Multiuser Quadrature Allocation 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 propose the adaptive multicarrier quadrature division–multiuser quadrature allocation (AMQD-MQA) multiple access technique for continuous-variable quantum key distribution (CVQKD), and analyze the performance of the scheme.
OCIS codes: (270.5568); (270.5585); (270.5565).

1. Introduction

The continuous-variable quantum key distribution (CVQKD) protocols allow the parties to realize unconditionally secure communication over the standard, currently established telecommunication networks [1–5]. The CVQKD schemes have several benefits over the discrete variable (DV) quantum key distribution (QKD) protocols; most importantly, they do not require single-photon encoding and decoding, which allows its practical implementation by standard, currently available technologies and devices. The single-carrier modulation does not perform such advanced techniques within CVQKD as it is already available in a traditional telecommunication scenario. As a corollary, several important communication techniques cannot be implemented within the framework of the CVQKD protocols. To eliminate these drawbacks, the adaptive multicarrier quadrature division (AMQD) modulation has been recently introduced [4], which allows the parties to significantly extend the possibilities of single-carrier CVQKD protocols. The AMQD is based on the use of the Gaussian subcarrier CVs (continuous-variables) and continuous unitary operations and offers several benefits over the single-carrier modulation. It provides higher noise resistance, higher tolerable loss, improved rates, and transmission distances for the parties.

The AMQD-MQA scheme exploits and extends the benefits of AMQD modulation into a multiple access scenario [2,5]. The AMQD-MQA allows the realization of multiple input–multiple output transmission within CVQKD, making it possible for users to have a simultaneous reliable communication over the physical Gaussian quantum channel by the dynamic allocation of the Gaussian subcarrier CVs. The subcarrier CVs divide the physical Gaussian channel into Gaussian sub-channels, each dedicated for the transmission of a given Gaussian subcarrier with an independent noise variance. The inputs of the selected independent transmit users are conveyed by the Gaussian subcarrier CV states, which are received by the independent parties using an inverse continuous unitary. The noise acts on the position and momentum quadratures of the Gaussian subcarrier CVs. The AMQD-MQA is equipped with all the benefits of AMQD, such as improved tolerable loss and excess noise, higher transmission distances, and optimized key rates. It extends the possibilities of AMQD for a multiuser scenario, which allows all users to simultaneously achieve the benefits provided by the AMQD framework similar to the well-known orthogonal frequency-division multiplexing multiple access (OFDMA) of traditional networking. As an important corollary, the AMQD-MQA overwhelms the problems of single-carrier protocols to reach a much more efficient and significantly optimized multiple access transmission compared with a single-carrier multiuser scheme.

2. 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. The standard setting of $K \rightarrow K$ AMQD-MQA is summarized in Figure 1 [4].

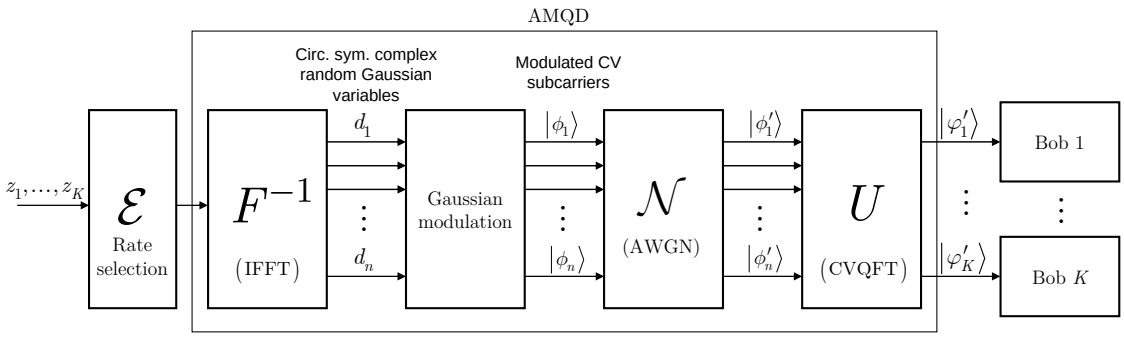

Figure 1. The AMQD-MQA multiple access scheme with a single transmitter and multiple receivers. The encoder ($\mathcal{E}$) modulates and transmits the subcarriers of the *K*-independent users by an AMQD modulation. In the rate-selection phase, Alice selects the users for the transmission and the $\sigma^2_{\omega_{0,k}}$ initial modulation variance (per quadrature components) of variable z_k. The data of the transmit users are then fed into the IFFT (inverse fast Fourier transform) operation.

3. Results

The results on the $\mathbb{C}$ capacity region of $\left(R_1, R_2\right)$ of U_1 and U_2 in AMQD-MQA are summarized in Figure 3. The corner points C_1 and C_2 identify the maximal rates at with a single user can communicate. The line between the two corner points represents that trade-off between the rates of users U_1 and U_2, at which simultaneously reliable transmission is possible, where F stands for the CVQFT (Continuous-Variable Quantum Fourier Transformation), T is the channel transmittance, $\sigma^2_{\mathcal{N}}$ is the sub-channel noise variance [4].

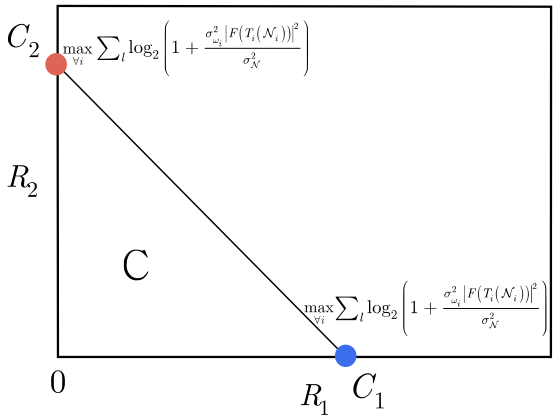

Figure 2. The $\mathbb{C}$ capacity region of the AMQD-MQA with two users U_1 and U_2. The transmission is realized through *l* subcarriers, each having a constant modulation variance σ^2_{ω} per quadrature components. The two users communicate over the Gaussian quantum channel with rates R_1 and R_2. At the corner points C_1 and C_2 (red and blue dots), only one user is allowed to transmit and all degrees of freedom is allocated to that user.

The rate allocation of the users is performed through the sophisticated handling of the subcarrier CVs and continuous unitary operations. We showed that in the AMQD-MQA, the users can optimally perform simultaneously reliable capacity-achieving communication over the Gaussian sub-channels. The AMQD-MQA allows optimal multiple input–multiple output, capacity-achieving simultaneous transmission for the users, which is particularly convenient in an experimental long-distance CVQKD scenario, specifically in the crucial low-SNR regimes.

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).