Multicarrier Continuous-Variable Quantum Key Distribution

Laszlo Gyongyosi

[1] School of Electronics and Computer Science
University of Southampton
Southampton SO17 1BJ, UK

[2] MTA-BME Information Systems Research Group
Hungarian Academy of Sciences
7 Nador st., Budapest, H-1051 Hungary

[3] Department of Networked Systems and Services
Budapest University of Technology and Economics
2 Magyar tudosok krt., Budapest, H-1117 Hungary

Abstract

In a continuous-variable quantum key distribution (CVQKD) system, the information is conveyed by coherent state carriers. The quantum continuous variables are sent through a quantum channel, where the presence of the eavesdropper adds a white Gaussian noise to the transmission. The amount of tolerable noise and loss is a crucial point in CVQKD, since it determines the overall performance of the protocol, including the secure key rates and transmission distances. In this work, we propose the adaptive multicarrier quadrature division (AMQD) modulation technique for 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: quantum key distribution; quantum communication; 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]. 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) 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 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.

The AMQD framework allows us to define multiple-access multicarrier CVQKD [22], to prove the improved secret key rates and security thresholds of multicarrier CVQKD [24], and due to the fact that the multicarrier modulation injects several extra degrees of freedom into the transmission, it makes possible to introduce advanced phenomena that are not available in a single-carrier CVQKD setting such as singular layer transmission [23], multidimensional manifold extraction [25], utilization of the sub-carrier domain [26], and advanced quadrature detection with sub-channel estimation [27-29].

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. Section 5 studies the performance of AMQD modulation. Section 6 provides the security proof of AMQD against optimal Gaussian collective attacks. Finally, Section 7 concludes the results.

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 $x_i \in \mathbb{N}\left(0, \sigma^2_{\omega_0}\right)$, $p_i \in \mathbb{N}\left(0, \sigma^2_{\omega_0}\right)$, where $\sigma^2_{\omega_0}$ 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 $z \in \mathcal{CN}\left(0, \sigma^2_{\omega_z}\right)$, with variance $\sigma^2_{\omega_z} = \mathbb{E}\left[|z|^2\right]$, and with i.i.d. real and imaginary zero-mean Gaussian random components, $\operatorname{Re}\left(z_i\right) \in \mathbb{N}\left(0, \sigma^2_{\omega_0}\right)$, $\operatorname{Im}\left(z_i\right) \in \mathbb{N}\left(0, \sigma^2_{\omega_0}\right)$.

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

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

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

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

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

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

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

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

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

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

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

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

where $\Delta \in \mathcal{CN}\left(0, \sigma^2_\Delta\right)$, $\sigma^2_\Delta = \mathbb{E}\left[|\Delta|^2\right]$, models the Gaussian noise of the quantum channel (also a zero-mean, symmetric circular complex Gaussian random variable), with independent quadrature components $\Delta_x \in \mathbb{N}\left(0, \sigma^2_\mathcal{N}\right)$, $\Delta_p \in \mathbb{N}\left(0, \sigma^2_\mathcal{N}\right)$.

This Gaussian quantum channel is equipped with a capacity of

$$C\left(\mathcal{N}\right) = \log_2\left(1 + \frac{\sigma_{\omega_0}^2 \left|T(\mathcal{N})\right|^2}{\sigma_{\mathcal{N}}^2}\right), \tag{7}$$

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 $\mathcal{N}_i$, $i = 0 \dots n-1$, each with an independent noise variance $\sigma_{\mathcal{N}_i}^2$, each for the transmission of a continuous variable subcarrier $\left|\phi_i\right\rangle$, which leads to the output for the i-th sub-channel:

$$y_i = T\left(\mathcal{N}_i\right)x_i + \Delta_i, \ i = 0 \dots n-1, \tag{8}$$

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

$$C\left(\mathcal{N}\right) = \max_{\forall i} \sum_{i=0}^{n-1} \log_2\left(1 + \frac{\sigma_{\omega}^2 \left|T(\mathcal{N}_i)\right|^2}{\sigma_{\mathcal{N}_i}^2}\right), \tag{9}$$

where $\sigma_{\omega}^2 = \frac{1}{n}\sum_{i=0}^{n-1}\sigma_{\omega_i}^2 = \sigma_{\omega_0}^2$ 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 (7) and (9) 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

$$C\left(\mathcal{N}\right) = \tfrac{1}{2}\log_2\left(1 + \frac{\sigma_{\omega_0}^2 \left|T(\mathcal{N})\right|^2}{\sigma_{\mathcal{N}}^2}\right), \tag{10}$$

while the complex dimension capacity is precisely

$$C\left(\mathcal{N}\right) = \log_2\left(1 + \frac{\sigma_{\omega}^2 \left|T(\mathcal{N})\right|^2}{\sigma_{\mathcal{N}}^2}\right). \tag{11}$$

In (11) 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

$$\mathrm{SNR} = \frac{\sigma_{\omega_0}^2 \left|T(\mathcal{N})\right|^2}{\sigma_{\mathcal{N}}^2}. \tag{12}$$

For the precise clarification, we will use the complex-domain capacity formula throughout, since the coherent state in the phase space is a complex variable. (*Note*: For the achievable secret key rates of AMQD at a heterodyne and homodyne measurement setting see [24]. For an adaptive

quadrature detection mechanism (homodyne and heterodyne) developed for AMQD, see [27]).

3 Multicarrier Quadrature Division Modulation

3.1 Continuous-Variable Quantum Fourier Transform

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

$$g\left(x\right) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-x^2}{2\sigma^2}}, \ x \in \mathbb{N}\left(0, \sigma^2\right), \tag{13}$$

where $\int_{-\infty}^{\infty} g\left(x\right) dx = 1$. The Fourier transform of (13) is expressed as

$$F\left(g\left(x\right)\right) = G\left(\omega\right) = e^{\frac{-\omega^2\sigma^2}{2}}, \ \omega \in \mathbb{N}\left(0, \sigma^2\right). \tag{14}$$

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]:

$$F\left(x\right) = \int_{-\infty}^{\infty} F^{-1}\left(\omega\right) e^{-\mathrm{i}x\omega} d\omega, \tag{15}$$

where

$$F^{-1}\left(\omega\right) = \frac{1}{2\pi} \int_{-\infty}^{\infty} F\left(x\right) e^{\mathrm{i}x\omega} dx. \tag{16}$$

For an n-dimensional Gaussian random vector $\mathbf{g} \in \left(0, \mathbf{K_g}\right)$, $\mathbf{g} = \left(g_0, , g_{n-1}\right)^T$, where $\mathbf{K_g} = \mathbb{E}\left[\mathbf{gg}^T\right]$ is the covariance matrix, the Fourier transform and its inverse:

$$F\left(\mathbf{g}\right) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} F^{-1}\left(\mathbf{w}\right) e^{-\mathrm{i}\mathbf{g}\cdot\mathbf{w}} d\mathbf{w}, \tag{17}$$

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

$$F^{-1}\left(\mathbf{w}\right) = \frac{1}{\left(2\pi\right)^n} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} F\left(\mathbf{g}\right) e^{\mathrm{i}\mathbf{g}\cdot\mathbf{w}} d\mathbf{g}. \tag{18}$$

Proposition 1. *The σ_F^2 variance of a Gaussian subcarrier CV $\left|\phi_i\right\rangle$ is the reciprocal of $\sigma_{\omega_0}^2$, $\sigma_F^2 = 1 \big/ \sigma_{\omega_0}^2$, 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.

Assuming $\left|x\right\rangle$ position computational basis, function $F(\cdot)$ acts on the coherent input $\left|\varphi_i\right\rangle$ as follows [1]:

$$F\left(\left|\varphi_i\right\rangle\right) = F\left(\left\langle x\left|\varphi_i\right\rangle\right.\right) \rightarrow \left\langle p\left|\varphi_i\right\rangle\right., \tag{19}$$

where

$$\left\langle x\left|\varphi_i\right\rangle\right. = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \left\langle p\left|\varphi_i\right\rangle\right. dp\, e^{ipx}, \tag{20}$$

and

$$\left\langle p\left|\varphi_i\right\rangle\right. = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \left\langle x\left|\varphi_i\right\rangle\right. dx\, e^{-ipx} \tag{21}$$

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

$$\left\langle x\left|\psi\right\rangle\right. = \int_{-\infty}^{\infty} f\left(x - x'\right)\psi\left(x'\right) dx', \tag{22}$$

where $f\left(x - x'\right) = \left\langle x\left|x'\right\rangle\right.$ and $\psi\left(x\right) = \left\langle x\left|\psi\right\rangle\right.$. 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

$$\psi\left(q\right) = \int_{-\infty}^{\infty} c\left(p\right)u\left(p;q\right) dp, \tag{23}$$

where

$$\begin{aligned}
c\left(p\right) &= \left\langle u\left(p;q\right), \psi\left(q\right)\right\rangle \\
&= \left\langle u\left(p;q\right), \int_{-\infty}^{\infty} c\left(p\right)u\left(p;q\right) dp \right\rangle \\
&= \int_{-\infty}^{\infty} f\left(p - p'\right)c\left(p'\right) dp'.
\end{aligned} \tag{24}$$

The inverse function of (19) is defined as

$$F^{-1}\left(\left\langle p\left|\varphi_i\right\rangle\right.\right) = \left\langle x\left|\varphi_i\right\rangle\right.. \tag{25}$$

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 $z_i \in \mathcal{CN}\left(0, \sigma_{\omega_{z_i}}^2\right)$, $\sigma_{\omega_{z_i}}^2 = \left[\mathbb{E}\left|z_i\right|^2\right]$, as

$$z_i = x_i + \mathrm{i}p_i, \tag{26}$$

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,

$$\left|\varphi_i\right\rangle = \left|z_i\right\rangle. \tag{27}$$

The variable $e^{\mathrm{i}\varphi_i} z_i$ has the same distribution of z_i for any φ_i, i.e., $\mathbb{E}\left[z_i\right] = \mathbb{E}\left[e^{\mathrm{i}\varphi_i} z_i\right] = \mathbb{E}e^{\mathrm{i}\varphi_i}\left[z_i\right]$ and $\sigma_{z_i}^2 = \mathbb{E}\left[\left|z_i\right|^2\right]$. The density of z_i is

$$f\left(z_i\right) = \frac{1}{2\pi\sigma_{\omega_0}^2} e^{\frac{-\left(\left|z_i\right|^2\right)}{2\sigma_{\omega_0}^2}} = f\left(x_i, p_i\right) = \frac{1}{2\pi\sigma_{\omega_0}^2} e^{\frac{-\left(x_i^2 + p_i^2\right)}{2\sigma_{\omega_0}^2}}, \tag{28}$$

