle, \ldots, |N\text{-}1\rangle\}$ as the encoding basis for MD-QKD. Alice's encoder is composed of an adaptive, reconfigurable Slepian-WBG, to be implemented in PIC technology, and a circulator. To encode Alice randomly selects the orthogonal impulse response (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 [3]. 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 [4] and as such are suitable for large-scale integration. To probe for Eve's presence Alice reconfigures the WBG to generate the superposition state $([0\rangle+|1\rangle+ \ldots + |N\text{-}1\rangle)/\sqrt{N}$. On receiver side, Bob employs another reconfigurable matched-Slepian-WBG. The matched-Slepian-WBG reflects the pulse back, and the SPD at port 3 of circulator detects the presence of pulse, and Bob is able to identify the transmitted symbol, when Alice used the same basis state $|n\rangle$. When non-matched Slepian-WBG is used, Bob will not be able to detect the presence of pulse. To improve the SKR, it is possible to employ a series of matched WBGs, on Bob's side. Only the matched WBG reflects the pulse back, and corresponding SPD at circulator output port 3 will able to detect the presence of pulse and thus identify the matched IR. 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 higher than the prescribed threshold they abort protocol, otherwise, they continue with the protocol. All other signaling intervals contribute to the sifted key. After that, the classical postprocessing steps are applied.

Regarding the *MD-CV-QKD protocols*, we propose to employ Slepian-states as a new degree of freedom to implement parallel CV-QKD schemes, which is illustrated in Fig. 5, for the discrete modulation CV-QKD case. Given that optical circulators are difficult to implement in integrated optics, we propose to employ the *transmissive WBGs* instead. The transmissive FBGs have been already studied for use in picosecond optical signal processing [5], and we believe that fabrication of transmissive WBGs to generate Slepian-states will be possible too. 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 (MPSK) 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. 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 with matched transmissive WBG filter. The k-th (k=1,2,…,K) matched WBG output signal undergoes the heterodyne detection, and in the phase noise cancellation (PNC) stage the in-phase and quadrature signals are squared and added, and after the proper low-pass filter the output signal will be proportional to the modulated RF subcarrier, with frequency difference term being removed out. On such a way, the detected RF subcarrier signal is insensitive to the laser phase noise and frequency offset fluctuations [6]. The classical postprocessing is then applied on the whole raw key.

To illustrate high potential of proposed Slepian-sates-based QKD protocols, in Fig. 6 we provide SKR results per single Slepian-state and single wavelength for both DV- and CV-QKD protocols for different SMF distances. In simulations, we assume that recently fabricated ultra-low-loss fiber with attenuation 0.1419 dB/km at 1560 nm is used [7]. Regarding the CV-QKD protocols, we assume that heterodyne detection is used for both Gaussian modulation (GM) and RF-assisted discrete modulation (DM) with 8-states as described in [6]. 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). Now 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. Now be employing both polarization states, 10 Slepian-states, and 10 wavelength channels the total SKR of 720 Mb/s can be achieved, which would represent the record SKR for distance of 200 km. Finally, when the RF-assisted DM with 8 states is employed (for ε=10^{-3} and v_{el}=10^{-2}), we can achieve the total SKR of 0.73 Mb/s×2×10×10=146 Mb/s.

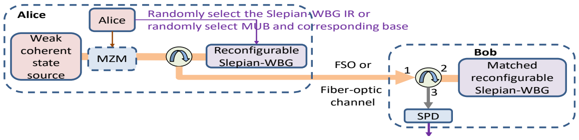
Alice
Alice
Randomly select the Slepian-WBG IR or
randomly select MUB and corresponding base
Weak coherent state source
MZM
Reconfigurable Slepian-WBG
FSO or
Fiber-optic channel
Bob
1
2
3
Matched reconfigurable Slepian-WBG
SPD

Figure 3. Reconfigurable Slepian-WBG-based WCS-QKD scheme implementing random base selection PM protocol.

