Singular Layer Transmission for Continuous-Variable Quantum Key Distribution

Laszlo Gyongyosi[1,2], Sandor Imre[1]
[1]*Quantum Technologies Laboratory, Department of Telecommunications, Budapest University of Technology, 2 Magyar tudosok krt., Budapest, H-1117, HUNGARY,*
[2]*MTA-BME Information Systems Research Group, Hungarian Academy of Sciences, 7 Nador u., Budapest, H-1051, HUNGARY*
gyongyosi@hit.bme.hu

Abstract: We develop a singular layer transmission model for continuous-variable quantum key distribution (CVQKD). We show that the singular layer assistance provides improved secret key rates for CVQKD, particularly in crucial low signal-to-noise ratio regimes.
OCIS codes: (270.5568); (270.5585); (270.5565).

1. Introduction

The continuous-variable quantum key distribution (CVQKD) protocols allow for the legal parties to transmit information with unconditional security over the current, well-established standard telecommunication networks. The CVQKD protocols use continuous quantum systems for the information transmission, practically Gaussian random distributed position and momentum quadratures in the phase space [1]. These quadratures identify a continuous-variable (CV) quantum state in the phase space, which are then transmitted over a noisy quantum link (e.g., via an optical fiber or a wireless optical channel), which is attacked by an eavesdropper [2-3]. Because the optimal attack against CVQKD protocols is a Gaussian attack, the noise of the physical quantum link can be provably modeled as an additive white Gaussian noise and the link as a Gaussian channel. The CVQKD protocols are equipped with several benefits in comparison with the discrete-variable (DV) QKD; however, in comparison with the traditional telecommunication protocols, the efficiency of CVQKD still requires significant improvements. An enhancement is particularly crucial and essential for the low signal-to-noise ratio (SNR) regimes, at which the experimental long-distance CVQKD protocols are operating. For this purpose, the adaptive multicarrier quadrature division (AMQD) modulation scheme has been recently introduced for CVQKD [2], which injects several convenient abilities into CVQKD regarding the transmission rates, distances, and tolerable noise level, similar to the orthogonal frequency-division multiplexing (OFDM) of traditional networking. In particular, the AMQD modulation granulates the transmit information into Gaussian subcarrier CVs and formulates Gaussian sub-channels from the physical Gaussian link, leading to improved transmission distances, higher secret key rates, and enhanced tolerable excess noise. The benefits of AMQD have also been extended to a multiuser scenario within the framework of the AMQD–multiuser quadrature allocation (MQA) multiple-access scheme. The AMQD-MQA [4] uses the Gaussian subcarriers and the AMQD modulation for the reliable simultaneous transmission of the users' input CVs and provides capacity-achieving multiple-access communication for the parties over a shared physical Gaussian quantum channel. The singular value decomposition (SVD) is a well-known tool in linear algebra, with a widespread application from mathematical statistic to signal processing. In this work, we show that the benefits of SVD can also be exploited in a CVQKD scenario. We reveal that the information transmission of CVQKD over the Gaussian quantum channel can be rephrased in terms of SVD, which is called the singular layer transmission model throughout. The singular layer injects an additional degree of freedom into the transmission, which can be exploited in the protocol. Specifically, the singular layer defines a higher-level layer above the physical layer and transforms the quantum channel onto a set of *eigenchannels* [5]. From the layer structure, it follows that the singular layer transmission does not require any change in the lower layers, because the SVD defines a purely logical layer over the physical layer transmission.

2. SVD-assisted AMQD-MQA

In the standard $K \rightarrow K$ AMQD-MQA scheme, a single transmitter generates the input messages of the *K*-independent users. The scheme is based on the AMQD modulation and its sub-channel allocation mechanism [2]. The aim of the *K*-independent users is to provide a simultaneous reliable transmission for *K*-independent receivers through the physical Gaussian quantum channel $\mathcal{N}$. The multiple access communication is realized by the AMQD modulation, which granulates the inputs of the users into several Gaussian subcarrier CVs. These Gaussian subcarrier CVs are then transmitted through the $\mathcal{N}_i$ Gaussian sub-channels, following the steps of AMQD. The subset $\mathcal{A}$ of transmit users is selected via the procedure of rate selection at the $\mathcal{E}$ encoder. Each $\mathcal{N}_i$ is allocated by

a constant modulation variance σ_ω^2 per the *x* and *p* quadrature components, which provably provide an optimal solution in low-SNR regimes because its performance is very close to the exact allocation [2]. The Gaussian quadratures that sent via AMQD modulation are dedicated to *K*-independent users. In Fig. 1, the elements of the additional layer injected by the SVD are depicted above the functional components of AMQD-MQA.