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

$$f\left(\left|z_i\right|\right) = \frac{\left|z_i\right|}{\sigma_{\omega_{z_i}}^2} e^{\frac{-\left|z_i\right|^2}{2\sigma_{\omega_{z_i}}^2}}, \left|z_i\right| \geq 0, \tag{29}$$

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

$$f\left(\left|z_i\right|^2\right) = \frac{1}{\sigma_{\omega_{z_i}}^2} e^{\frac{-\left|z_i\right|^2}{\sigma_{\omega_{z_i}}^2}}, \left|z_i\right|^2 \geq 0. \tag{30}$$

The i-th *subcarrier* CV is defined as

$$\left|\phi_i\right\rangle = \left|\mathrm{IFFT}\left(z_i\right)\right\rangle = \left|F^{-1}\left(z_i\right)\right\rangle = \left|d_i\right\rangle, \tag{31}$$

where IFFT stands for the Inverse Fast Fourier Transform, and subcarrier continuous variable $\left|\phi_i\right\rangle$ in (31) is also a zero-mean, circular symmetric complex Gaussian random variable $d_i \in \mathcal{CN}\left(0, \sigma_{d_i}^2\right)$, $\sigma_{d_i}^2 = \mathbb{E}\left[\left|d_i\right|^2\right]$, $d_i = x_{d_i} + \mathrm{i}p_{d_i}$, 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 (31) results the single-carrier CV from the subcarrier CV as follows:

$$\left|\varphi_i\right\rangle = \mathrm{CVQFT}\left(\left|\phi_i\right\rangle\right) = F\left(\left|d_i\right\rangle\right) = \left|F\left(F^{-1}\left(z_i\right)\right)\right\rangle = \left|z_i\right\rangle, \tag{32}$$

where CVQFT is the continuous-variable QFT operation.

Let us to derive the Fourier transform of the Gaussian input [7-8]. First, we rewrite (28) in the position basis x as $g(x) = \frac{1}{\sqrt{2\pi\sigma^2_{\omega_0}}} e^{\frac{-x^2}{a^2}}$, where $a^2 = 2\sigma^2_{\omega_0}$. Then, the Fourier transformed signal $G(p)$ is precisely evaluated as

$$
\begin{aligned}
F(g(x)) &= G(p) \\
&= \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{2\pi\sigma^2_{\omega_0}}} \int_{-\infty}^{\infty} g(x) e^{-\mathrm{i}px} dx \\
&= \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{2\pi\sigma^2_{\omega_0}}} \int_{-\infty}^{\infty} e^{\frac{-x^2}{a^2}} e^{-\mathrm{i}px} dx \\
&= \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{2\pi\sigma^2_{\omega_0}}} \int_{-\infty}^{\infty} e^{\left(\frac{-x^2}{a^2}-\mathrm{i}px\right)} dx \\
&= \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{2\pi\sigma^2_{\omega_0}}} e^{-\frac{a^2 p^2}{4}} \int_{-\infty}^{\infty} e^{-\left(\frac{x}{a}+\frac{\mathrm{i}ap}{2}\right)^2} dx. \\
&= \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{2\pi\sigma^2_{\omega_0}}} e^{\frac{-a^2 p^2}{4}} \int_{-\infty}^{\infty} e^{-\frac{\left(x+\frac{\mathrm{i}a^2 p}{2}\right)^2}{a^2}} dx \\
&= \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{2\pi\sigma^2_{\omega_0}}} e^{-\frac{\sigma^2_{\omega_0} p^2}{2}} = \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{2\pi\sigma^2_{\omega_0}}} e^{-\frac{p^2}{2\sigma^2_F}} \\
&= \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{\frac{2\pi}{\sigma^2_F}}} e^{-\frac{p^2}{2\sigma^2_F}}.
\end{aligned}
\tag{33}
$$

The $G(p)$ Fourier transform of the Gaussian signal $g(x)$ is also Gaussian in the conjugate-variable space, with variance $\sigma^2_F = 1/\sigma^2_{\omega_0}$. 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^2_ω of the input Gaussian signal increases, the variance σ^2_F 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 $\Delta p = 1/\sigma_{\omega_0}$, then $\Delta x \Delta p = 1$.

∎

The normalized Gaussian functions $g(x) = \frac{1}{\sqrt{2\pi\sigma^2_{\omega_i}}\sqrt{2\sigma_{\omega_i}}} e^{\frac{-x^2}{2\sigma^2_{\omega_i}}}$ and $G(p) = \frac{\sqrt{2\sigma_{\omega_i}}}{\sqrt{2\pi\sigma^2_{\omega_i}}} e^{-\frac{p^2}{2\sigma^2_{F_i}}}$ are shown in Fig. 1. In terms of the quadratures, the momentum p is the Fourier transform of the position x, and the position x is the inverse-Fourier transform of the momentum p.

9
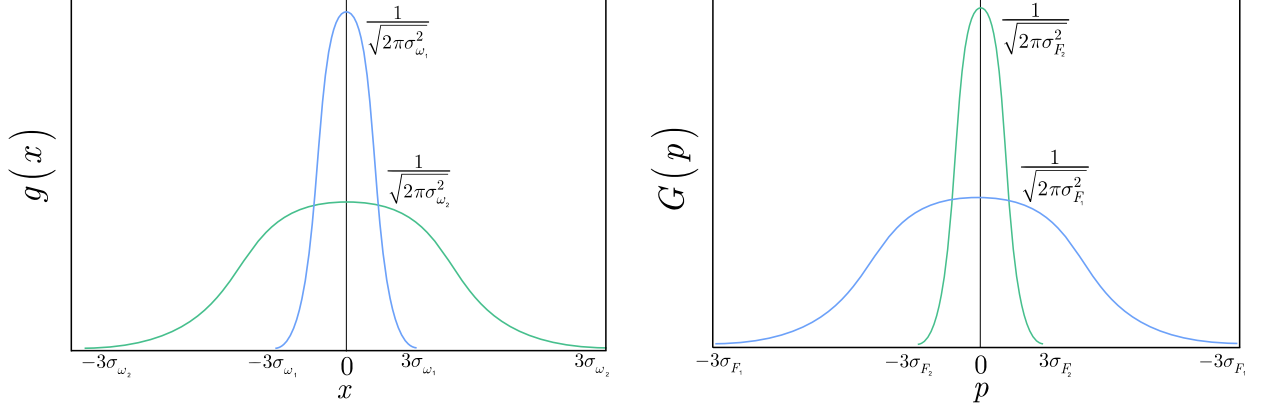
Figure 1. The input Gaussian state in the position basis (a) and the CVQFT transformed signal in the momentum basis, where $\sigma_{F_i}^2 = 1/\sigma_{\omega_i}^2$ (b).

The characterization of the Gaussian sub-channels is proposed Theorem 1.

Theorem 1. *The AMQD divides the Gaussian channel $\mathcal{N}$ into n Gaussian sub-channels $\mathcal{N}_i$, $i = 0, \ldots, n-1$, with independent noise variances $\sigma_{\mathcal{N}_i}^2$, where $\frac{1}{n}\sum_{i=0}^{n-1} \sigma_{\mathcal{N}_i}^2 = \sigma_{\mathcal{N}}^2$.*

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

$$\mathbf{z} = \mathbf{x} + \mathrm{i}\mathbf{p} = \left(z_0, \ldots, z_{n-1}\right)^T \in \mathcal{CN}\left(0, \mathbf{K_z}\right), \tag{34}$$

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, $\mathbf{x} = \left(x_0, \ldots, x_{n-1}\right)^T$ and $\mathbf{p} = \left(p_0, \ldots, p_{n-1}\right)^T$, with zero-mean Gaussian random variables

$$f\left(x_i\right) = \frac{1}{\sigma_{\omega_0}\sqrt{2\pi}} e^{\frac{-x_i^2}{2\sigma_{\omega_0}^2}}, \ f\left(p_i\right) = \frac{1}{\sigma_{\omega_0}\sqrt{2\pi}} e^{\frac{-p_i^2}{2\sigma_{\omega_0}^2}}, \tag{35}$$

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 $\mathbf{z}$:

$$\mathbf{K_z} = \mathbb{E}\left[\mathbf{z}\mathbf{z}^\dagger\right], \tag{36}$$

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

$$\mathbb{E}\big[\mathbf{z}\big] = \mathbb{E}\big[e^{\mathrm{i}\gamma}\mathbf{z}\big] = \mathbb{E}e^{\mathrm{i}\gamma}\big[\mathbf{z}\big] \tag{37}$$

holds, and

$$\mathbb{E}\big[\mathbf{z}\mathbf{z}^T\big] = \mathbb{E}\bigg[e^{\mathrm{i}\gamma}\mathbf{z}\big(e^{\mathrm{i}\gamma}\mathbf{z}\big)^T\bigg] = \mathbb{E}e^{\mathrm{i}2\gamma}\big[\mathbf{z}\mathbf{z}^T\big], \tag{38}$$

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

$$f\big(\mathbf{z}\big) = \frac{1}{\pi^n \det \mathbf{K_z}} e^{-\mathbf{z}^\dagger \mathbf{K_z}^{-1}\mathbf{z}}. \tag{39}$$

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 $\mathbb{N}\big(0,1\big)_n$. This vector is characterized by its covariance matrix $\mathfrak{C}\big(\mathbf{x}\big) = \mathbb{E}\big[\mathbf{x}\mathbf{x}^T\big] = \mathbf{A}\mathbf{A}^T$, as

$$\mathbf{x} = \frac{1}{\big(\sqrt{2\pi}\big)^n \sqrt{\det\big(\mathbf{A}\mathbf{A}^T\big)}} e^{-\frac{\mathbf{x}^T\mathbf{x}}{2\big(\mathbf{A}\mathbf{A}^T\big)}}. \tag{40}$$

