Adaptive Multicarrier Quadrature Division Modulation for Long-Distance Continuous-Variable Quantum Key Distribution

L. Gyongyosi*[a,b], S. Imre[a]

[a] Quantum Technologies Laboratory, Department of Telecommunications, Budapest University of Technology and Economics, 2 Magyar tudosok krt, H-1111, Budapest, Hungary;

[b] MTA-BME Information Systems Research Group, Mathematics and Natural Sciences, Hungarian Academy of Sciences, H-1518, Budapest, Hungary

*Electronic address: gyongyosi@hit.bme.hu

ABSTRACT

We propose the adaptive multicarrier quadrature division (AMQD) modulation technique for continuous-variable quantum key distribution (CVQKD). The method granulates the Gaussian random input into Gaussian subcarrier continuous variables in the encoding phase, which are then decoded by a continuous unitary transformation. The subcarrier coherent variables formulate Gaussian sub-channels from the physical link with strongly diverse transmission capabilities, which leads to significantly improved transmission efficiency, higher tolerable loss, and excess noise. We also investigate a modulation-variance adaption technique within the AMQD scheme, which provides optimal capacity-achieving communication over the sub-channels in the presence of a Gaussian noise.

Keywords: continuous-variable quantum key distribution, Gaussian modulation, quantum cryptography, quantum Shannon theory.

1. INTRODUCTION

Continuous-variable (CV) quantum key distribution (QKD) systems allow for the establishment of an unconditionally secure quantum communication over the current standard telecommunication networks. CVQKD systems possess several benefits and advantages over the DV (discrete variable) protocols, since they do not require specialized devices or unreachable special requirements in an experimental scenario [11-18], [22-30]. CVQKD systems are based on continuous variables such as Gaussian random position and momentum quadratures in the phase space. The Gaussian modulated coherent states are transmitted over a noisy quantum channel, where the presence of an eavesdropper adds a white Gaussian noise to the transmission. Since CVQKD schemes were developed and introduced just a few years ago, there are still many open questions regarding the optimal encoding scheme. A Gaussian modulation is a robust and easily applicable finding in a practical scenario, and allows for the implementation of the protocol in the experiment; however, CVQKD is still very sensitive to the imperfections of the transmission and the practical devices. The performance of the protocol is strongly determined by the excess noise of the quantum channel, and the transmittance parameter of the physical link (specifically, the Gaussian noise of the quantum channel models the eavesdropper's optimal entangling cloner attack [2-3], [11-18], and the channel is referred to as a Gaussian quantum channel). Since the amount of tolerable loss and the excess noise are central parameters from the viewpoint of the running of CVQKD, it would be very desirable to make some optimization steps in the encoding and decoding process to override the current limitations and to improve the quality of the quantum-level transmission. Our aim is to provide a solution to this problem by introducing the *adaptive multicarrier quadrature division* (AMQD [23]) modulation technique for CVQKD, which can be applied both in one-way and two-way CVQKD to increase the tolerable loss and excess noise. In traditional telecommunications, OFDM (orthogonal frequency-division multiplexing) is a well-known and widely applied technique for improving the bandwidth efficiency over noisy communication networks [6-10]. In an OFDM scheme, the information is encoded in multiple carrier frequencies, and its main advantage over single-carrier transmission is that the subcarrier-based transmission can attenuate and overwhelm the problems of diverse and unfavorable channel conditions. OFDM systems have been admitted to be a useful encoding method in traditional networking; however, no similar method exists for CVQKD. If a similar solution were available for continuous variables, one could enjoy similar benefits in a quantum-communication scenario; however, up to this point no analogous answer exists for quantum-level transmission. With this in mind, we introduce the idea of AMQD, which works on continuous variables and for which similar benefits can be reached in the process of quantum-level information transmission, e.g., in a classical scenario by the application of the

Updated 1 March 2012

OFDM. In the standard coding scenario, Alice, the sender, modulates and separately transmits each coherent state in the phase space. This standard modulation scheme is referred as single-carrier modulation throughout, consistent to its traditional meaning.

The key idea behind AMQD modulation is as follows. Alice draws a zero-mean, circular symmetric complex Gaussian random vector, which is then transformed by the inverse Fourier operation. At a given modulation variance, Alice prepares her Gaussian subcarrier CVs, which are then fed into the channel. Bob, the receiver, applies the inverse unitary of Alice's operation, which makes it possible for him to recover the noisy version of Alice's input coherent states. This kind of communication will be referred as multicarrier modulation.

What are the main advantages of this kind of communication? There are several fine corollaries. First of all, the Gaussian subcarrier CV states sent through the channel, which overall allows higher tolerable loss and excess noise at a given modulation variance. Second, the Gaussian quantum channel can be viewed as several parallel Gaussian quantum channels, called sub-channels, each dedicated for the transmission of a given subcarrier with an independent, and significantly lower noise variance. Third, the information transmission capability of the sub-channels is very diverse, depending on the variance of the subcarrier CV, which allows for the development of smart adaptive modulation techniques for the proposed multicarrier quadrature division-encoding technique. The idea behind this is to use only the "good" Gaussian sub-channels for the transmission, and to not send any valuable information over the so noisy sub-channels. It is a particularly convenient approach, since the result of the adaptive allocation is a better performance of the protocol at low SNRs (signal-to-noise ratio) and higher tolerable loss, which are crucial cornerstones in an experimental CVQKD that operates in practice at very low SNRs. From these, the purposes are now clear. We have to find the operation that works on continuous variables and outputs the subcarrier quadratures, which can divide the physical Gaussian channel into Gaussian sub-channels. We also need the continuous unitary inverse of this operation. If we have it, then we have to find an adaptive modulation-variance allocation mechanism, which allows no to send valuable information over the very noisy Gaussian sub-channels. Fortunately, these features are all included in our AMQD coding scheme. The AMQD modulation granulates Alice's initial Gaussian states into several subcarrier Gaussian CVs, which divide the physical channel into several Gaussian sub-channels. Bob applies an inverse continuous unitary operation, which allows him to obtain Alice's initial (noisy) coherent states. The proposed AMQD modulation offers several important features, but the main improvement is in the quality of the quantum-level transmission, since the subcarriers allow a more efficient communication over the same quantum channel at a given modulation variance.

This paper is organized as follows. In Section 2, preliminaries are proposed. Section 3 introduces the multicarrier quadrature division scheme. In Section 4, the adaptive modulation variance allocation mechanism is discussed. Finally, Section 5 concludes the results. For further details and information see [23].

2. PRELIMINARIES

In the standard single-carrier modulation scheme, the input coherent state $\left|\varphi_i\right\rangle = \left|x_i + \mathrm{i}p_i\right\rangle$ is a Gaussian state in the phase space $\mathcal{S}$, with i.i.d. Gaussian random position and momentum quadratures $x_i \in \mathbb{N}\left(0, \sigma_{\omega_0}^2\right)$, $p_i \in \mathbb{N}\left(0, \sigma_{\omega_0}^2\right)$, where $\sigma_{\omega_0}^2$ is the modulation variance. The coherent state $\left|\varphi_i\right\rangle$ in the phase space $\mathcal{S}$ can be modeled as a zero-mean, circular symmetric complex Gaussian random variable $z \in \mathcal{C}\mathbb{N}\left(0, \sigma_{\omega_z}^2\right)$, with variance $\sigma_{\omega_z}^2 = \mathbb{E}\left[\left|z\right|^2\right]$, and with i.i.d. real and imaginary zero-mean Gaussian random components, $\mathrm{Re}\left(z_i\right) \in \mathbb{N}\left(0, \sigma_{\omega_0}^2\right)$, $\mathrm{Im}\left(z_i\right) \in \mathbb{N}\left(0, \sigma_{\omega_0}^2\right)$.

