Discretized Gaussian Modulation-based Continuous Variable (CV)-QKD

Ivan B. Djordjevic
University of Arizona, Department of Electrical and Computer Eng., 1230 E. Speedway Blvd., Tucson, AZ 85721, USA
E-mail: ivan@email.arizona.edu

Abstract– To overcome the low-reconciliation-efficiency problem of Gaussian modulation (GM)-based-CV-QKD, we propose to use discretized-GM-based-CV-QKD. This scheme has complexity and reconciliation-efficiency similar to discrete modulation (DM)-based-CV-QKD and at the same time solves for the problem of nonexistence of strict security proofs for DM-CV-QKD under collective attacks.

I. Introduction

Thanks to recent satellite-to-ground QKD demonstration [1], the research in QKD is getting momentum. Discrete variable (DV)-QKD schemes achieve unconditional security by employing no-cloning theorem. On the other hand, continuous variable (CV)-QKD schemes employ the uncertainty principle. One of the key limitations for DV-QKD represents long deadtime of the single-photon detectors (SPDs), which limits the baud rate and therefore the secret-key rate (SKR). On the other hand, the CV-QKD schemes employ the homodyne/heterodyne detection instead and as such do not exhibit this problem. Very popular CV-QKD protocols are those based on either discrete modulation (DM) [2]-[6] or Gaussian modulation (GM) [7],[8]. One of the key disadvantages of GM is related to its low reconciliation efficiency [7],[8]. On the other hand, the DM-based CV-QKD protocols have much better information reconciliation (error correction) efficiency and are compatible with state-of-the-art fiber-optics communications' equipment. Unfortunately, strict security proofs of DM-based CV-QKD for collective attacks are still not well developed.

To overcome these key challenges for DV-QKD as well as for DM-based CV-QKD, such as a nonexistence of accurate security proofs, we propose to employ discretized GM-based CV-QKD protocol. The proposed QKD scheme employs the Gaussian source implemented in electrical domain instead of the optical Gaussian source. This scheme has complexity and reconciliation efficiency comparable to that of DM-CV-QKD schemes and solves for the strict unconditional security problem of DM-DV-QKD under collective attacks. We demonstrate that for all transmission losses the 32-points generated from Gaussian source in digital-domain in time-varying fashion are sufficient to closely approach theoretical SKR-limit. We also show that signal constellations designed to faithfully represent the Gaussian source can also closely approach the SKR-limit, but in high transmission loss regime only.

II. Proposed RF-assisted Discretized Gaussian Modulation-based CV-QKD scheme

To initialize the QKD system, Alice and Bob pre-share the common sequence of seeds, corresponding to different sizes M of signal constellations generated from Gaussian source, to be used in subsequent discretized GM-DV-QKD. In initialization stage, Alice selects at random seed to be used for Gaussian noise generator. She then generates at random a sequence of points from Gaussian random generator. She splits this sequence into subsequences of length M. She selects subsequences closely approaching the mutual information between Alice and Bob. In transmission stage, Alice further randomly selects the subsequence (Gaussian signal constellation) to use, followed by a random selection of point from that subsequence, and imposes it on an RF subcarrier. In-phase and quadrature components of such generated points, with the help of arbitrary waveform generator (AWG), are used as RF inputs of an electro-optical (EO) I/Q modulator, as shown in Fig. 1. After the adjustment of the variance v_A by the variable optical attenuator (VOA), such obtained pulse is sent to Bob over the quantum channel. The channel is characterized by transmissivity T and excess noise ε so that total channel added noise variance, referred to the channel input, can be expressed in shot-noise unit (SNU) by $\chi_{line}=1/T-1+\varepsilon$.

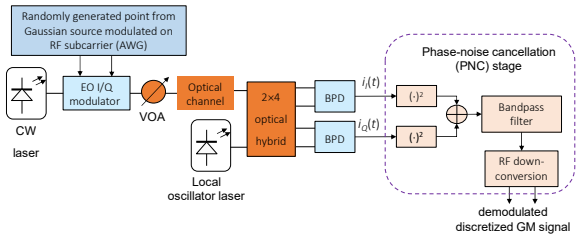

Fig. 1 The proposed RF-assisted discretized GM-CV-QKD scheme. VOA: variable optical attenuator, BPD: balanced photodetector, BPF: bandpass filter.

On receiver side, Bob employs the heterodyne coherent detection together with a phase-noise cancellation (PNC) stage [2],[6] 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 [9]. The PNC stage further performs bandpass filtering to remove DC component and double-frequency terms, followed by the down-conversion, implemented with the help of multipliers and low-pass filters. On such a way Bob detects a point out of M possible points from the subsequence, in similar fashion as for DM. Given that PNC stage cancels the phase noise and frequency offset fluctuations, it exhibits better tolerance to the excess noise compared to the traditional DM-based CV-QKD schemes.

In sifting procedure, Alice announces the indices of the seeds being used in every signaling interval. Given that Bob knows the seeds he can easily identify Gaussian

978-1-7281-0615-1/19/$31.00 ©2019 IEEE

signal constellation being used. After that Alice and Bob perform conventional parameter estimation and classical postprocessing (information reconciliation and privacy amplification) steps. Clearly, the receiver complexity is comparable to DM QKD schemes, but the proposed scheme preserves the unconditional security under collective attacks offered by GM-based QKD scheme.