The Fourier transformation $F\big(\cdot\big)$ of the n-dimensional Gaussian random vector $\mathbf{v} = \big(v_0,\ldots,v_{n-1}\big)^T$ results in the n-dimensional Gaussian random vector $\mathbf{m} = \big(m_0,\ldots,m_{n-1}\big)^T$:

$$\mathbf{m} = F\big(\mathbf{v}\big) = e^{\frac{-\mathbf{m}^T\mathbf{A}\mathbf{A}^T\mathbf{m}}{2}} = e^{\frac{-\sigma_{\omega_0}^2\big(m_0^2+\ldots+m_{n-1}^2\big)}{2}}. \tag{41}$$

In the first step of AMQD, Alice applies the inverse FFT operation to vector $\mathbf{z}$ (see (34)), which results in an n-dimensional zero-mean, circular symmetric complex Gaussian random vector $\mathbf{d}$, $\mathbf{d} \in \mathcal{CN}\big(0, \mathbf{K_d}\big)$, $\mathbf{d} = \big(d_0,\ldots,d_{n-1}\big)^T$, precisely as

$$\mathbf{d} = F^{-1}\big(\mathbf{z}\big) = e^{\frac{\mathbf{d}^T\mathbf{A}\mathbf{A}^T\mathbf{d}}{2}} = e^{\frac{\sigma_{\omega_0}^2\big(d_0^2+\ldots+d_{n-1}^2\big)}{2}}, \tag{42}$$

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

$$x_{d_i} \in \mathbb{N}\big(0, \sigma_F^2\big), \ p_{d_i} \in \mathbb{N}\big(0, \sigma_F^2\big), \tag{43}$$

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

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

$$\big|\phi_i\big\rangle = \big|d_i\big\rangle = \big|F^{-1}\big(z\big)\big\rangle. \tag{44}$$

The result of (42) 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 $\mathbf{y} \in \mathcal{CN}\left(0, \mathbb{E}\left[\mathbf{y}\mathbf{y}^\dagger\right]\right)$. The m-th element of vector $\mathbf{y}$ is y_m, expressed as follows:

$$
\begin{aligned}
y_m &= F\left(\mathbf{T}\left(\mathcal{N}\right)\right)z_m + F\left(\Delta\right) \\
&= F\left(\mathbf{T}\left(\mathcal{N}\right)\right)F\left(F^{-1}\left(z_m\right)\right) + F\left(\Delta\right) \\
&= \sum_n F\left(T_i\left(\mathcal{N}_i\right)\right)F\left(d_i\right) + F\left(\Delta_i\right),
\end{aligned}
\tag{45}
$$

where

$$
\mathbf{T}\left(\mathcal{N}\right) = \left[T_0\left(\mathcal{N}_0\right), \ldots, T_{n-1}\left(\mathcal{N}_{n-1}\right)\right]^T \in \mathcal{C}^n,
\tag{46}
$$

where

$$
T_i\left(\mathcal{N}_i\right) = \mathrm{Re}\left(T_i\left(\mathcal{N}_i\right)\right) + \mathrm{i}\,\mathrm{Im}\left(T_i\left(\mathcal{N}_i\right)\right) \in \mathcal{C},
\tag{47}
$$

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 $0 \le \mathrm{Re}\,T_i\left(\mathcal{N}_i\right) \le 1/\sqrt{2}$, $0 \le \mathrm{Im}\,T_i\left(\mathcal{N}_i\right) \le 1/\sqrt{2}$. 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:

$$
F\left(\mathbf{T}\left(\mathcal{N}\right)\right) = \sum_{i=0}^{n-1} F\left(T_i\left(\mathcal{N}_i\right)\right) = \sum_{i=0}^{n-1}\sum_{k=0}^{n-1} T_k e^{\frac{-\mathrm{i}2\pi ik}{n}} \in \mathcal{C}^n,
\tag{48}
$$

where $F\left(\mathbf{T}\left(\mathcal{N}\right)\right)$ is the Fourier transform of (46). The n-dimensional $F\left(\Delta\right)$ complex vector is evaluated as

$$
F\left(\Delta\right) = e^{\frac{-F(\Delta)^T \mathfrak{C}(F(\Delta))F(\Delta)}{2}} = e^{\frac{-\left[F(\Delta_0)^2 \sigma_{\mathcal{N}_0}^2 + \ldots + F(\Delta_{n-1})^2 \sigma_{\mathcal{N}_{n-1}}^2\right]}{2}},
\tag{49}
$$

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

$$
\Delta = \left(\Delta_0, \ldots, \Delta_{n-1}\right)^T \in \mathcal{CN}\left(0, \mathfrak{C}\left(\Delta\right)\right),
\tag{50}
$$

where $\mathfrak{C}\left(\Delta\right) = \mathbb{E}\left[\Delta\Delta^\dagger\right]$, with independent, zero-mean Gaussian random components

$\Delta_{x_i} \in \mathbb{N}\left(0, \sigma_{\mathcal{N}_i}^2\right)$, $\Delta_{p_i} \in \mathbb{N}\left(0, \sigma_{\mathcal{N}_i}^2\right)$ with variance $\sigma_{\mathcal{N}_i}^2$, 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 (49) can be rewritten as

$$F\left(\Delta\right) = \left(F\left(\Delta_0\right), ..., F\left(\Delta_{n-1}\right)\right)^T, \tag{51}$$

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

$$\mathfrak{C}\left(F\left(\Delta\right)\right) = \mathbb{E}\left[F\left(\Delta\right)F\left(\Delta\right)^\dagger\right], \tag{52}$$

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

$$\begin{aligned}
\sigma_{F(\mathcal{N})}^2 \mathbf{I}_{n \times n} &= \frac{1}{n}\sum_{i=0}^{n-1}\sigma_{F(\mathcal{N}_i)}^2 \\
&= \sigma_{F(\mathcal{N})}^2 = \frac{1}{\sigma_{\mathcal{N}}^2},
\end{aligned} \tag{53}$$

where $\sigma_{\mathcal{N}}^2$ is the noise variance of the Gaussian quantum channel $\mathcal{N}$, $\mathbf{I}_{n \times n}$ is the $n \times n$ identity matrix, hence $F\left(\Delta_i\right) \in \mathcal{CN}\left(0, \sigma_{F(\Delta_i)}^2\right)$, and $\sigma_{F(\Delta_i)}^2 = \mathbb{E}\left[\left|F\left(\Delta_i\right)\right|^2\right]$, with independent noise variance $\sigma_{F(\mathcal{N})}^2$ on the quadrature components (For simplicity, the notation of $\mathbf{I}_{n \times n}$ will be omitted from the description.).

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

$$\mathbf{y}\left[j\right] = F\left(\mathbf{T}\left(\mathcal{N}\right)\right)F\left(\mathbf{d}\right)\left[j\right] + F\left(\Delta\right)\left[j\right], \; j = 1, ..., n, \tag{54}$$

where j is the index of the AMQD block, $F\left(\mathbf{T}\left(\mathcal{N}\right)\right)$ is defined in (48), $F\left(\mathbf{d}\right) = F\left(F^{-1}\left(\mathbf{z}\right)\right)$, where $F^{-1}\left(\mathbf{z}\right)$ is shown in (42), while

$$\begin{aligned}
\mathbf{y}\left[j\right] &= \left(y_1\left[j\right], ..., y_n\left[j\right]\right)^T, \\
F\left(\mathbf{d}\right)\left[j\right] &= \left(F\left(d_1\right)\left[j\right], ..., F\left(d_n\right)\left[j\right]\right)^T, \\
F\left(\Delta\right)\left[j\right] &= \left(F\left(\Delta_1\right)\left[j\right], ..., F\left(\Delta_n\right)\left[j\right]\right)^T.
\end{aligned} \tag{55}$$

The squared magnitude

$$\tau = \left\|F\left(\mathbf{d}\right)\left[j\right]\right\|^2 \tag{56}$$

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

$$\mathbb{E}\big[\tau\big] \leq n2\sigma_\omega^2\,, \tag{57}$$

while the average quadrature modulation variance is

$$\sigma_\omega^2 = \tfrac{1}{n}\sum_{i=0}^{n-1}\sigma_{\omega_i}^2 = \sigma_{\omega_0}^2\,, \tag{58}$$

where $\sigma_{\omega_i}^2$ is the modulation variance of the quadratures of the subcarrier $\big|\phi_i\big\rangle$ transmitted by sub-channel $\mathcal{N}_i$.

The transformed vector $\mathbf{y}$ in (45) and (55) 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.

$\blacksquare$

3.2 Gaussian Noise of the 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 $\big|\phi_i\big\rangle$ transmitted by $\mathcal{N}_i$ be

$$\big(x_{in,i}, p_{in,i}\big),\ x_{in,i} \in \mathbb{N}\Big(0,\sigma_{\omega_i}^2\Big),\ p_{in,i} \in \mathbb{N}\Big(0,\sigma_{\omega_i}^2\Big), \tag{59}$$

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

$$\big(x_{E,i}, p_{E,i}\big),\ \ x_{E,i} \in \mathbb{N}\Big(0,\sigma_{\omega_i}^2 + \sigma_{\mathcal{N}_i}^2\Big),\ p_{E,i} \in \mathbb{N}\Big(0,\sigma_{\omega_i}^2 + \sigma_{\mathcal{N}_i}^2\Big), \tag{60}$$

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

$$\big(x_{B,i}, p_{B,i}\big),\ \ x_{B,i} \in \mathbb{N}\Big(0,\sigma_{\omega_i}^2 + \sigma_{\mathcal{N}_i}^2\Big),\ p_{B,i} \in \mathbb{N}\Big(0,\sigma_{\omega_i}^2 + \sigma_{\mathcal{N}_i}^2\Big). \tag{61}$$

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 $T_{Eve,i} \in \mathcal{C}$, $0 < \big|T_{Eve,i}\big|^2 < 1$, and an entangled ancilla $\big|\Psi_{EB}\big\rangle$ with variance W. The quadratures of the i-th sub-channel are $\big(x_{in,i}, p_{in,i}\big)$, Eve's quadratures are $\big(x_{E,i}, p_{E,i}\big)$, Bob's received noisy quadratures are $\big(x'_{in,i}, p'_{in,i}\big)$. Each sub-channel is characterized with a Gaussian noise $\mathbb{N}\Big(0,\sigma_{\mathcal{N}_i}^2\Big)$ on the quadrature components, with independent noise variance $\sigma_{\mathcal{N}_i}^2$. As shown in (50), Eve's optimal Gaussian attacks define an n-dimensional zero-mean, circular symmetric complex Gaussian random noise vector.
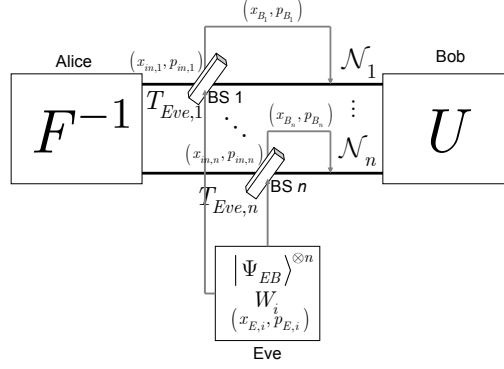
Figure 2. The entangler cloning attack in the multicarrier modulation scheme. The unitary refers to the CVQFT operation.