In the single-carrier scenario, the transmission of this complex variable over the Gaussian quantum channel $\mathcal{N}$ can be characterized by the $T\left(\mathcal{N}\right)$ normalized complex transmittance variable

$$T\left(\mathcal{N}\right) = \mathrm{Re}\,T\left(\mathcal{N}\right) + \mathrm{i}\,\mathrm{Im}\,T\left(\mathcal{N}\right) \in \mathcal{C}, \tag{1}$$

where $0 \leq \mathrm{Re}\,T\left(\mathcal{N}\right) \leq 1/\sqrt{2}$ stands for the transmission of the position quadrature, $0 \leq \mathrm{Im}\,T\left(\mathcal{N}\right) \leq 1/\sqrt{2}$ is the transmission of the momentum quadrature, with relation

$$\operatorname{Re} T(\mathcal{N}) = \operatorname{Im} T(\mathcal{N}) \tag{2}$$

by our convention. The $0 \le |T(\mathcal{N})| \le 1$ magnitude of the $T(\mathcal{N})$ complex variable is

$$|T(\mathcal{N})| = \sqrt{\operatorname{Re} T(\mathcal{N})^2 + \operatorname{Im} T(\mathcal{N})^2} = \sqrt{2} \operatorname{Re} T(\mathcal{N}) \in \mathbb{R} \tag{3}$$

and the squared magnitude of $T(\mathcal{N})$ is

$$|T(\mathcal{N})|^2 = \operatorname{Re} T(\mathcal{N})^2 + \operatorname{Im} T(\mathcal{N})^2 = 2 \operatorname{Re} T(\mathcal{N})^2 \in \mathbb{R}, \tag{4}$$

where $0 \le |T(\mathcal{N})|^2 \le 1$. Assuming a 0 dB loss, the quadrature transmittance is parameterized with $\operatorname{Re} T(\mathcal{N}) = \operatorname{Im} T(\mathcal{N}) = \frac{1}{\sqrt{2}}$ and

$$|T(\mathcal{N})| = |T(\mathcal{N})|^2 = 1. \tag{5}$$

At a given input *x*, the channel output *y* can be expressed as

$$y = T(\mathcal{N}) x + \Delta, \tag{6}$$

where

$$\Delta \in \mathcal{C}\mathbb{N}\left(0, \sigma_{\Delta}^2\right), \; \sigma_{\Delta}^2 = \mathbb{E}\left[|\Delta|^2\right], \tag{7}$$

models the Gaussian noise of the quantum channel (also a zero-mean, symmetric circular complex Gaussian random variable), with independent quadrature components $\Delta_x \in \mathbb{N}\left(0, \sigma_{\mathcal{N}}^2\right)$, $\Delta_p \in \mathbb{N}\left(0, \sigma_{\mathcal{N}}^2\right)$.

This Gaussian quantum channel is equipped with a capacity of

$$C(\mathcal{N}) = \log_2\left(1 + \frac{\sigma_{\omega_0}^2 |T(\mathcal{N})|^2}{\sigma_{\mathcal{N}}^2}\right), \tag{8}$$

where $\sigma_{\omega_0}^2$ is the modulation variance (single-carrier) of the input Gaussian signal.

In the multicarrier case, the Gaussian quantum channel is divided into *n* Gaussian sub-channels $\mathcal{N}_i$, $i = 1 \ldots n$, each with an independent noise variance $\sigma_{\mathcal{N}_i}^2$, each for the transmission of a continuous variable subcarrier $|\phi_i\rangle$, which leads to the output for the *i*-th sub-channel:

$$y_i = T(\mathcal{N}_i) x_i + \Delta_i, \; i = 1 \ldots n, \tag{9}$$

where $T(\mathcal{N}_i) \in \mathcal{C}$, $\Delta_i \in \mathcal{C}\mathbb{N}\left(0, \sigma_{\Delta_i}^2\right)$, and the resulting transmission capacity is

$$C(\mathcal{N}) = \max_{\forall i} \sum_{i=1}^{n} \log_2\left(1 + \frac{\sigma_{\omega}^2 |T(\mathcal{N}_i)|^2}{\sigma_{\mathcal{N}_i}^2}\right), \tag{10}$$

where

$$\sigma_{\omega}^2 = \frac{1}{n} \sum\nolimits_{i=1}^{n} \sigma_{\omega_i}^2 = \sigma_{\omega_0}^2 \tag{11}$$

is the average modulation variance of the *i*-th Gaussian subcarrier CV transmitted via the *i*-th Gaussian sub-channel.

At this point, the capacity formulas of (8) and (10) require some clarification. Assuming a Gaussian quantum channel, one can find two different capacity formulas for the real dimension and the complex dimension. The reason is as follows.

The noise is independent on the real and imaginary parts (i.e., on the position and momentum quadratures), and each use of the complex Gaussian channel is in particular analogous to two uses of the real Gaussian channel. From this distinction, two different types of capacity formulas can be derived for the same Gaussian channel, i.e., the *real-dimension* capacity and the *complex-dimension* capacity.

The real dimension capacity of an AWGN is

$$C\left(\mathcal{N}\right) = \tfrac{1}{2}\log_2\left(1 + \frac{\sigma_{\omega_0}^2\left|T\left(\mathcal{N}\right)\right|^2}{\sigma_{\mathcal{N}}^2}\right), \tag{12}$$

while the complex dimension capacity is precisely

$$C\left(\mathcal{N}\right) = \log_2\left(1 + \frac{\sigma_{\omega}^2\left|T\left(\mathcal{N}\right)\right|^2}{\sigma_{\mathcal{N}}^2}\right). \tag{13}$$

In (13) the use of the complex domain is justified by the fact that circular symmetric complex Gaussian random variables will be transmitted through the Gaussian quantum channel.

The SNR of the channel is

$$\mathrm{SNR} = \frac{\sigma_{\omega_0}^2\left|T\left(\mathcal{N}\right)\right|^2}{\sigma_{\mathcal{N}}^2}. \tag{14}$$

For further information see [23].

3. MULTICARRIER QUADRATURE DIVISION MODULATION

In terms of the CV scenario, by a convention the $\left|x\right\rangle$ position quadrature could be used as a computational basis. We will also do this throughout. (The continuous-variable quantum Fourier transformation will be abbreviated as CVQFT.)

Let the Gaussian variable be

$$g\left(x\right) = \frac{1}{\sigma\sqrt{2\pi}}e^{\frac{-x^2}{2\sigma^2}},\ x \in \mathbb{N}\left(0,\sigma^2\right), \tag{15}$$

where $\int_{-\infty}^{\infty} g\left(x\right)dx = 1$. The Fourier transform of (15) is expressed as

$$F\left(g\left(x\right)\right) = G\left(\omega\right) = e^{\frac{-\omega^2\sigma^2}{2}},\ \omega \in \mathbb{N}\left(0,\sigma^2\right). \tag{16}$$

Between the Fourier transform $F\left(x\right)$ and the inverse Fourier transform function $F^{-1}\left(\omega\right)$, the connection is as follows [7-8]:

$$F\left(x\right) = \int_{-\infty}^{\infty} F^{-1}\left(\omega\right)e^{-\mathrm{i}x\omega}d\omega, \tag{17}$$

where

$$F^{-1}\left(\omega\right) = \frac{1}{2\pi}\int_{-\infty}^{\infty} F\left(x\right)e^{\mathrm{i}x\omega}dx. \tag{18}$$

For an *n*-dimensional Gaussian random vector $\mathbf{g} \in \left(0,\mathbf{K}_{\mathbf{g}}\right)$, $\mathbf{g} = \left(g_1,,g_n\right)^T$, where $\mathbf{K}_{\mathbf{g}} = \mathbb{E}\left[\mathbf{g}\mathbf{g}^T\right]$ is the covariance matrix, the Fourier transform and its inverse:

$$F\left(\mathbf{g}\right)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\ldots\int_{-\infty}^{\infty}F^{-1}\left(\mathbf{w}\right)e^{-\mathrm{i}\mathbf{g}\cdot\mathbf{w}}d\mathbf{w}, \tag{19}$$

where $\mathbf{w}\in\left(0,\mathbf{K}_{\mathbf{w}}\right)$ is a *n*-dimensional Gaussian random vector with covariance matrix $\mathbf{K}_{\mathbf{w}}=\mathbb{E}\left[\mathbf{w}\mathbf{w}^{T}\right]$, and

$$F^{-1}\left(\mathbf{w}\right)=\frac{1}{\left(2\pi\right)^{n}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\ldots\int_{-\infty}^{\infty}F\left(\mathbf{g}\right)e^{\mathrm{i}\mathbf{g}\cdot\mathbf{w}}d\mathbf{g}\,. \tag{20}$$