III. Illustrative SKR Results

The expression for secret fraction (SF), obtained by one-way postprocessing, for reverse reconciliation, is given by:

$$SF = \beta I(A;B) - \chi(B;E),$$

where $I(A;B)$ represents the mutual information between Alice and Bob, while the second term $\chi(B;E)$ corresponds to the Holevo information between Eve and Bob, calculated as described in [7],[8] (for collective attacks). We use β to denote the reconciliation efficiency. The mutual information $I(A;B)$ is calculated as described in [10]. For CV-QKD schemes, the secrecy rate can be interpreted as the normalized SKR, where the normalization is with respect to the signaling rate R_s.

In Fig. 2, we provide the SKR results for the proposed discretized GM-QKD protocol, for different subsequences (constellation) sizes. In calculations, the electrical noise variance is set to $v_{el}=10^{-2}$, the excess noise variance to $\varepsilon=10^{-3}$, detector efficiency is set to $\eta=0.85$, and reconciliation efficiency is set to $\beta=0.85$. Clearly, for channel loss larger than 15 dB, discretized GM with 16 points is sufficient to achieve the theoretical GM-CV-QKD limit. For smaller channel loss values there is a certain degradation in normalized SKR. On the other hand, the discretized-GM with 32 points closely approaches the SKR-limit for all channel losses.

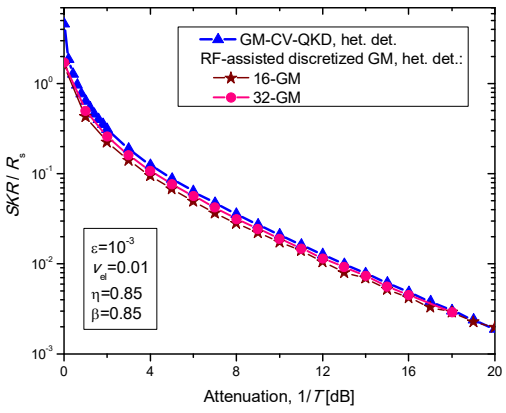

Fig. 2 Normalized SKRs for proposed discretized GM-QKD protocol vs. channel loss for different signal constellation sizes.

We also study the SKR performance of simplified version of discretized GM-QKD, in which for each seed the optimized signal constellation design (OSCD) algorithm [11] is run based on a training sequence from the Gaussian generator to get faithful representation of the source. In this version, the coordinates of corresponding OSCD constellations are stored in look-up-table (LUT). The index of the seed is now used as an address to get the coordinates from the LUT. The SKR results are summarized in Fig. 3, for the same parameters being used in Fig. 2. For channel loss larger than 18 dB, the 8-OSCD-based QKD scheme closely approaches theoretical GM-QKD SKR-limit. For comparison purposes, the SKR results for eight-state DM-CV-QKD protocol, proposed in [5], are provided as well, which are well below the 8-OSCD-based CV-QKD scheme.

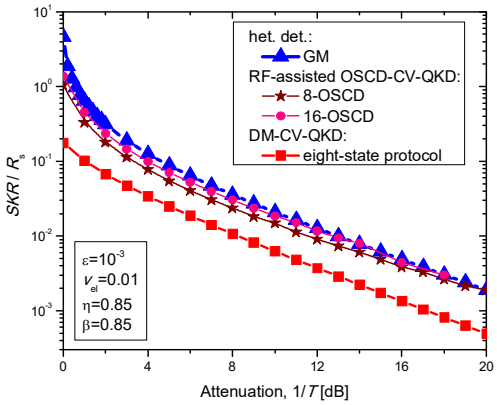

Fig. 3 Normalized SKRs when simplified OSCD-based QKD is used for different signal constellation sizes.

IV. Concluding Remarks

To solve for low-reconciliation-efficiency problem of the GM-based-CV-QKD scheme, we have proposed to use the discretized-GM-based-CV-QKD. This scheme has complexity and reconciliation-efficiency similar to the DM-based-CV-QKD and at the same time solves for the problem of nonexistence of strict security proofs for DM-CV-QKD under collective attacks. In medium and high transmission loss regimes this scheme closely approaches the theoretical GM-QKD SKR-limit. The simplified 16-OSCD-based QKD scheme closely approaches SKR-limit for channel loss larger than 14 dB.

References

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

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

[3] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, p. 010303(R), 1999.

[4] R. Namiki, T. Hirano, "Security of quantum cryptography using balanced homodyne detection," *Phys. Rev. A*, vol. 67, p. 022308, 2003.

[5] A. Becir, *et al*., "Continuous-variable quantum key distribution protocols with eight-state discrete modulation," *Int. J. Quantum Inform.*, vol. 10, p. 1250004, 2012.

[6] 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.

[7] R. Garcia-Patron, *Quantum Information with Optical Continuous Variables: from Bell Tests to Key Distribution*. Ph.D. Thesis, Université Libre de Bruxelles, 2007.

[8] C. Weedbrook, *et al*., "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, p. 621, 2012.

[9] I. B. Djordjevic, *Advanced Optical and Wireless Communications Systems*. Springer International Publishing, Switzerland, 2017.

[10] I. Djordjevic, "LDPC-coded MIMO optical communication over the atmospheric turbulence channel using Q-ary pulse-position modulation," *Optics Express*, vol. 15, pp. 10026-10032, 2007.

[11] T. Liu, I. B. Djordjevic, "On the optimum signal constellation design for high-speed optical transport networks," *Optics Express*, vol. 20, no. 18, pp. 20396-20406, 27 August 2012.