In the AMQD scenario, the appropriate noise vector is given by (49) and (52), as $F(\Delta) \in \mathcal{CN}\left(0, \mathfrak{C}\left(F(\Delta)\right)\right)$, and $F(\Delta_i) \in \mathcal{CN}\left(0, \sigma^2_{F(\Delta_i)}\right)$, respectively. For the security proof of AMQD against optimal Gaussian collective attacks is being presented in Theorem 4.

3.3 Crosstalk Noise on the Sub-channels

The crosstalk is an additive noise in multicarrier transmission that can occur between adjacent sub-channels. Crosstalk noise can result from a nonperfect sub-channel separation and sub-channel filtering procedure. As a result of interchannel crosstalk, some information from neighboring channels can leak, which acts as noise to the receiver. In practice, crosstalk arises from the imperfections of optical filters, optical switches or other optical components, e.g., from the imperfect isolation of different wavelength ports [19].

The effect of interchannel crosstalk in an AMQD modulation is depicted in Fig. 3. Crosstalk noise has no effect on the security of AMQD modulation, since it allows no more leaking of information to an eavesdropper than single-carrier CVQKD protocols (see Theorem 4).
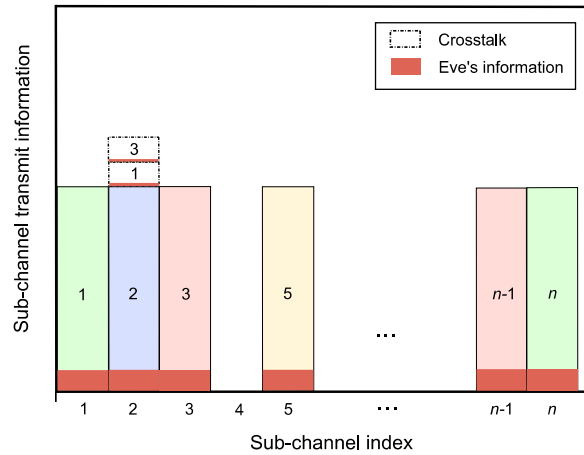
Figure 3. The effect of crosstalk noise between sub-channels. Due to the imperfections of practical devices, some information from neighboring sub-channels can be leaked to a given sub-channel, which acts as noise to the receiver.

As it is depicted in Fig. 3, for sub-channel 2, some crosstalk information brings up from neighboring sub-channels, 1 and 3. Any nonzero crosstalk information can leak information of only negligible valuable to Eve, as is proven in Theorem 4.

The crosstalk information $\gamma\left(\mathcal{N}_i\right)$ on the i-th sub-channel $\mathcal{N}_i$, $i = 0...n-1$, is evaluated from the interference noise of the neighboring sub-channels as follows:

$$\gamma\left(\mathcal{N}_i\right) = \sum_{j \neq i} x_j \chi\left(A_j : B_j\right), \tag{62}$$

where $0 \leq x_j \leq 1$, $\chi\left(A_j : B_j\right) = H\left(B_j\right) - H\left(B_j \middle| A_j\right)$ is the Holevo information of Alice and Bob conveyed by the neighboring sub-channel $\mathcal{N}_j$, for all $j \neq i$. The average crosstalk on the n sub-channels is expressed as

$$\tilde{\gamma}\left(\mathcal{N}\right) = \tfrac{1}{n} \sum_n \sum_{j \neq i} x_j \chi\left(A_j : B_j\right). \tag{63}$$

Since the crosstalk noise $\gamma_i\left(\mathcal{N}_i\right)$ on sub-channel $\mathcal{N}_i$ acts for Bob as Gaussian noise (which is justified by the Central Limit Theorem, more precisely for $i \to \infty$), it can be modeled by $\gamma_i \in \mathcal{CN}\left(0, \sigma_{\gamma_i}^2\right)$ with variance $\sigma_{\gamma_i}^2 = \mathbb{E}\left[\left|\gamma_i\right|^2\right]$. This additional noise does not change the rate formulas of AMQD (see (74) and (80)), because this additional noise is already contained in the sub-channel's noise variance $\sigma_{\mathcal{N}_i}^2$.

In other words, the mutual information between Alice and Bob is completely characterized for a given $\mathcal{N}_i$ by the noise variance $\sigma_{\mathcal{N}_i}^2$, which can be decomposed as

$$\sigma_{\mathcal{N}_i}^2 = \sigma_{Eve,i}^2 + \sigma_{\gamma_i}^2, \tag{64}$$

where $\sigma_{Eve,i}^2$ is the noise variance of Eve's optimal Gaussian collective attack.

Assuming that l sub-channels have been allocated for the multicarrier transmission, the mutual information function of Alice and Bob remains untouched under the presence of nonzero crosstalk, i.e., $I\left(A : B\right) = \tfrac{1}{l} \sum_l I\left(A_j : B_j\right)$. However, the $\chi\left(B : E\right)$ Holevo information of Eve, in the presence of a nonzero crosstalk between the sub-channels changes as follows:

$$\begin{aligned}
\chi\left(B : E\right)_{\gamma_i} &= \chi\left(B : E\right) + \sum_n \left|T_{Eve,i}\right|^2 \gamma\left(\mathcal{N}_i\right) \\
&= \chi\left(B : E\right) + \sum_n \sum_{j \neq i} \left|T_{Eve,i}\right|^2 x_j \chi\left(A_j : B_j\right),
\end{aligned} \tag{65}$$

where $\left|T_{Eve,i}\right|^2$ is the squared magnitude of Eve's $T_{Eve,i}$ normalized complex transmittance $T_{Eve,i} = \operatorname{Re} T_{Eve,i} + \mathrm{i} \operatorname{Im} T_{Eve,i} \in \mathcal{C}$, where $0 \leq \operatorname{Re} T_{Eve,i} \leq 1/\sqrt{2}$, $0 \leq \operatorname{Im} T_{Eve,i} \leq 1/\sqrt{2}$ that characterizes the attack of sub-channel $\mathcal{N}_i$, and the quantity $\gamma\left(\mathcal{N}_i\right)$ is calculated with respect to the n sub-channel (a nonzero crosstalk can also occur on an unused sub-channel, hence all sub-channels have to be taken into consideration in the RHS of (65)).

For detailed security proof of AMQD against optimal Gaussian collective attacks, see Theorem 4.

3.4 Run of Multicarrier Quadrature Division

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 $\mathbf{z} = \mathbf{x} + \mathrm{i}\mathbf{p} = \left(z_0,...,z_{n-1} \right)^T \in \mathcal{CN}\left(0, \mathbf{K_z} \right)$, $z_i = p_i + \mathrm{i}q_i$, 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 $\mathbf{d} = \mathbf{x} + \mathrm{i}\mathbf{p} = \left(d_0,...,d_{n-1} \right)^T \in \mathcal{CN}\left(0, \mathbf{K_d} \right)$. According to $\mathbf{d}$, she prepares the $\left| \phi_{1...n} \right\rangle$ 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, $\left| \varphi_{0...n-1}' \right\rangle = \left| z_{0...n-1}' \right\rangle = \left| \mathbf{z}' \right\rangle$, and the Fourier transformed sub-channel noise variance $\sigma_{F\left(\mathcal{N}_i \right)}^2$. 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. 4.
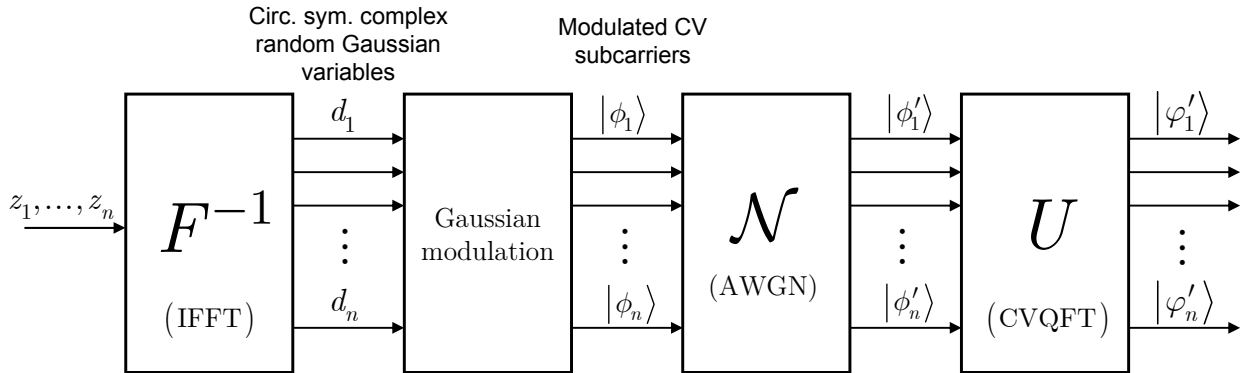
Figure 4. The AMQD modulation scheme. Alice draws an n-dimensional, zero-mean, circular symmetric complex Gaussian random vector $\mathbf{z}$, which are then inverse Fourier-transformed by F^{-1}. The resulting vector $\mathbf{d}$ encodes the subcarrier quadratures for the Gaussian modulation. In the 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 adaptive modulation sends information through only the high-quality sub-channels, while the noisy sub-channels transmit no information, as it is proposed in the next section.