Proposition 1. *The σ_{F}^{2} variance of a Gaussian subcarrier CV $\left|\phi_{i}\right\rangle$ is the reciprocal of $\sigma_{\omega_{0}}^{2}$, $\sigma_{F}^{2}=\frac{1}{\sigma_{\omega_{0}}^{2}}$, where $\sigma_{\omega_{0}}^{2}$ is the single-carrier modulation variance.*

Proof.
First, we propose the CVQFT operation acting on the continuous variables, and then we rewrite it as a zero-mean, circular symmetric complex Gaussian random variable [23].
Assuming $\left|x\right\rangle$ position computational basis, function $F\left(\cdot\right)$ acts on the coherent input $\left|\varphi_{i}\right\rangle$ as follows [1]:

$$F\left(\left|\varphi_{i}\right\rangle\right)=F\left(\left\langle x|\varphi_{i}\right\rangle\right)\to\left\langle p|\varphi_{i}\right\rangle, \tag{21}$$

where

$$\left\langle x|\varphi_{i}\right\rangle=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\left\langle p|\varphi_{i}\right\rangle dpe^{\mathrm{i}px}\,, \tag{22}$$

and

$$\left\langle p|\varphi_{i}\right\rangle=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\left\langle x|\varphi_{i}\right\rangle dxe^{-\mathrm{i}px} \tag{23}$$

wavefunctions in the position space *x*, and momentum space *p* for the state $\left|\varphi_{i}\right\rangle$, respectively. The notation $\left\langle x|\psi\right\rangle$ stands for the inner product [1], which can be rewritten as

$$\left\langle x|\psi\right\rangle=\int_{-\infty}^{\infty}f\left(x-x'\right)\psi\left(x'\right)dx'\,, \tag{24}$$

where $f\left(x-x'\right)=\left\langle x|x'\right\rangle$ and $\psi\left(x\right)=\left\langle x|\psi\right\rangle$. Assuming a complete set of orthonormal wavefunctions $\left\{\varphi_{n}\right\}$ [1], the arbitrary wavefunction ψ is as $\psi=\sum_{n}c_{i}\varphi_{i}$, from which

$$\psi\left(q\right)=\int_{-\infty}^{\infty}c\left(p\right)u\left(p;q\right)dp\,, \tag{25}$$

where

$$\begin{aligned}c\left(p\right)&=\left\langle u\left(p;q\right),\psi\left(q\right)\right\rangle\\&=\left\langle u\left(p;q\right),\int_{-\infty}^{\infty}c\left(p\right)u\left(p;q\right)dp\right\rangle\\&=\int_{-\infty}^{\infty}f\left(p-p'\right)c\left(p'\right)dp'.\end{aligned} \tag{26}$$

The inverse function of (21) is defined as

$$F^{-1}\left(\left\langle p\middle|\varphi_i\right\rangle\right)=\left\langle x\middle|\varphi_i\right\rangle. \tag{27}$$

A Gaussian modulated coherent state $\left|\varphi_i\right\rangle=\left|x_i+\mathrm{i}p_i\right\rangle$, where $x_i\in\mathbb{N}\left(0,\sigma_{\omega_0}^2\right)$, $p_i\in\mathbb{N}\left(0,\sigma_{\omega_0}^2\right)$ are the position and momentum quadratures, respectively; can be rewritten as a zero-mean, circular symmetric complex Gaussian random variable $z_i\in\mathcal{C}\mathbb{N}\left(0,\sigma_{\omega_{z_i}}^2\right)$, $\sigma_{\omega_{z_i}}^2=\left[\mathbb{E}\left|z_i\right|^2\right]$, as

$$z_i=x_i+\mathrm{i}p_i, \tag{28}$$

where $x_i\in\mathbb{N}\left(0,\sigma_{\omega_0}^2\right)$, $p_i\in\mathbb{N}\left(0,\sigma_{\omega_0}^2\right)$ are i.i.d. zero-mean Gaussian random variables. As follows,

$$\left|\varphi_i\right\rangle=\left|z_i\right\rangle. \tag{29}$$

The variable $e^{\mathrm{i}\varphi_i}z_i$ has the same distribution of z_i for any φ_i, i.e.,

$$\mathbb{E}\left[z_i\right]=\mathbb{E}\left[e^{\mathrm{i}\varphi_i}z_i\right]=\mathbb{E}e^{\mathrm{i}\varphi_i}\left[z_i\right]\text{ and }\sigma_{z_i}^2=\mathbb{E}\left[\left|z_i\right|^2\right]. \tag{30}$$

The density of z_i is

$$f\left(z_i\right)=\frac{1}{2\pi\sigma_{\omega_0}^2}e^{\frac{-\left(\left|z_i\right|^2\right)}{2\sigma_{\omega_0}^2}}=f\left(x_i,p_i\right)=\frac{1}{2\pi\sigma_{\omega_0}^2}e^{\frac{-\left(x_i{}^2+p_i{}^2\right)}{2\sigma_{\omega_0}^2}}, \tag{31}$$

where $\left|z_i\right|=\sqrt{x_i^2+p_i^2}$ is the magnitude, which is a Rayleigh random variable with density

$$f\left(\left|z_i\right|\right)=\frac{\left|z_i\right|}{\sigma_{\omega_{z_i}}^2}e^{\frac{-\left|z_i\right|^2}{2\sigma_{\omega_{z_i}}^2}},\left|z_i\right|\geq 0, \tag{32}$$

while the $\left|z_i\right|^2=x_i^2+p_i^2$ squared magnitude is exponentially distributed with density

$$f\left(\left|z_i\right|^2\right)=\frac{1}{\sigma_{\omega_{z_i}}^2}e^{\frac{-\left|z_i\right|^2}{\sigma_{\omega_{z_i}}^2}},\left|z_i\right|^2\geq 0. \tag{33}$$

The *i*-th *subcarrier* CV is defined as

$$\left|\phi_i\right\rangle=\left|\mathrm{IFFT}\left(z_i\right)\right\rangle=\left|F^{-1}\left(z_i\right)\right\rangle=\left|d_i\right\rangle, \tag{34}$$

where IFFT stands for the Inverse Fast Fourier Transform, and subcarrier continuous variable $\left|\phi_i\right\rangle$ in (34) is also a zero-mean, circular symmetric complex Gaussian random variable $d_i\in\mathcal{C}\mathbb{N}\left(0,\sigma_{d_i}^2\right)$, $\sigma_{d_i}^2=\mathbb{E}\left[\left|d_i\right|^2\right]$, $d_i=x_{d_i}+\mathrm{i}p_{d_i}$, where $x_{d_i}\in\mathbb{N}\left(0,\sigma_{\omega_F}^2\right)$, $p_{d_i}\in\mathbb{N}\left(0,\sigma_{\omega_F}^2\right)$ are i.i.d. zero-mean Gaussian random variables, and $\sigma_{\omega_F}^2$ is the variance of the Fourier transformed Gaussian signal.

The inverse of (34) results the single-carrier CV from the subcarrier CV as follows:

$$\left|\varphi_i\right\rangle=\mathrm{CVQFT}\left(\left|\phi_i\right\rangle\right)=F\left(\left|d_i\right\rangle\right)=\left|F\left(F^{-1}\left(z_i\right)\right)\right\rangle=\left|z_i\right\rangle, \tag{35}$$

where CVQFT is the continuous-variable QFT operation.