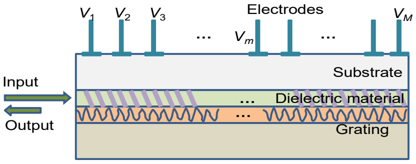

Figure 4. Implementation of Slepian-WBG (modified from [3]).

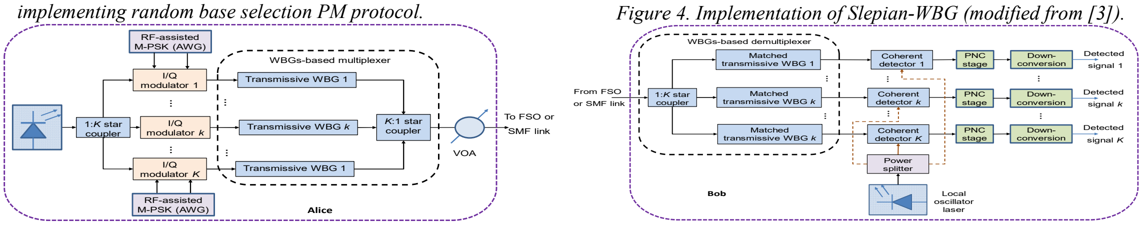

Figure 5. The proposed scheme for parallel WBGs-based RF-assisted CV-QKD protocol: (left) Alice's transmitter and (right) Bob's receiver. (Only the details for single polarization and single wavelength are shown to facilitate the explanations.)

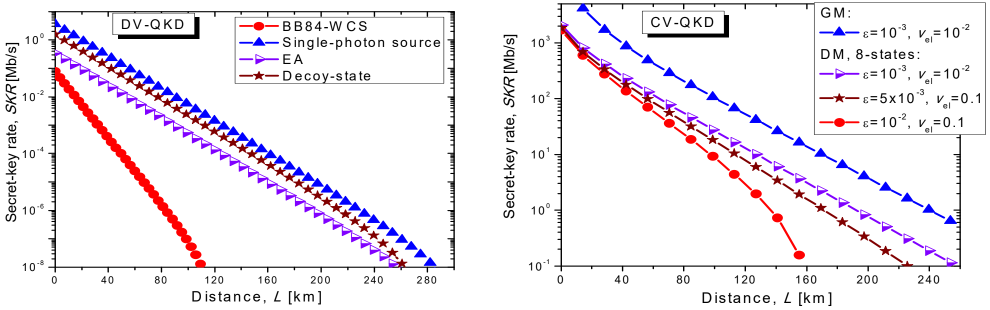

Figure 6. SKRs per single wavelength and single Slepian-sate vs. distance for: (left) DV-QKD and (right) CV-QKD protocols. For DV-QKD protocols, we assume that detector efficiency is 0.2, visibility is 0.99, dark counts' probability is 10^{-6}, the dead time of 10 ns, while the mean photon number is optimum. For CV-QKD, we assume that both detector and reconciliation efficiencies are 0.9 each. The baud rate for CV-QKD is 10 GBd, while RF subcarrier for DM is set to 10 GHz.

REFERENCES

[1] I. B. Djordjevic: FBG-based weak coherent state and entanglement assisted multidimensional QKD, *IEEE Photonics Journal*, vol. 10, no. 4, p. 7600512, 2018.

[2] N.T. Islam, *et al.*: Provably secure and high-rate quantum key distribution with time-bin qudits, *Sci. Adv.*, vol. 3, p. e1701491, 2017.

[3] 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.

[4] A. Guarino, *et al.*: Electro-optically tunable microring resonators in lithium niobate, *Nature Photonics*, vol. 1, no. 7, p. 407-410, July 2007.

[5] M.R. Fernández-Ruiz, *et al.*: Picosecond optical signal processing based on transmissive fiber Bragg gratings, *Opt. Lett.*, vol. 38, pp. 1247-1249, 2013.

[6] 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.

[7] Y. Tamura, *et al.*: The First 0.14-dB/km loss optical fiber and its impact on submarine transmission, *J. Lightw. Technol.*, vol. 36, pp. 44-49, 2018.