4 Adaptive Modulation Variance

Theorem 2. (Adaptive modulation variance.) *The ratio* $\nu_i = \sigma_{\mathcal{N}}^2 \big/ \big| F\big(T_i\big(\mathcal{N}_i\big)\big)\big|^2$, *where*

$\big| F\big(T_i\big(\mathcal{N}_i\big)\big)\big|^2 = \left| \sum_{k=0}^{n-1} T_k e^{\frac{-i2\pi ik}{n}} \right|^2$, $i = 0\dots n-1$, *provides the* $\sigma_{\omega}^2 = \nu_{Eve} - \min\big(\nu_i\big)$ *optimal constant modulation variance for the Gaussian sub-channels, where* ν_{Eve} *is a security bound of the optimal Gaussian collective attack.*

Proof.
Note the proof throughout the section focuses on the transmission of classical information. The rigorous derivation of the private classical capacity and the achievable secret key rates of AMQD are included in [24].
The proof consists of two parts. First, we show that there exists an optimal constant modulation variance for the sub-channels with average $\sigma_{\omega}^2 = \frac{1}{n}\sum_n \sigma_{\omega_i}^2 = \nu_{Eve} - \big(\nu\big)$, where ν_{Eve} is the security bound of Eve's optimal Gaussian collective attack, and ν is

$$\nu = \frac{1}{n}\sum_n \nu_i = \frac{1}{n}\frac{\sum_n \sigma_{\mathcal{N}_i}^2}{\sum_{i=0}^{n-1}\left|\sum_{k=0}^{n-1}T_k e^{\frac{-i2\pi ik}{n}}\right|^2} = \frac{\sigma_{\mathcal{N}}^2}{\sum_{i=0}^{n-1}\left|F\big(T_i\big(\mathcal{N}_i\big)\big)\right|^2}, \tag{66}$$

where $\nu_i = \sigma_{\mathcal{N}_i}^2 \big/ \left|\sum_{k=0}^{n-1} T_k e^{\frac{-i2\pi ik}{n}}\right|^2$ for the i-th sub-channel $\mathcal{N}_i$, $\sigma_{\mathcal{N}_i}^2$ is the noise variance of $\mathcal{N}_i$, while $\left|\sum_{k=0}^{n-1} T_k e^{\frac{-i2\pi ik}{n}}\right|^2$ is the squared magnitude of the sum of the Fourier coefficients of the n Gaussian sub-channels. Then, we show that for low SNRs, the optimal solution is $\nu = \min\big(\nu_i\big)$. 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

$$\nu_{Eve} = \frac{1}{\lambda}, \tag{67}$$

where λ is the *Lagrange multiplier* as

$$\lambda = \left|F\big(T_{\mathcal{N}}^*\big)\right|^2 = \frac{1}{n}\sum_{i=0}^{n-1}\left|\sum_{k=0}^{n-1}T_k^* e^{\frac{-i2\pi ik}{n}}\right|^2, \tag{68}$$

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

$$\mathcal{L}\left(\lambda, \sigma_{\omega_0}^2 \ldots \sigma_{\omega_{n-1}}^2\right) = \sum_{i=0}^{n-1} \log_2\left(1 + \frac{\sigma_{\omega_i}^2 \left|F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2}{\sigma_{\mathcal{N}}^2}\right) - \lambda \sum_{i=0}^{n-1} \sigma_{\omega_i}^2 . \tag{69}$$

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:

$$\sigma_\omega^2 = \frac{1}{n} \sum_{i=0}^{n-1} \left(\nu_{Eve} - \frac{\sigma_{\mathcal{N}}^2}{\left|F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2}\right) = \frac{1}{n} \sum_{i=0}^{n-1} \left(\nu_{Eve} - \nu_i\right), \tag{70}$$

where ν is shown in (66). One can readily see that in (70), 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:

$$\sigma_\omega^2 = \frac{1}{l} \sum_{i=0}^{l-1} \left(\nu_{Eve} - \frac{\sigma_{\mathcal{N}}^2}{\max_i \left|F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2}\right) = \nu_{Eve} - \min\left(\nu_i\right). \tag{71}$$

It is particular convenient, since at a given ν_{Eve} bound, it is enough to find a given $\max_i \left|F\left(T_{0\ldots l-1}\left(\mathcal{N}_{0\ldots l-1}\right)\right)\right|^2$ for those $\mathcal{N}_i$ sub-channels, for which $\nu_i < \nu_{Eve}$ hold (*Note*: It can be determined in a pre-calibration phase prior to the main run of the protocol. In practice, this phase can be established in one simple step by sending empty "pilot" continuous variables over the sub-channels that contain no valuable information.), and then allocating the same modulation variance σ_ω^2 for all of these sub-channels.

Particularly, the significance of the adaptive-variance modulation proposed in (71) 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],

19

[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.

The algorithm of the optimal constant [9-10] modulation variance adaption is summarized as follows.

Algorithm

1. *Let the squared magnitudes of the Fourier-transformed sub-channel transmittance coefficients given in an ordered list*
   $L = \left| F\left(T_{0...l}\left(\mathcal{N}_{0...l-1}\right)\right)\right|^2$ *so that* $\left| F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2 \geq \left| F\left(T_{i+1}\left(\mathcal{N}_{i+1}\right)\right)\right|^2$
   and $\nu_i \leq \nu_{i+1}$, *and let* λ *be the Lagrange coefficient and* $\nu_{Eve} = 1/\lambda$.
   Let χ *be the largest index in the list, denoted by* $L\left(\chi\right)$, *for which*
   $\left| F\left(T_\chi\left(\mathcal{N}_\chi\right)\right)\right|^2 > \lambda$. *For* $L\left(i > \chi\right)$, $\left| F\left(T_{\chi+1...n}\left(\mathcal{N}_{\chi+1...n}\right)\right)\right|^2 \leq \lambda$.

2. *Determine the constant modulation variance* σ_ω^2 *as* $\sigma_\omega^2 = \frac{1}{\chi}\sum_\chi \sigma_{\omega_i}^2$.

3. *If* $\nu_{\chi+1} \geq \sigma_\omega^2 + \nu_1$ *then* $L\left(\chi\right) = L\left(\chi-1\right)$, *and re-determine* σ_ω^2 *as*
   $\sigma_\omega^2 = \frac{1}{\chi-1}\sum_{\chi-1} \sigma_{\omega_i}^2$.

4. *If* $\nu_{\chi+1} < \sigma_\omega^2 + \nu_1$, *then* $L\left(\chi\right) = L\left(\chi+1\right)$, *compute*
   $\sum_{i=1}^{\chi+1} \log_2\left(1 + \frac{\sigma_\omega^2\left|F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2}{\sigma_{\mathcal{N}}^2}\right)$, *where* $\left| F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2 = \left|\sum_{k=0}^{n-1} T_k e^{\frac{-i2\pi ik}{n}}\right|^2$.

The rate over the $\chi+1$ Gaussian sub-channels is $R = \sum_{\chi+1} \log_2\left(1 + \frac{\sigma_\omega^2\left|F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2}{\sigma_{\mathcal{N}}^2}\right)$, which approximates the complex domain capacity by precisely $\sum_{\chi+1} 2^{-\log_2\left(1 + \frac{\sigma_\omega^2\left|F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2}{\sigma_{\mathcal{N}}^2}\right)} / \ln 2$ [9-10].

The modulation variance adaption scheme is summarized in Fig. 5. 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 (71), 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., $\sigma_{\omega_i}^2 = 0$.
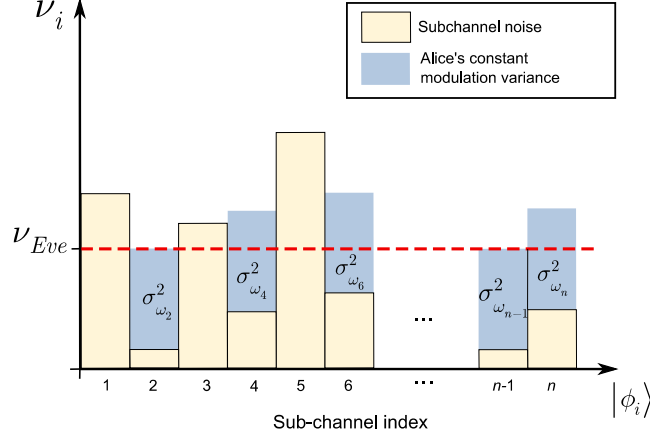
Figure 5. The constant modulation variance allocation mechanism. If the i-th sub-channel $\mathcal{N}_i$ is very noisy, i.e., $\nu_i \geq \nu_{Eve}$, Alice will not use that sub-channel, i.e., the modulation variance $\sigma^2_{\omega_i}$ of $|\phi_i\rangle$ is 0. Only those sub-channels will be used 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 $\sigma^2_{\omega_i} = \nu_{Eve} - \min\left(\nu_0, \ldots, \nu_{n-1}\right)$, 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.

The adaptive modulation variance can be rephrased in terms of the normalized $\frac{1}{n}\left|T\left(\mathcal{N}\right)\right|^2$ squared magnitude of the channel transmittance $T\left(\mathcal{N}\right)$, where n is the number of subcarrier CVs. Let $\nu = \sigma^2_{\mathcal{N}} \left/ \left|F\left(\frac{1}{n}\left|T\left(\mathcal{N}\right)\right|^2\right)\right|^2 \right.$, and $\sigma^2_{\omega}\left(\frac{1}{n}\left|T\left(\mathcal{N}\right)\right|^2\right) = \nu_{Eve} - \frac{\sigma^2_{\mathcal{N}}}{\max\left|F\left(\frac{1}{n}\left|T\left(\mathcal{N}\right)\right|^2\right)\right|^2}$. In this approach, the optimal modulation variance is

$$\int_0^{\frac{1}{2}\left|T\left(\mathcal{N}\right)\right|^2} \sigma^2_{\omega}\left(x\right) dx = \sigma^2_{\omega}, \tag{72}$$

where $x = \frac{1}{n}\left|T\left(\mathcal{N}\right)\right|^2$, see (71).

In Fig. 6, the adaptive modulation variance technique in terms of the normalized quantity [6] $\frac{1}{n}\left|T\left(\mathcal{N}\right)\right|^2$ and parameter $\nu = \sigma^2_{\mathcal{N}} \left/ \left|F\left(\frac{1}{n}\left|T\left(\mathcal{N}\right)\right|^2\right)\right|^2 \right.$ is shown. The maximal value of $\left|F\left(T\right)\right|^2$ is obtained at $\frac{1}{n}\left|T\left(\mathcal{N}\right)\right|^2 \to 0$, because as n increases, the normalized quantity represents a finer sampling of $T\left(\mathcal{N}\right)$ of the physical quantum link.