Let us to derive the Fourier transform of the Gaussian input [7-8]. First, we rewrite (31) in the position basis *x* as $g(x) = \frac{1}{\sqrt{2\pi\sigma_{\omega_0}^2}} e^{\frac{-x^2}{a^2}}$, where $a^2 = 2\sigma_{\omega_0}^2$. Then, the Fourier transformed signal $G(p)$ is precisely evaluated as

$$\begin{aligned} F(g(x)) &= G(p) \\ &= \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{2\pi\sigma_{\omega_0}^2}} \int_{-\infty}^{\infty} g(x) e^{-\mathrm{i}px} dx \\ &= \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{2\pi\sigma_{\omega_0}^2}} \int_{-\infty}^{\infty} e^{\frac{-x^2}{a^2}} e^{-\mathrm{i}px} dx \\ &= \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{2\pi\sigma_{\omega_0}^2}} e^{\frac{-a^2p^2}{4}} \int_{-\infty}^{\infty} e^{-\frac{\left(x+\frac{\mathrm{i}a^2p}{2}\right)^2}{a^2}} dx \\ &= \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{2\pi\sigma_{\omega_0}^2}} e^{-\frac{\sigma_{\omega_0}^2 p^2}{2}} = \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{2\pi\sigma_{\omega_0}^2}} e^{-\frac{p^2}{2\sigma_F^2}} \\ &= \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{\frac{2\pi}{\sigma_F^2}}} e^{-\frac{p^2}{2\sigma_F^2}}. \end{aligned} \tag{36}$$

The $G(p)$ Fourier transform of the Gaussian signal $g(x)$ is also Gaussian in the conjugate-variable space, with variance $\sigma_F^2 = \frac{1}{\sigma_{\omega_0}^2}$. In other words, the $F(|\varphi_i\rangle)$ Fourier transform of the Gaussian coherent state $|\varphi_i\rangle$ is also a Gaussian state. Since the position and momentum quadratures are Fourier-transform pairs, it follows that as the modulation variance σ_ω^2 of the input Gaussian signal increases, the variance σ_F^2 of the Fourier transformed signal decreases. From the uncertainty principle, it can be concluded that if $\Delta x = \sigma_{\omega_0}$ (i.e., the uncertainty of the Gaussian is proportional to the standard deviation) and $\Delta p = \frac{1}{\sigma_{\omega_0}}$, then $\Delta x \Delta p = 1$.

■

Theorem 1. *The AMQD divides the Gaussian channel $\mathcal{N}$ into n Gaussian sub-channels $\mathcal{N}_i$, $i = 1,\ldots,n$, with independent noise variances $\sigma_{\mathcal{N}_i}^2$, where $\frac{1}{n}\sum_{i=1}^{n} \sigma_{\mathcal{N}_i}^2 = \sigma_{\mathcal{N}}^2$.*

Proof.

Let *n* is the number of Alice's input Gaussian states. The *n* input coherent states are modeled by an *n*-dimensional, zero-mean, circular symmetric complex random Gaussian vector

$$\mathbf{z} = \mathbf{x} + \mathrm{i}\mathbf{p} = \left(z_1,\ldots,z_n\right)^T \in \mathcal{CN}\left(0,\mathbf{K_z}\right), \tag{37}$$

where each z_i can be modeled as a zero-mean, circular symmetric complex Gaussian random variable $z_i \in \mathcal{CN}\left(0,\sigma_{\omega_{z_i}}^2\right)$, $z_i = x_i + \mathrm{i}p_i$.

The real and imaginary variables (i.e., the position and momentum quadratures) formulate *n*-dimensional real Gaussian random vectors, $\mathbf{x} = \left(x_1,\ldots,x_n\right)^T$ and $\mathbf{p} = \left(p_1,\ldots,p_n\right)^T$, with zero-mean Gaussian random variables

$$f\left(x_i\right) = \frac{1}{\sigma_{\omega_0}\sqrt{2\pi}} e^{\frac{-x_i^2}{2\sigma_{\omega_0}^2}},\; f\left(p_i\right) = \frac{1}{\sigma_{\omega_0}\sqrt{2\pi}} e^{\frac{-p_i^2}{2\sigma_{\omega_0}^2}}, \tag{38}$$

where $\sigma_{\omega_0}^2$ is the stands for single-carrier modulation variance (precisely, the variance of the real and imaginary components of z_i), while $\mathbf{K_z}$ is the $n \times n$ Hermitian covariance matrix of $\mathbf{z}$:

$$\mathbf{K_z} = \mathbb{E}\left[\mathbf{z}\mathbf{z}^\dagger\right], \tag{39}$$

where $\mathbf{z}^\dagger$ is the adjoint of $\mathbf{z}$. For vector $\mathbf{z}$,

$$\mathbb{E}\left[\mathbf{z}\right] = \mathbb{E}\left[e^{\mathrm{i}\gamma}\mathbf{z}\right] = \mathbb{E}e^{\mathrm{i}\gamma}\left[\mathbf{z}\right] \tag{40}$$

holds, and

$$\mathbb{E}\left[\mathbf{z}\mathbf{z}^T\right] = \mathbb{E}\left[e^{\mathrm{i}\gamma}\mathbf{z}\left(e^{\mathrm{i}\gamma}\mathbf{z}\right)^T\right] = \mathbb{E}e^{\mathrm{i}2\gamma}\left[\mathbf{z}\mathbf{z}^T\right], \tag{41}$$

for any $\gamma \in \left[0, 2\pi\right]$. The density of $\mathbf{z}$ is as follows (if $\mathbf{K_z}$ is invertible):

$$f\left(\mathbf{z}\right) = \frac{1}{\pi^n \det \mathbf{K_z}} e^{-\mathbf{z}^\dagger \mathbf{K_z}^{-1}\mathbf{z}}. \tag{42}$$

A *n*-dimensional Gaussian random vector is expressed as $\mathbf{x} = \mathbf{A}\mathbf{s}$, where $\mathbf{A}$ is an (invertible) linear transform from $\mathbb{R}^n$ to $\mathbb{R}^n$, and $\mathbf{s}$ is an *n*-dimensional standard Gaussian random vector $\mathbb{N}\left(0,1\right)_n$. This vector is characterized by its covariance matrix $\mathfrak{C}\left(\mathbf{x}\right) = \mathbb{E}\left[\mathbf{x}\mathbf{x}^T\right] = \mathbf{A}\mathbf{A}^T$, as

$$\mathbf{x} = \frac{1}{\left(\sqrt{2\pi}\right)^n \sqrt{\det\left(\mathbf{A}\mathbf{A}^T\right)}} e^{-\frac{\mathbf{x}^T\mathbf{x}}{2\left(\mathbf{A}\mathbf{A}^T\right)}}. \tag{43}$$

The Fourier transformation $F\left(\cdot\right)$ of the *n*-dimensional Gaussian random vector $\mathbf{v} = \left(v_1, \ldots, v_n\right)^T$ results in the *n*-dimensional Gaussian random vector $\mathbf{m} = \left(m_1, \ldots, m_n\right)^T$:

$$\mathbf{m} = F\left(\mathbf{v}\right) = e^{\frac{-\mathbf{m}^T\mathbf{A}\mathbf{A}^T\mathbf{m}}{2}} = e^{\frac{-\sigma_{\omega_0}^2\left(m_1^2+\ldots+m_n^2\right)}{2}}. \tag{44}$$

In the first step of AMQD, Alice applies the inverse FFT operation to vector $\mathbf{z}$ (see (37)), which results in an *n*-dimensional zero-mean, circular symmetric complex Gaussian random vector $\mathbf{d}$, $\mathbf{d} \in \mathcal{CN}\left(0, \mathbf{K_d}\right)$, $\mathbf{d} = \left(d_1, \ldots, d_n\right)^T$, precisely as

$$\mathbf{d} = F^{-1}\left(\mathbf{z}\right) = e^{\frac{\mathbf{d}^T\mathbf{A}\mathbf{A}^T\mathbf{d}}{2}} = e^{\frac{\sigma_{\omega_0}^2\left(d_1^2+\ldots+d_n^2\right)}{2}}, \tag{45}$$

where $d_i = x_{d_i} + \mathrm{i}p_{d_i}$, $d_i \in \mathcal{CN}\left(0, \sigma_{d_i}^2\right)$, and the position and momentum quadratures of $\left|\phi_i\right\rangle$ are i.i.d. Gaussian random variables

$$x_{d_i} \in \mathbb{N}\left(0, \sigma_F^2\right),\; p_{d_i} \in \mathbb{N}\left(0, \sigma_F^2\right), \tag{46}$$

where $\mathbf{K_d} = \mathbb{E}\left[\mathbf{dd}^{\dagger}\right]$, $\mathbb{E}\left[\mathbf{d}\right] = \mathbb{E}\left[e^{\mathrm{i}\gamma}\mathbf{d}\right] = \mathbb{E}e^{\mathrm{i}\gamma}\left[\mathbf{d}\right]$, and $\mathbb{E}\left[\mathbf{dd}^{T}\right] = \mathbb{E}\left[e^{\mathrm{i}\gamma}\mathbf{d}\left(e^{\mathrm{i}\gamma}\mathbf{d}\right)^{T}\right] = \mathbb{E}e^{\mathrm{i}2\gamma}\left[\mathbf{dd}^{T}\right]$ for any $\gamma \in \left[0, 2\pi\right]$.