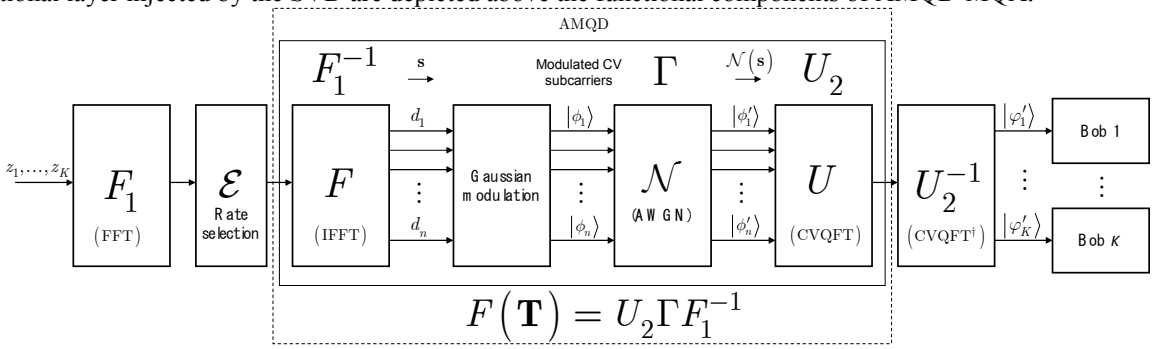

Figure 1. The singular layer transmission model of the $K \rightarrow K$ AMQD-MQA multiple-access scheme. The model consists of a single encoder and *K*-independent receivers. The SVD of AMQD is expressed by the matrix $F(\mathbf{T}) = U_2 \Gamma F_1^{-1}$. The pre- and post-unitaries of the singular layer are the F_1 scaled FFT operation and its unitary inverse CV operation U_2^{-1}.

3. Results

The singular layer of CVQKD injects an extra degree of freedom into the transmission to extend the achievable distances and to improve the secret key rates. From the SVD of $F(\mathbf{T}) = U_2 \Gamma F_1^{-1}$ and $F(\mathbf{T}) = U_2 \Gamma U_1^{-1}$, the additional degree of freedom can be exploited to reach an improved performance in the multicarrier transmission of AMQD. The effect of the singular layer on the modulation variance allocation mechanism of the Gaussian sub-channels is illustrated in Fig. 2.

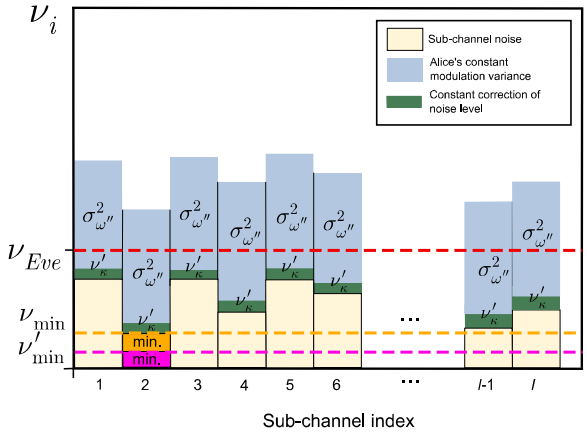

Figure 2. The effect of singular layer on the sub-channel modulation variance. In an AMQD modulation, the Gaussian subcarrier CVs are transmitted over *l* good (i.e., $\nu_i < \nu_{Eve}$) Gaussian sub-channels $\mathcal{N}_i$. The sub-channel noise $\nu_{\min}$ is decreased from $\nu_{\min} = \sigma_{\mathcal{N}}^2 \Big/ \max_{\forall i} \left|F(T_i(\mathcal{N}_i))\right|^2$ *to* $\nu'_{\min} = \sigma_{\mathcal{N}}^2 \Big/ \max_{n_{\min}} \lambda_i^2$. The total constraint is increased to $\frac{1}{l}\sum_l \sigma_{\omega_i''}^2 = \sigma_{\omega''}^2 > \sigma_\omega^2$.

The results confirm that the additional degree of freedom brought in by the singular layer can be significantly exploited in the crucial low-SNR regimes, which is particularly convenient for long-distance CVQKD scenarios.

4. References

[1] F. Grosshans, P. Grangier, Reverse reconciliation protocols for quantum cryptography with continuous variables, arXiv:quant-ph/0204127v1 (2002).

[2] L. Gyongyosi, Adaptive Multicarrier Quadrature Division Modulation for Continuous-variable Quantum Key Distribution, arXiv:1310.1608 (2013).

[3] S. Imre and L. Gyongyosi. Advanced Quantum Communications - An Engineering Approach. Wiley-IEEE Press (New Jersey, USA), (2012).

[4] L. Gyongyosi, Multiuser Quadrature Allocation for Continuous-Variable Quantum Key Distribution, arXiv:1312.3614, (2013).

[5] L. Gyongyosi: Singular Layer Transmission for Continuous-Variable Quantum Key Distribution, arXiv:1402.5110 (2014).