21
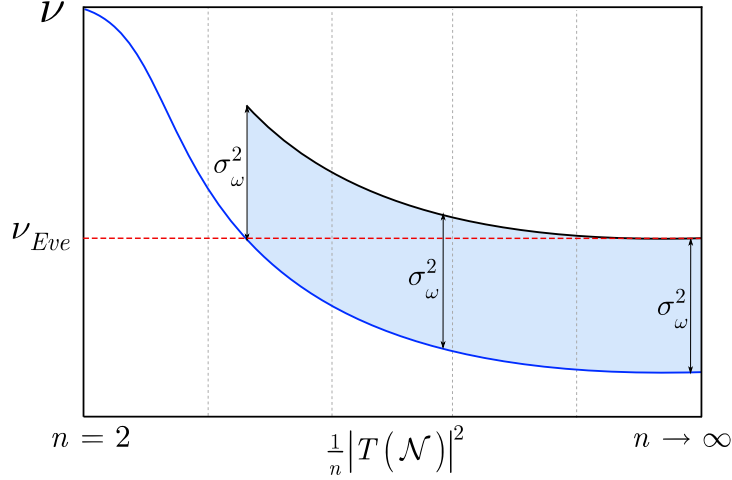
Figure 6. The constant modulation variance allocation in function of the normalized squared magnitude. As the number of subcarrier goes to infinity, the rate goes arbitrary close to the real capacity of the Gaussian quantum channel. Only those sub-channels get nonzero modulation variance σ_ω^2 for which $\nu_i < \nu_{Eve}$ holds.

For the l Gaussian sub-channels $\mathcal{N}_i$, $\nu_i < \nu_{Eve}$, the mutual information is evaluated as follows. Assuming a single-carrier modulation over a Gaussian channel $\mathcal{N}$ with noise variance $\sigma_{\mathcal{N}}^2$, and modulation variance $\sigma_{\omega_0}^2$, let the $R_{single}\left(\mathcal{N}\right)$ maximal rate between Alice and Bob is

$$R_{single}\left(\mathcal{N}\right) = \log_2\left(1 + \frac{\sigma_{\omega_0}^2 \left|T(\mathcal{N})\right|^2}{\sigma_{\mathcal{N}}^2}\right). \tag{73}$$

For the l Gaussian sub-channels $R_{AMQD}\left(\mathcal{N}\right)$ is evaluated as

$$R_{AMQD}\left(\mathcal{N}\right) = \max_{\forall i} \sum_{i=0}^{l-1} \log_2\left(1 + \frac{\sigma_{\omega_i}^2 \left|F\left(T_i(\mathcal{N}_i)\right)\right|^2}{\sigma_{\mathcal{N}}^2}\right), \tag{74}$$

where $\sigma_{\mathcal{N}}^2 = \sigma_{\mathcal{N}}^2 \mathbf{I}_{l \times l} = \frac{1}{l}\sum_{i=0}^{l-1}\sigma_{\mathcal{N}_i}^2$ follows from (52) for the noise variance of the l Gaussian sub-channels. For the σ_ω^2 averaged modulation variance of the l sub-channels, the relation

$$\sigma_\omega^2 = \frac{1}{l}\sum_{i=0}^{l-1}\sigma_{\omega_i}^2 < \sigma_{\omega_0}^2 \tag{75}$$

follows, see (58). The multicarrier modulation transmits the same amount of information, hence at (75), $\sigma_{\omega_0}^2 \left|T\left(\mathcal{N}\right)\right|^2 = \frac{1}{l}\sum_l \sigma_{\omega_i}^2 \left|F\left(T\left(\mathcal{N}_i\right)\right)\right|^2$ holds, i.e.,

$$R_{AMQD}\left(\mathcal{N}\right) = R_{single}\left(\mathcal{N}\right). \tag{76}$$

Furthermore, (76) can be increased by improving the average modulation variance in (75) up to $\sigma_\omega^2 = \sigma_{\omega_0}^2$. In this case, between (73) at $\sigma_{\omega_0}^2$, and (74) at $\sigma_\omega^2 = \sigma_{\omega_0}^2$, the connection is $\sigma_{\omega_0}^2 \left| T\left(\mathcal{N}\right)\right|^2 < \frac{1}{l}\sum_l \sigma_{\omega_i}^2 \left| F\left(T\left(\mathcal{N}_i\right)\right)\right|^2$, hence:

$$R_{AMQD}\left(\mathcal{N}\right) > R_{single}\left(\mathcal{N}\right), \tag{77}$$

which shows that better rates can be reached by the AMQD modulation at a given noise variance $\sigma_\mathcal{N}^2$ and modulation variance $\sigma_{\omega_0}^2$, in comparison to the single-carrier modulation.

Let $0 \leq \Omega \leq 1$ be the probability that the $\sum_l \left| F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2$ sum of the squared magnitude of the Fourier transformed channel transmission coefficients of the l Gaussian sub-channels pick up the maximum $\sum_l \left| F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2 = \max_{\forall i} \sum_l \left| F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2$:

$$\Omega = \Pr\left(\sum_l \left| F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2 = \max_{\forall i}\sum_l \left| F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2\right). \tag{78}$$

From this, the achievable rate is

$$R_{AMQD}\left(\mathcal{N}\right) = \Omega \log_2\left(1 + \frac{\max_i \sum_l \left| F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2}{\Omega} \cdot \mathrm{SNR}\right). \tag{79}$$

It can be concluded that the adaptive modulation variance increases the performance, especially in low SNR regimes, in which situation a constant modulation variance for all sub-channels is optimal. It also optimizes the received modulation variance at the decoder.

Finally, in terms of (72) the rate is evaluated as

$$R_{AMQD}\left(\mathcal{N}\right) = \int_0^{\frac{1}{2}\left| T\left(\mathcal{N}\right)\right|^2} \log_2\left(1 + \frac{\sigma_\omega^2\left(x\right)\left| F\left(\frac{1}{n}\left| T\left(\mathcal{N}\right)\right|^2\right)\right|^2}{\sigma_\mathcal{N}^2}\right) dx\,, \tag{80}$$

where $x = \frac{1}{n}\left| T\left(\mathcal{N}\right)\right|^2$ and $n \to \infty$.

These results conclude the proof of Theorem 2.

■

5 Tolerable Excess Noise of AMQD

Theorem 3 (Tolerable excess noise of the AMQD modulation). *At a given $\left| T\left(\mathcal{N}\right)\right|^2$, $N_{tol,AMQD} \geq N_{tol,single}$, where $N_{tol,single}$ and $N_{tol,AMQD}$ are the tolerable excess noise of single-carrier CVQKD and AMQD.*

Proof.

The efficiency of the adaptive multicarrier division technique can be approached by how efficiently the allocated modulation variances are utilized at a given secret key rate. Assuming a single-carrier quadrature encoding-scheme with efficiency

$$\eta_{single} = \frac{bR}{\sigma_{\omega_0}^2},$$ (81)

where $b = 2$ is the number of quadrature bases (position and momentum bases), R is the secret key rate, and $\sigma_{\omega_0}^2$ is the modulation variance used for the modulation of n coherent states. In the adaptive multicarrier division technique, the rate R given in (81) can be reached with efficiency:

$$\eta_{AMQD} = \frac{bR}{\sigma_\omega^2},$$ (82)

where σ_ω^2 is the constant modulation variance is used for the l subcarriers. If $\sigma_\omega^2 < \sigma_{\omega_0}^2$ holds at a given R, the multicarrier modulation scheme transmits the same amount of information such as the single-carrier modulation scheme, with increased efficiency, $\eta_{AMQD} > \eta_{single}$.

The improvement in the tolerable loss is as follows. In the single-carrier modulation scheme, at the 3.1 dB of signal attenuation the quantum channel makes no possible to transmit any information. In the multicarrier modulation, the tolerable loss is more than 3.1 dB at the same modulation variance $\sigma_{\omega_0}^2$ (justified by the convention of full width at half maximum (FWHM)).

For $\sigma_{\omega_0}^2$ and AMQD modulation, the -3.1 dB attenuation brings up at diverse amount of loss, which is equivalent to the use of an improved *virtual* modulation variance $A\sigma_{\omega_0}^2$, where $A > 1$. At $\sigma_{\omega_0}^2$, a higher modulation variance $A\sigma_{\omega_0}^2$ can be virtually simulated by the multicarrier transmission, which result higher tolerable loss (dBs) and higher tolerable excess noise in overall. To demonstrate it, let the input Gaussian be

$$g_1\left(x\right) = \frac{1}{\sigma_{\omega_0}\sqrt{2\pi}}e^{\frac{-x^2}{2\sigma_{\omega_0}^2}}.$$ (83)

The $\sigma_\omega^2 < \sigma_{\omega_0}^2$ modulation variance of the l sub-channels leads to a Gaussian

$$g_2\left(x\right) = \frac{1}{\sigma_\omega\sqrt{2\pi}}e^{\frac{-x^2}{2\sigma_\omega^2}}.$$ (84)

From (84) the *virtual* Gaussian signal at a modulation variance $\sigma_{\omega_0}^2$ is as follows

$$g_3\left(x\right) = \frac{1}{\sqrt{A}\sigma_{\omega_0}\sqrt{2\pi}}e^{\frac{-x^2}{2A\sigma_{\omega_0}^2}},$$ (85)

where $A\sigma_{\omega_0}^2 > \sigma_{\omega_0}^2$, and $A > 1$, which is evaluated as

$$A = \frac{\frac{1}{l}\sum_l |F(T_i(\mathcal{N}_i))|^2}{|T(\mathcal{N})|^2} = \frac{\frac{1}{l}\sum_{i=0}^{l-1}\left|\sum_{k=0}^{l-1} T_k e^{\frac{-i2\pi ik}{l}}\right|^2}{|T(\mathcal{N})|^2}. \tag{86}$$

The FWHMs of these Gaussian signals are as follows:

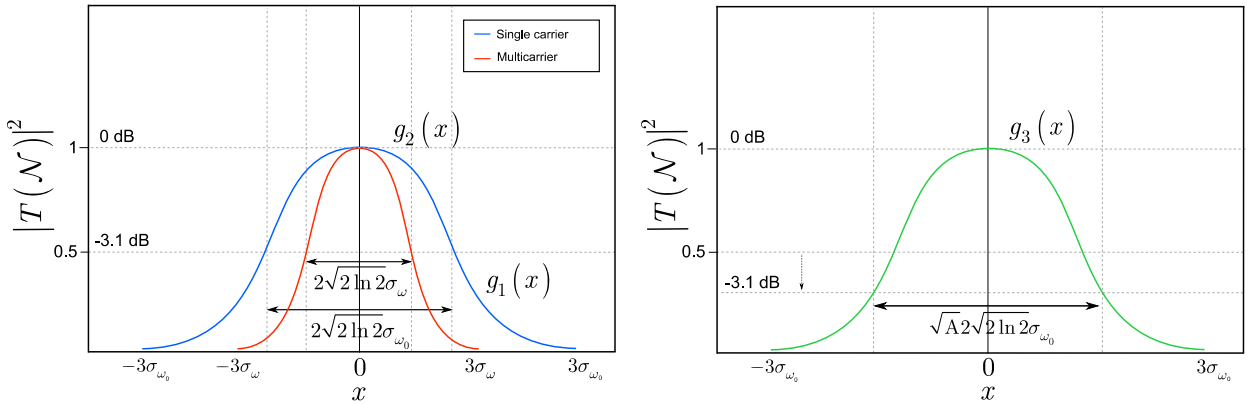$$\text{FWHM}\big(g_1(x)\big) = 2\sqrt{2\ln 2}\sigma_{\omega_0}, \tag{87}$$

$$\text{FWHM}\big(g_2(x)\big) = 2\sqrt{2\ln 2}\sigma_{\omega} \tag{88}$$

and

$$\text{FWHM}\big(g_3(x)\big) = \sqrt{A}2\sqrt{2\ln 2}\sigma_{\omega_0}. \tag{89}$$

These results are summarized in Fig. 7.

Figure 7. (a). The FWHM of the single-carrier Gaussian signal (blue) and the Gaussian signal of the subcarrier transmission (red). (b). The FWHM of the virtual Gaussian signal at a modulation variance of $\sigma_{\omega_0}^2$ is $\sqrt{A}2\sqrt{2\ln 2}\sigma_{\omega_0}$, $A > 1$. The AMQD allows more tolerable loss at a given modulation variance $\sigma_{\omega_0}^2$.

The improvement in the excess noise is as follows [3]. In the single-carrier case, at a given T_{Eve} and W, the *excess noise* is as [3]:

$$N_{single} = \frac{(W-1)\big(|T_{Eve}|^2\big)}{1-|T_{Eve}|^2}, \tag{90}$$

where $|T_{Eve}|^2 < |T|^2 \in [0,1]$ is the squared magnitude of the complex variable T_{Eve}.
In the AMQD modulation, at a given W, the excess noise is reduced to

$$N_{AMQD} = \frac{(W-1)\big(\frac{1}{n}\sum_n |F(T_{Eve,i})|^2\big)}{1-\frac{1}{n}\sum_n |F(T_{Eve,i})|^2}, \tag{91}$$

where

25

$$F\left(T_{Eve,i}\right) = \sum_{k=0}^{n-1} T_{Eve,k} e^{\frac{-i2\pi ik}{n}} \tag{92}$$

and

$$\tfrac{1}{n}\sum_n \left|F\left(T_{Eve,i}\right)\right|^2 = \tfrac{1}{n}\sum_n \left|\sum_{k=0}^{n-1} T_{Eve,k} e^{\frac{-i2\pi ik}{n}}\right|^2 \leq \left|T_{Eve}\right|^2 < \left|T\right|^2 \leq \tfrac{1}{n}\sum_n \left|F\left(T_i\right)\right|^2, \tag{93}$$

which relation is justified by the CVQFT transformation. Since, at a given W, the tolerable excess noise depends only on T_{Eve}, from (93) it follows, that in the AMQD modulation scheme higher amount of excess noise N can be tolerated.

The improvement in the tolerable excess noise can be approached by the ratio $\kappa \geq 1$ between the excess noise N_{single} and N_{AMQD} as:

$$\begin{aligned}
\kappa &= \frac{N_{single}}{N_{AMQD}} \\
&= \frac{(W-1)\left(\left|T_{Eve}\right|^2\right)}{1-\left|T_{Eve}\right|^2} \frac{1-\tfrac{1}{n}\sum_n\left|F\left(T_{Eve,i}\right)\right|^2}{(W-1)\left(\tfrac{1}{n}\sum_n\left|F\left(T_{Eve,i}\right)\right|^2\right)} \\
&= \frac{\left|T_{Eve}\right|^2 - \left|T_{Eve}\right|^2 \tfrac{1}{n}\sum_n\left|F\left(T_{Eve,i}\right)\right|^2}{\tfrac{1}{n}\sum_n\left|F\left(T_{Eve,i}\right)\right|^2 - \left|T_{Eve}\right|^2 \tfrac{1}{n}\sum_n\left|F\left(T_{Eve,i}\right)\right|^2} \\
&= \frac{\left|T_{Eve}\right|^2 - \left|T_{Eve}\right|^2 \tfrac{1}{n}\sum_n\left|F\left(T_{Eve,i}\right)\right|^2}{\left|T\right|^2 \tfrac{1}{n}\sum_n\left|F\left(T_{Eve,i}\right)\right|^2}.
\end{aligned} \tag{94}$$

The $N_{tol,AMQD}$ tolerable excess noise in AMQD modulation with homodyne measurement [3] is depicted in Fig. 8. The improvement in the tolerable excess noise is $N_{tol,AMQD} = \alpha N_{tol,single}$, where $N_{tol,single}$ is the tolerable excess noise of a single-carrier CVQKD, $\alpha = x\kappa = x N_{single}/N_{AMQD} \geq 1$, and $N_{AMQD}/N_{single} \leq x \leq 1$, yielding $N_{tol,AMQD} \geq N_{tol,single}$.
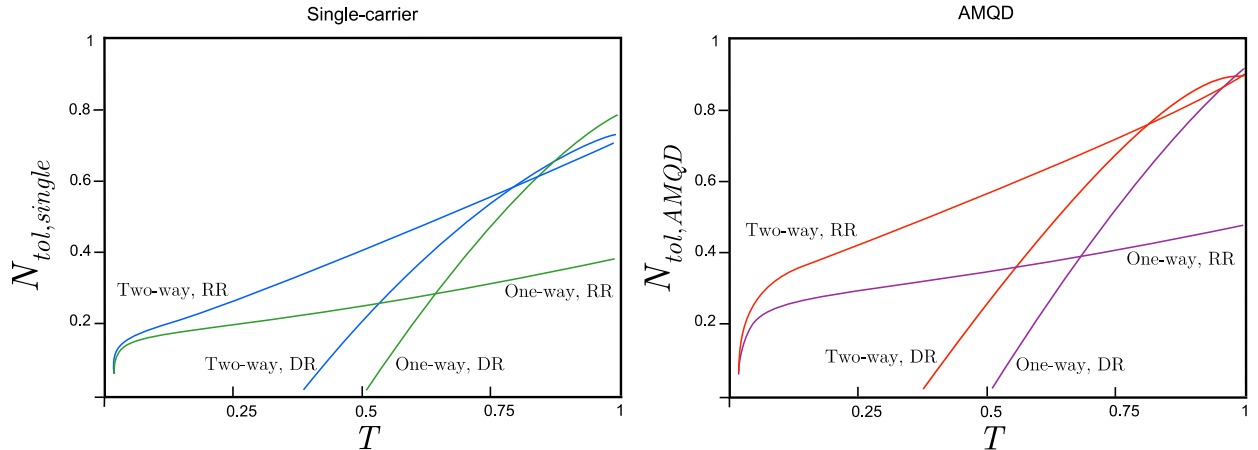
Figure 8. Tolerable excess noise in function of the T channel transmittance in a single-carrier Gaussian modulation with homodyne measurement (a) and in AMQD modulation (b). (DR – Direct Reconciliation, RR – Reverse Reconciliation, $N_{tol,single}$ and $N_{tol,AMQD}$ refer to the tolerable excess noise of single-carrier CVQKD and AMQD, respectively.)

The improvement in the amount of tolerable excess noise is more significant in two-way CVQKD, since the multicarrier transmission is present in both directions between Alice to Bob.

∎

5.1 Secret Key Rates of AMQD

To express the S secret key rates of AMQD, let l Gaussian sub-channels with $\nu_i < \nu_{Eve}$, and let the variance of Eve's EPR-ancilla W [2-3]. For a detailed proof on the achievable secret key rates and security thresholds of AMQD, see [24].

5.1.1 AMQD Modulation in One-way CVQKD

5.1.1.1 Homodyne measurement, Reverse Reconciliation

$$S_{one-way}^{RR,\mathrm{hom}} = \tfrac{1}{2}\log_2 \frac{W}{\left(1-\frac{1}{l}\sum_l \left|F(T_i(\mathcal{N}_i))\right|^2\right)b} - \left(\tfrac{W+1}{2}\log_2 \tfrac{W+1}{2} - \tfrac{W-1}{2}\log_2 \tfrac{W-1}{2}\right) \tag{95}$$

where

$$b = \left(1 - \left(\tfrac{1}{l}\sum_l \left|F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2\right)\right)W + \tfrac{1}{l}\sum_l \left|F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2. \tag{96}$$

5.1.1.2 Homodyne measurement, Direct Reconciliation

$$\begin{aligned}
S_{one-way}^{DR,\mathrm{hom}} &= \tfrac{1}{2}\log_2 \frac{\left(\frac{1}{l}\sum_l \left|F\left(T_i(\mathcal{N}_i)\right)\right|^2\right)e}{\left(1-\left(\frac{1}{l}\sum_l \left|F\left(T_i(\mathcal{N}_i)\right)\right|^2\right)\right)b} \\
&\quad + \left(\tfrac{\sqrt{Wb/e}+1}{2}\log_2 \tfrac{\sqrt{Wb/e}+1}{2} - \tfrac{\sqrt{Wb/e}-1}{2}\log_2 \tfrac{\sqrt{Wb/e}-1}{2}\right), \\
&\quad - \left(\tfrac{W+1}{2}\log_2 \tfrac{W+1}{2} - \tfrac{W-1}{2}\log_2 \tfrac{W-1}{2}\right),
\end{aligned} \tag{97}$$

where

$$e = \left(1 - \tfrac{1}{l}\sum_l \left|F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2\right) + \left(\tfrac{1}{l}\sum_l \left|F\left(T_i\left(\mathcal{N}_i\right)\right)\right|^2\right)W. \tag{98}$$