In the next step, Alice modulates the coherent Gaussian subcarriers as follows:

$$\left|\phi_i\right\rangle = \left|d_i\right\rangle = \left|F^{-1}\left(z\right)\right\rangle. \tag{47}$$

The result of (45) defines *n*, independent $\mathcal{N}_i$ Gaussian sub-channels, each with noise variance $\sigma_{\mathcal{N}_i}^2$, one for each subcarrier coherent state $\left|\phi_i\right\rangle$. After the CV subcarriers are transmitted through the noisy channel, Bob applies the CVQFT, which results him the noisy version $\left|\varphi_i'\right\rangle = \left|z_i'\right\rangle$ of Alice's input z_i.

On Bob's side, the received system $\mathbf{y}$ is an *n*-dimensional zero-mean, circular symmetric complex Gaussian random vector $\mathbf{y} \in \mathcal{CN}\left(0, \mathbb{E}\left[\mathbf{yy}^{\dagger}\right]\right)$. The *m*-th element of vector $\mathbf{y}$ is y_m, expressed as follows:

$$\begin{aligned} y_m &= F\left(\mathbf{T}\left(\mathcal{N}\right)\right)z_m + F\left(\Delta\right) \\ &= F\left(\mathbf{T}\left(\mathcal{N}\right)\right)F\left(F^{-1}\left(z_m\right)\right) + F\left(\Delta\right) \\ &= \sum\nolimits_n F\left(T_i\left(\mathcal{N}_i\right)\right)F\left(d_i\right) + F\left(\Delta_i\right), \end{aligned} \tag{48}$$

where

$$\mathbf{T}\left(\mathcal{N}\right) = \left[T_1\left(\mathcal{N}_1\right), \ldots, T_n\left(\mathcal{N}_n\right)\right]^T \in \mathcal{C}^n, \tag{49}$$

where

$$T_i\left(\mathcal{N}_i\right) = \mathrm{Re}\left(T_i\left(\mathcal{N}_i\right)\right) + \mathrm{i}\,\mathrm{Im}\left(T_i\left(\mathcal{N}_i\right)\right) \in \mathcal{C}, \tag{50}$$

is a complex variable, which quantifies the position and momentum quadrature transmission (i.e., gain) of the *i*-th Gaussian sub-channel $\mathcal{N}_i$, in the phase space $\mathcal{S}$, with real and imaginary parts $0 \leq \mathrm{Re}\,T_i\left(\mathcal{N}_i\right) \leq 1/\sqrt{2}$, $0 \leq \mathrm{Im}\,T_i\left(\mathcal{N}_i\right) \leq 1/\sqrt{2}$. The $T_i\left(\mathcal{N}_i\right)$ variable has a magnitude of $\left|T_i\left(\mathcal{N}_i\right)\right| = \sqrt{\mathrm{Re}\,T_i\left(\mathcal{N}_i\right)^2 + \mathrm{Im}\,T_i\left(\mathcal{N}_i\right)^2} \in \mathbb{R}$, where $\mathrm{Re}\,T_i\left(\mathcal{N}_i\right) = \mathrm{Im}\,T_i\left(\mathcal{N}_i\right)$, by our convention.

The CVQFT-transformed channel transmission parameters are (upscaled by $\sqrt{n}$) expressed by the complex vector:

$$\begin{aligned} F\left(\mathbf{T}\left(\mathcal{N}\right)\right) &= \sum_{i=1}^{n} F\left(T_i\left(\mathcal{N}_i\right)\right) \\ &= \sum_{i=1}^{n}\sum_{k=1}^{n} T_k e^{\frac{-\mathrm{i}2\pi ik}{n}} \in \mathcal{C}^n, \end{aligned} \tag{51}$$

where $F\left(\mathbf{T}\left(\mathcal{N}\right)\right)$ is the Fourier transform of (49). The *n*-dimensional $F\left(\Delta\right)$ complex vector is evaluated as

$$F\left(\Delta\right) = e^{\frac{-F\left(\Delta\right)^T \mathfrak{C}\left(F\left(\Delta\right)\right)F\left(\Delta\right)}{2}} = e^{\frac{-\left(F\left(\Delta_1\right)^2\sigma_{\mathcal{N}_1}^2 + \ldots + F\left(\Delta_n\right)^2\sigma_{\mathcal{N}_n}^2\right)}{2}}, \tag{52}$$

which is the Fourier transform of the *n*-dimensional zero-mean, circular symmetric complex Gaussian noise vector $\Delta \in \mathcal{CN}\left(0, \sigma_{\Delta}^2\right)_n$,

$$\Delta = \left(\Delta_1,\ldots,\Delta_n\right)^T \in \mathcal{C}\mathbb{N}\left(0,\mathfrak{C}\left(\Delta\right)\right), \tag{53}$$

where $\mathfrak{C}\left(\Delta\right) = \mathbb{E}\left[\Delta\Delta^\dagger\right]$, with independent, zero-mean Gaussian random components $\Delta_{x_i} \in \mathbb{N}\left(0,\sigma^2_{\mathcal{N}_i}\right)$, $\Delta_{p_i} \in \mathbb{N}\left(0,\sigma^2_{\mathcal{N}_i}\right)$ with variance $\sigma^2_{\mathcal{N}_i}$, for each Δ_i, which identifies the Gaussian noise of the *i*-th sub-channel $\mathcal{N}_i$ on the quadrature components in the phase space $\mathcal{S}$.

The CVQFT-transformed noise vector in (52) can be rewritten as

$$F\left(\Delta\right) = \left(F\left(\Delta_1\right),\ldots,F\left(\Delta_n\right)\right)^T, \tag{54}$$

with independent components $F\left(\Delta_{x_i}\right) \in \mathbb{N}\left(0,\sigma^2_{F\left(\mathcal{N}_i\right)}\right)$ and $F\left(\Delta_{p_i}\right) \in \mathbb{N}\left(0,\sigma^2_{F\left(\mathcal{N}_i\right)}\right)$ on the quadratures, for each $F\left(\Delta_i\right)$. It also defines an *n*-dimensional zero-mean, circular symmetric complex Gaussian random vector $F\left(\Delta\right) \in \mathcal{C}\mathbb{N}\left(0,\mathfrak{C}\left(F\left(\Delta\right)\right)\right)$ with a covariance matrix

$$\mathfrak{C}\left(F\left(\Delta\right)\right) = \mathbb{E}\left[F\left(\Delta\right)F\left(\Delta\right)^\dagger\right], \tag{55}$$

and the noise variance $\sigma^2_{F\left(\mathcal{N}\right)}$ of the independent Fourier-transformed quadratures is evaluated as

$$\begin{aligned} \sigma^2_{F\left(\mathcal{N}\right)}\mathbf{I}_{n\times n} &= \tfrac{1}{n}\sum_{i=1}^{n}\sigma^2_{F\left(\mathcal{N}_i\right)} \\ &= \sigma^2_{F\left(\mathcal{N}\right)} = \tfrac{1}{\sigma^2_{\mathcal{N}}}, \end{aligned} \tag{56}$$

where $\sigma^2_{\mathcal{N}}$ is the noise variance of the Gaussian quantum channel $\mathcal{N}$, $\mathbf{I}_{n\times n}$ is the $n \times n$ identity matrix, hence $F\left(\Delta_i\right) \in \mathcal{C}\mathbb{N}\left(0,\sigma^2_{F\left(\Delta_i\right)}\right)$, and $\sigma^2_{F\left(\Delta_i\right)} = \mathbb{E}\left[\left|F\left(\Delta_i\right)\right|^2\right]$, with independent noise variance $\sigma^2_{F\left(\mathcal{N}\right)}$ on the quadrature components (For simplicity, the notation of $\mathbf{I}_{n\times n}$ will be omitted from the description.). The LHS of (55) is justified by Proposition 1 and (36). It is an important corollary regarding the noise variance of the Fourier-transformed vector (54).

An AMQD *block* is formulated from *n* Gaussian subcarrier continuous variables, as follows:

$$\mathbf{y}\left[j\right] = F\left(\mathbf{T}\left(\mathcal{N}\right)\right)F\left(\mathbf{d}\right)\left[j\right] + F\left(\Delta\right)\left[j\right],\ j = 1,\ldots,n, \tag{57}$$

where *j* is the index of the AMQD block, $F\left(\mathbf{T}\left(\mathcal{N}\right)\right)$ is defined in (51), $F\left(\mathbf{d}\right) = F\left(F^{-1}\left(\mathbf{z}\right)\right)$, where $F^{-1}\left(\mathbf{z}\right)$ is shown in (45), while

$$\begin{aligned} \mathbf{y}\left[j\right] &= \left(y_1\left[j\right],\ldots,y_n\left[j\right]\right)^T, \\ F\left(\mathbf{d}\right)\left[j\right] &= \left(F\left(d_1\right)\left[j\right],\ldots,F\left(d_n\right)\left[j\right]\right)^T, \\ F\left(\Delta\right)\left[j\right] &= \left(F\left(\Delta_1\right)\left[j\right],\ldots,F\left(\Delta_n\right)\left[j\right]\right)^T. \end{aligned} \tag{58}$$

The squared magnitude

$$\tau = \left\|F\left(\mathbf{d}\right)\left[j\right]\right\|^2 \tag{59}$$

identifies an exponentially distributed variable, with density $f\left(\tau\right) = \left(1/2\sigma_\omega^{2n}\right)e^{-\tau/2\sigma_\omega^2}$, and from the Parseval theorem [6] it follows that

$$\mathbb{E}\left[\tau\right] \leq n 2\sigma_{\omega}^{2}, \tag{60}$$

while the average quadrature modulation variance is

$$\sigma_{\omega}^{2} = \frac{1}{n}\sum_{i=1}^{n}\sigma_{\omega_i}^{2} = \sigma_{\omega_0}^{2}, \tag{61}$$

where $\sigma_{\omega_i}^{2}$ is the modulation variance of the quadratures of the subcarrier $\left|\phi_i\right\rangle$ transmitted by sub-channel $\mathcal{N}_i$.
The transformed vector $\mathbf{y}$ in (48) and (58) clearly demonstrates that the physical Gaussian channel is, in fact, divided into *n* Gaussian quantum channels with independent noise variances. Each $\mathcal{N}_i$ Gaussian sub-channel is dedicated for the transmission of one Gaussian subcarrier CV from the *n* subcarrier CVs.

■

For the further details see [23].

3.1 Gaussian noise of the Gaussian sub-channels

Eve's optimal entangling cloner attack [2] in the multicarrier modulation setting is described as follows. Let the quadratures of the *i*-th subcarrier $\left|\phi_i\right\rangle$ transmitted by $\mathcal{N}_i$ be

$$\left(x_{in,i}, p_{in,i}\right),\ x_{in,i} \in \mathbb{N}\left(0, \sigma_{\omega_i}^{2}\right),\ p_{in,i} \in \mathbb{N}\left(0, \sigma_{\omega_i}^{2}\right), \tag{62}$$

where $\sigma_{\omega_i}^{2}$ is the modulation variance of the CVQFT transformed subcarrier CVs. Eve, equipped with *n* EPR ancilla pairs $\left|\Psi_{EB}\right\rangle^{\otimes n}$ each with variance W_i, and prepares her E_i as follows:

$$\left(x_{E,i}, p_{E,i}\right),\ x_{E,i} \in \mathbb{N}\left(0, \sigma_{\omega_i}^{2} + \sigma_{\mathcal{N}_i}^{2}\right),\ p_{E,i} \in \mathbb{N}\left(0, \sigma_{\omega_i}^{2} + \sigma_{\mathcal{N}_i}^{2}\right), \tag{63}$$

The part B_i of is sent back to $\mathcal{N}_i$, which system has the following quadratures:

$$\left(x_{B,i}, p_{B,i}\right),\ x_{B,i} \in \mathbb{N}\left(0, \sigma_{\omega_i}^{2} + \sigma_{\mathcal{N}_i}^{2}\right),\ p_{B,i} \in \mathbb{N}\left(0, \sigma_{\omega_i}^{2} + \sigma_{\mathcal{N}_i}^{2}\right). \tag{64}$$

The simplified view of Eve's Gaussian attack in the multicarrier scenario is summarized in Fig. 2. Eve attacks each sub-channel with a BS with transmittance $T_{Eve,i} \in \mathcal{C}$, $0 < \left|T_{Eve,i}\right|^{2} < 1$, and an entangled ancilla $\left|\Psi_{EB}\right\rangle$ with variance *W*. The quadratures of the *i*-th sub-channel are $\left(x_{in,i}, p_{in,i}\right)$, Eve's quadratures are $\left(x_{E,i}, p_{E,i}\right)$, Bob's received noisy quadratures are $\left(x'_{in,i}, p'_{in,i}\right)$. Each sub-channel is characterized with a Gaussian noise $\mathbb{N}\left(0, \sigma_{\mathcal{N}_i}^{2}\right)$ on the quadrature components, with independent noise variance $\sigma_{\mathcal{N}_i}^{2}$.

As shown in (53), Eve's optimal Gaussian attacks define an *n*-dimensional zero-mean, circular symmetric complex Gaussian random noise vector. In the AMQD scenario, the appropriate noise vector is given by (52) and (55), as $F\left(\Delta\right) \in \mathcal{CN}\left(0, \mathfrak{C}\left(F\left(\Delta\right)\right)\right)$, and $F\left(\Delta_i\right) \in \mathcal{CN}\left(0, \sigma_{F\left(\Delta_i\right)}^{2}\right)$, respectively. For the security proof of AMQD against optimal Gaussian collective attacks is being presented in Theorem 4. For the further details see [23].

4. ADAPTIVE MODULATION VARIANCE ALLOCATION MECHANISM

The run of the multicarrier quadrature division is sketched as follows. In the initial phase, Alice draws an *n*-dimensional, zero-mean circular symmetric complex Gaussian random vector $\mathbf{z} = \mathbf{x} + \mathrm{i}\mathbf{p} = \left(z_1, \ldots, z_n\right)^{T} \in \mathcal{CN}\left(0, \mathbf{K_z}\right)$,

$z_i = p_i + \mathrm{i}q_i$, and $x_i \in \mathbb{N}\left(0,\sigma_{\omega_0}^2\right)$, $p_i \in \mathbb{N}\left(0,\sigma_{\omega_0}^2\right)$ are i.i.d. Gaussian random variables that identifies the *x* position and *p* momentum quadratures in the phase space $\mathcal{S}$, while $\sigma_{\omega_0}^2$ is the modulation variance (at a single-carrier transmission).

In the next step, Alice applies the inverse FFT on $\mathbf{z}$, that gives her the results of an *n*-dimensional, zero-mean circular symmetric complex Gaussian random vector $\mathbf{d} = \mathbf{x} + \mathrm{i}\mathbf{p} = \left(d_1,\ldots,d_n\right)^T \in \mathcal{C}\mathbb{N}\left(0,\mathbf{K_d}\right)$. According to $\mathbf{d}$, she prepares the $\left|\phi_{1\ldots n}\right\rangle$ Gaussian subcarrier CVs, by modulating with $\sigma_\omega^2 \neq \sigma_{\omega_0}^2$ the position and momentum quadratures, where $\left|\phi_i\right\rangle$ is the *i*-th subcarrier continuous variable. The *n* subcarrier coherent states $\left|\phi_i\right\rangle$ divide the physical Gaussian quantum channel into *n* physical Gaussian quantum channels, each equipped with an independent noise variance $\sigma_{\mathcal{N}_i}^2$.

In the decoding phase, Bob applies the CVQFT unitary operation U on the received noisy Gaussian subcarrier CVs, $\left|\phi_i'\right\rangle$, which results him the noisy coherent state versions of Alice's Gaussian variables, $\left|\varphi_{1\ldots n}'\right\rangle = \left|z_{1\ldots n}'\right\rangle = \left|\mathbf{z}'\right\rangle$, and the Fourier transformed sub-channel noise variance $\sigma_{F(\mathcal{N}_i)}^2$. The CVQFT-transformed $\left|F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2$ transmission parameters of the Gaussian sub-channels are strongly diverse (this will be shown in Section 4), which makes available the use of an *adaptive variance modulation* to improve the tolerable noise and excess noise.

The steps of multicarrier quadrature division modulation are summarized in Fig. 1 [23].

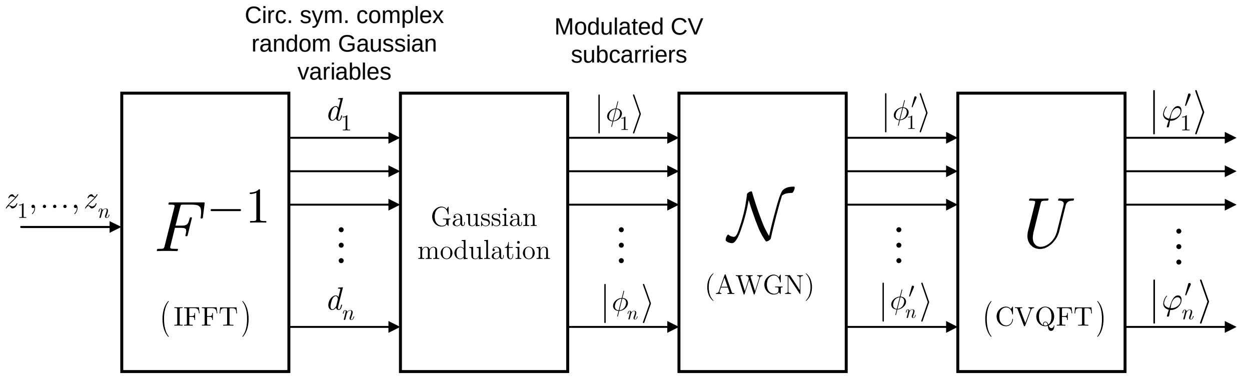

Figure 1. The AMQD modulation scheme. Alice draws an *n*-dimensional, zero-mean, circular symmetric complex Gaussian random vector $\mathbf{z}$, which are then inverse Fourier-transformed by F^{-1}. The resulting vector $\mathbf{d}$ encodes the subcarrier quadratures for the Gaussian modulation. In the decoding, Bob applies the *U* unitary CVQFT on the *n* subcarriers to recover the noisy version of Alice's original variable as a continuous variable in the phase space.

(*Note*: In the two-way protocol, Bob sends the subcarrier CVs to Alice, who generates coupled Gaussian CVs with her BS. The resulting Gaussian subcarrier CV is then sent back to Bob, who applies the CVQFT operation. Alice also applies a CVQFT operation on her system.) The reason behind the improvement is that the dB limits of the transmission over the Gaussian quantum channel can significantly be extended by the Fourier-transformed multicarrier continuous variables.

The modulation variances of each of the $\mathcal{N}_i$ sub-channels (zero or nonzero) are dependent on the value of ν_{Eve}. This parameter is defined as

$$\nu_{Eve} = \tfrac{1}{\lambda}, \tag{65}$$

where λ is the Lagrange multiplier as

$$\lambda = \left|F\left(T_{\mathcal{N}}^*\right)\right|^2 = \tfrac{1}{n}\sum\nolimits_{i=1}^{n}\left|\sum\nolimits_{k=1}^{n} T_k^* e^{\frac{-\mathrm{i}2\pi ik}{n}}\right|^2, \tag{66}$$

where $T_{\mathcal{N}}^{*}$ is the *expected* transmittance of the *n* sub-channels under an optimal Gaussian attack.

From λ, and the $\sigma_{\omega_i}^2$ modulation variances of the $\mathcal{N}_i$ sub-channels, a Lagrangian can be constructed as

$$\mathcal{L}\left(\lambda,\sigma_{\omega_1}^2\ldots\sigma_{\omega_n}^2\right)=\sum_{i=1}^{n}\log_2\left(1+\frac{\sigma_{\omega_i}^2\left|F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2}{\sigma_{\mathcal{N}}^2}\right)-\lambda\sum_{i=1}^{n}\sigma_{\omega_i}^2 . \tag{67}$$

By the Kuhn-Tucker condition [6], [9-10], follows that $\frac{\partial\mathcal{L}}{\partial\sigma_{\omega_i}^2}=0$ if only the *i*-th sub-channel gets a non-zero modulation variance, $\sigma_{\omega_i}^2>0$, while $\frac{\partial\mathcal{L}}{\partial\sigma_{\omega_i}^2}\leq 0$, if the sub-channel gets zero modulation variance, $\sigma_{\omega_i}^2=0$ [6], [9-10].

After some calculations, one gets the following average modulation variance:

$$\sigma_{\omega}^2=\frac{1}{n}\sum_{i=1}^{n}\left(\nu_{Eve}-\frac{\sigma_{\mathcal{N}}^2}{\left|F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2}\right)=\frac{1}{n}\sum_{i=1}^{n}\left(\nu_{Eve}-\nu_i\right). \tag{68}$$

One can readily see that in (68), each sub-channel is allocated by a different modulation variance, depending on the actual value of $\left|F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2$. The reason for this is as follows. Only those $l<n$ sub-channels can transmit information for which $\nu_i<\nu_{Eve}$; otherwise, the channel gets zero modulation variance. (In general, this kind of strategy is called water-filling [6], [9-10].) Since it is not a reasonable assumption in a practical CVQKD that the transmitter would have an *exact* knowledge about the state of each Gaussian sub-channels, at this point we have to introduce a more flexible technique. Our answer is as follows.

In fact, it is not a required condition to calculate with the exact ν_i parameters and modulation variances $\sigma_{\omega_i}^2$ for the sub-channels. A simplified solution exists: give a *constant* modulation variance σ_{ω}^2 for those *l* $\mathcal{N}_i$ sub-channels, for which $\nu_i<\nu_{Eve}$ is satisfied:

$$\sigma_{\omega}^2=\frac{1}{l}\sum_{i=1}^{l}\left(\nu_{Eve}-\frac{\sigma_{\mathcal{N}}^2}{\max_i\left|F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2}\right)=\nu_{Eve}-\min\left(\nu_i\right). \tag{69}$$

It is particular convenient, since at a given ν_{Eve} bound, it is enough to find a given $\max_i\left|F\left(T_{1\ldots l}\left(\mathcal{N}_{1\ldots l}\right)\right)\right|^2$ for those $\mathcal{N}_i$ sub-channels, for which $\nu_i<\nu_{Eve}$ hold.

Particularly, the significance of the adaptive-variance modulation proposed in (69) is crucial for low SNRs, which is precisely the case in a long-distance scenario, since the information transmission capability of the Gaussian sub-channels become very sensitive in the low SNR regimes [4], [6], [9-10]. At low SNRs the constant allocation provides an optimal solution [9-10], because its performance is very close to the exact allocation and can be performed with no exact knowledge about the state of the sub-channels. This is very good news, because the proposed AMQD modulation scheme allocates a constant modulation variance for the good Gaussian sub-channels. For the further details see [23].

The modulation variance adaption scheme is summarized in Fig. 2. The parameter ν_i of the Gaussian sub-channels is depicted in yellow. If ν_i is under a critical limit ν_{Eve}, the channel is assumed to be useful and can be used for information transmission. If $\nu_i<\nu_{Eve}$, Alice allocates a constant modulation variance $\sigma_{\omega_i}^2=\sigma_{\omega}^2$ according to (69), for the Gaussian sub-channel $\mathcal{N}_i$. If $\nu_i\geq\nu_{Eve}$, Alice allocates zero modulation variance for $\mathcal{N}_i$, i.e., $\sigma_{\omega_i}^2=0$ [23].

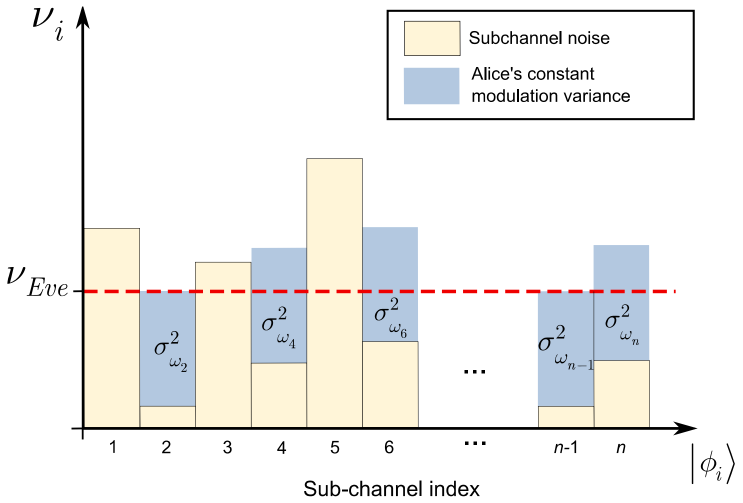

Figure 2. The constant modulation variance allocation mechanism. If the i-th sub-channel $\mathcal{N}_i$ is very noisy, i.e., $\nu_i \geq \nu_{Eve}$, Alice will not use that sub-channel, i.e., the modulation variance $\sigma^2_{\omega_i}$ of $|\phi_i\rangle$ is 0. Only those sub-channels will be used for the transmission for which ν_i is under the critical bound ν_{Eve} (red dashed line). Assuming l sub-channels with $\nu_i < \nu_{Eve}$, the modulation variance for these sub-channels is chosen to be a constant $\sigma^2_{\omega_i} = \nu_{Eve} - \min(\nu_1,\ldots,\nu_n)$, where $\sum_l \sigma^2_{\omega_i} = l\sigma^2_{\omega} < n\sigma^2_{\omega_0}$, and $\sigma^2_{\omega_0}$ is the single-carrier modulation variance.

The AMQD is equipped with all of those properties that allow it to meet the requirements of an experimental protocol, since its real potential is brought to life at very low SNRs. As a fine corollary, the transmission efficiency significantly can be boosted in an experimental long-distance CVQKD scenario [23].

5. CONCLUSIONS

The CVQKD protocols represent one of the most capable practical manifestations of quantum information theory. While the DVQKD protocols cannot be implemented within the framework of current technology, the CVQKD schemes can be established over standard communication networks and practical devices. Besides the attractive properties, the CVQKD schemes have an extreme sensitivity to the channel noise and other loss which allow no to use these protocols with such a high efficiency as it is available for traditional protocols in a traditional telecommunication scenario. To resolve the problem of low tolerable loss and excess noise, we introduced a new modulation scheme for CVQKD. The input Gaussian variables are transformed into several Gaussian subcarrier CVs, which are then transformed back by the continuous unitary CVQFT operation at the receiver. The transmission is realized through several Gaussian sub-channels, each dedicated to a given subcarrier with an independent noise variance. The AMQD modulation allows higher tolerable loss and excess noise in comparison with the standard modulation, and can be applied in both one-way and two-way CVQKD. We also investigated an adaptive modulation variance allocation mechanism for the scheme, which can significantly improve the efficiency of the transmission, particularly in the low SNR regimes.

ACKNOWLEDGEMENTS

The results discussed above are supported by the grant TAMOP-4.2.1/B-09/1/KMR-2010-0002, 4.2.2.B-10/1--2010-0009 and COST Action MP1006.

REFERENCES

[1] M R A Adcock, P Høyer, and B C Sanders, Limitations on continuous variable quantum algorithms with Fourier transforms, New Journal of Physics 11 103035 (2009)

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

[3] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Continuous Variable Quantum Cryptography using Two-Way Quantum Communication, arXiv:quant-ph/0611167v3 (2008).

[4] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, L. Gyongyosi. Wireless Myths, Realities, and Futures: From 3G/4G to Optical and Quantum Wireless, Proceedings of the IEEE, Volume: 100, Issue: Special Centennial Issue, pp. 1853-1888. (2012).

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

[6] D. Tse and P. Viswanath. Fundamentals of Wireless Communication, Cambridge University Press, (2005).

[7] David Middlet, An Introduction to Statistical Communication Theory: An IEEE Press Classic Reissue, Hardcover, IEEE, ISBN-10: 0780311787, ISBN-13: 978-0780311787 (1960)

[8] Steven Kay, Fundamentals of Statistical Signal Processing, Volumes I-III, Prentice Hall, (2013)

[9] P. S. Chow, Bandwidth optimized digital transmission techniques for spectrally shaped channels with impulse noise, Ph.D. thesis, Stanford University, 1993.

[10] W. Yu, J. M. Cioffi, On Constant Power Water-filling (2001)

[11] S. Pirandola, R. Garcia-Patron, S. L. Braunstein and S. Lloyd. Phys. Rev. Lett. 102 050503. (2009)

[12] S. Pirandola, A. Serafini and S. Lloyd. Phys. Rev. A 79 052327. (2009).

[13] S. Pirandola, S. L. Braunstein and S. Lloyd. Phys. Rev. Lett. 101 200504 (2008).

[14] C. Weedbrook, S. Pirandola, S. Lloyd and T. Ralph. Phys. Rev. Lett. 105 110501 (2010).

[15] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. Ralph, J. Shapiro, and S. Lloyd. Rev. Mod. Phys. 84, 621 (2012).

[16] M. Sun, X. Peng, Y. Shen, H. Guo. Int. J. Quant. Inf. 10 1250059 (2012)

[17] M. Sun, Xiang Peng and Hong Guo. J. Phys. B: At. Mol. Opt. Phys. 46 085501 (2013)

[18] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, arXiv:1210.6216v1 (2012).

[19] W. Shieh and I. Djordjevic. OFDM for Optical Communications. Elsevier (2010).

[20] M. Navascues, F. Grosshans, and A. Acin. Optimality of Gaussian Attacks in Continuous Variable Quantum Cryptography, Phys. Rev. Lett. 97, 190502 (2006).

[21] R. Garcia-Patron and N. J. Cerf. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. Phys. Rev. Lett. 97, 190503 (2006).

[22] L. Gyongyosi, Scalar Reconciliation for Gaussian Modulation of Two-Way Continuous-variable Quantum Key Distribution, arXiv:1308.1391 (2013).

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

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

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

[26] D. Petz, Quantum Information Theory and Quantum Statistics, Springer-Verlag, Heidelberg, Hiv: 6. (2008).

[27] S. Imre, F. Balazs: Quantum Computing and Communications – An Engineering Approach, John Wiley and Sons Ltd, ISBN 0-470-86902-X, 283 pages (2005).

[28] L. Gyongyosi: The Correlation Conversion Property of Quantum Channels, Quantum Information Processing, Springer, ISSN: 1570-0755 (print version), ISSN: 1573-1332 (2013).

[29] L. Gyongyosi, S. Imre: Distillable Entanglement from Classical Correlation, Proceedings of SPIE Quantum Information and Computation XI, (2013).

[30] L. Gyongyosi: The Structure and Quantum Capacity of a Partially Degradable Quantum Channel, IEEE Access, ISSN: 2169-3536, arXiv:1304.5666 (2014).

[31] L. Gyongyosi: Quantum Information Transmission over a Partially Degradable Channel, IEEE Access, ISSN: 2169-3536, arXiv:1303.0606 (2014).