5.1.2 AMQD Modulation in Two-way CVQKD

5.1.2.1 Homodyne measurement, Reverse Reconciliation

$$S_{two-way}^{RR,\mathrm{hom}} = \tfrac{1}{2}\log_2 \frac{\left[1 - \left(\frac{1}{l}\sum_l \left|F(T_i(\mathcal{N}_i))\right|^2\right) + \left(\frac{1}{l}\sum_l \left|F(T_i(\mathcal{N}_i))\right|^2\right)^2\right]}{\left(1-\frac{1}{l}\sum_l \left|F(T_i(\mathcal{N}_i))\right|^2\right)^2} - \left(\tfrac{W+1}{2}\log_2 \tfrac{W+1}{2} - \tfrac{W-1}{2}\log_2 \tfrac{W-1}{2}\right). \tag{99}$$

5.1.2.2 Homodyne measurement, Direct Reconciliation

$$S_{two-way}^{DR,\mathrm{hom}} = \tfrac{1}{2}\log_2 \frac{\frac{1}{l}\sum_l \left|F(T_i(\mathcal{N}_i))\right|^2}{\left(1-\frac{1}{l}\sum_l \left|F(T_i(\mathcal{N}_i))\right|^2\right)^2} - \left(\tfrac{W+1}{2}\log_2 \tfrac{W+1}{2} - \tfrac{W-1}{2}\log_2 \tfrac{W-1}{2}\right). \tag{100}$$

6 Security of AMQD for Optimal Gaussian Attacks

The main result regarding the security of AMQD is summarized in Theorem 4. It states that under an optimal Gaussian collective attack, any crosstalk among the sub-channels cannot allow leaking of more information to an eavesdropper than the single-carrier CVQKD.

Theorem 4 (Unconditional security of AMQD in presence of crosstalk.). *Let $\tilde{\gamma}\left(\mathcal{N}\right) > 0$ be a nonzero crosstalk among the sub-channels in an AMQD setting, and $\chi\left(B:E\right)_{single}$ be Eve's Holevo information under an optimal Gaussian collective attack for a single-carrier CVQKD. Then, $\chi\left(B:E\right)_{\tilde{\gamma}} \leq \chi\left(B:E\right)_{single}$, where $\chi\left(B:E\right)_{\tilde{\gamma}}$ is the Holevo information of Eve in AMQD modulation in the presence of nonzero crosstalk, under an optimal Gaussian collective attack.*

Proof.
The proof will assume reverse reconciliation, hence Eve's correlation will be quantified by the preserved correlation with Bob's system (B).

First, we express the eavesdropper information under an optimal Gaussian attack in an AMQD modulation. Then, we show that this attack – besides the fact that it maximizes Eve's Holevo information – cannot leak more information to an eavesdropper than the single-carrier case. (The optimality of Gaussian collective attacks for single-carrier CVQKD has already been proven in [20], [21] and the proof follows for the multicarrier case of AMQD. Therefore, we focus mainly on the analysis of the amount of leakable information in a multicarrier CVQKD scenario, assuming an optimal Gaussian collective attack.)

The notations used in our proof are summarized as follows. Let $\rho \in \mathcal{H}$ be the density matrix of a Gaussian state, and let $\rho' \in \mathcal{H}$ be the density matrix of a non-Gaussian state with the same co-variance matrix and displacement vector. Let $p\left(x\right)$ refer to the Gaussian probability distribution, and $p'\left(x\right)$ to an arbitrary probability distribution with the same first and second momenta as $p\left(x\right)$. Let ρ_{AB} be a Gaussian state between Alice and Bob, and let ρ'_{AB} refer to an arbitrary shared state. For these density matrices, the relation between the joint entropy is $H\left(\rho_{AB}\right) \geq H\left(\rho'_{AB}\right)$.

Let's assume that a Gaussian density matrix ρ_i is transmitted through sub-channel $\mathcal{N}_i$, and the shared state between Alice, Bob and Eve that is related to the i-th sub-channel is a pure system ρ_i^{ABE}. The measurement process is characterized as follows. Let X_i be Alice's classical variable that is encoded into the input system A_i, which is a density matrix ρ_i, and let B_i be the classical variable of Bob that results from a measurement $M_i = \left\{M_{i,B_i}\right\}_{B_i}$ applied on ρ_i, where M_{i,B_i} are positive operators, $\sum_i M_{i,B_i} M_{i,B_i}^{\dagger} = I$. The conditional entropy between A_i and B_i is $H\left(A_i \mid B_i\right) = H\left(\bar{A}_i\right) - H\left(B_i\right)$, where $\bar{A}_i$ refers to the measured density matrix $\bar{\rho}_i$ [20]. Let's

denote Eve's optimal Gaussian attack on the i-th sub-channel $\mathcal{N}_i$ by the CPTP map $\mathcal{T}_i$. Taking arbitrary density matrices ρ and σ, the relation $\mathcal{D}\big(\rho\|\sigma\big) \geq \mathcal{D}\big(\mathcal{T}_i\big(\rho\big)\|\mathcal{T}_i\big(\sigma\big)\big)$ follows, where $\mathcal{D}\big(\cdot\|\cdot\big)$ is the relative entropy function, along with the entropic relation $H\big(A\big) - H\big(A'\big) \geq H\mathcal{T}\big(A\big) - H\mathcal{T}\big(A'\big)$ [20].

In the next step, we express the Holevo information of the eavesdropper $\chi\big(B_i : E_i\big)_{\gamma,\mathcal{N}_i}$ on a sub-channel $\mathcal{N}_i$, assuming reverse reconciliation, and optimal Gaussian attack, where B_i is Bob's variable from the i-th sub-channel, while E_i identifies Eve's variable. During the optimal Gaussian attack against AMQD, Eve attacks each sub-channel separately with a beam splitter that has transmittance $T_{Eve,i}$.

Assuming an average modulation variance $\sigma_\omega^2 = \frac{1}{l}\sum_l \sigma_{\omega_i}^2 < \sigma_{\omega_0}^2$ in the AMQD setting with l sub-channels for the transmittance ($\sigma_{\omega_i}^2$-s are constant values due to the optimality consumption, see Theorem 2), the following relation holds for the Holevo information of the eavesdropper:

$$
\begin{aligned}
\tilde{\chi}\big(B : E\big) &= H\big(E\big) - H\big(E\,\big|\,B\big)\\
&= \tfrac{1}{l}\sum_l\big(H\big(E_i\big) - H\big(E_i\,\big|\,B_i\big)\big)\\
&\leq \chi\big(B : E\big)_{single} = H\big(E\big) - H\big(E\,\big|\,B\big)_{single}.
\end{aligned}
\tag{101}
$$

This relation follows from that in an AMQD modulation $H\big(E\,\big|\,X\big) \geq H\big(E\,\big|\,X\big)_{single}$, because the same amount of information is transmitted via modulation variance $\sigma_\omega^2 < \sigma_{\omega_0}^2$ over the l sub-channels.

At this point, we add the $\gamma > 0$ *crosstalk* into the picture. Assuming the use of sub-channel $\mathcal{N}_i$, the optimal Gaussian attack leads to

$$
\begin{aligned}
\chi\big(B : E\big)_{\gamma,\mathcal{N}_i} &= \chi\big(B : E\big)_{\mathcal{N}_i} + \big|T_{Eve,i}\big|^2 \gamma\big(\mathcal{N}_i\big)\\
&= \chi\big(B : E\big)_{\mathcal{N}_i} + \sum_{j\neq i}\big|T_{Eve,i}\big|^2 x_j\chi\big(A_j : B_j\big).
\end{aligned}
\tag{102}
$$

The average modulation ω on the l sub-channels leads to average Holevo information

$$
\tilde{\chi}\big(B : E\big) = \tfrac{1}{l}\sum_l \chi\big(B : E\big)_{\mathcal{N}_i},
\tag{103}
$$

while the average amount of crosstalk over all the n sub-channels is evaluated as

$$
\begin{aligned}
\tilde{\gamma}\big(\mathcal{N}\big) &= \tfrac{1}{n}\sum_n \gamma\big(\mathcal{N}_i\big)\\
&= \tfrac{1}{n}\sum_n\sum_{j\neq i} x_j\chi\big(A_j : B_j\big),
\end{aligned}
\tag{104}
$$

which together leads to the averaged Holevo information $\tilde{\chi}\big(B : E\big)_\gamma$ over all the (n) sub-channels, as

$$
\begin{aligned}
\tilde{\chi}\left(B:E\right)_{\tilde{\gamma}} &= \tfrac{1}{l}\sum_{l}\chi\left(B:E\right)_{\mathcal{N}_i} + \tfrac{1}{n}\sum_{n}\left|T_{Eve,i}\right|^2 \gamma\left(\mathcal{N}_i\right) \\
&= \tfrac{1}{l}\sum_{l}\chi\left(B:E\right)_{\mathcal{N}_i} + \tfrac{1}{n}\sum_{n}\sum_{j\neq i}\left|T_{Eve,i}\right|^2 x_j\chi\left(A_j:B_j\right) \\
&= \tfrac{1}{l}\sum_{l}\chi\left(B:E\right)_{\mathcal{N}_i} + \tfrac{1}{n}\sum_{j\neq i}\left|T_{Eve}\right|^2 x_j\chi\left(A_j:B_j\right) \\
&= \tfrac{1}{l}\sum_{l}\chi\left(B:E\right)_{\mathcal{N}_i} + \tfrac{1}{n}\sum_{n}\left|T_{Eve}\right|^2 \gamma\left(\mathcal{N}_i\right) \\
&= \tilde{\chi}\left(B:E\right) + \left|T_{Eve}\right|^2 \tilde{\gamma}\left(\mathcal{N}\right),
\end{aligned}
\tag{105}
$$

where $\left|T_{Eve}\right|^2 = \tfrac{1}{n}\sum_{n}\left|T_{Eve,i}\right|^2$.

For this quantity, the relation

$$
\tilde{\chi}\left(B:E\right)_{\tilde{\gamma}} \leq \chi\left(B:E\right)_{single}
\tag{106}
$$

follows, since for $\tilde{\gamma}\left(\mathcal{N}\right) > 0$

$$
\begin{aligned}
\tilde{\chi}\left(B:E\right) &= H\left(E\right) - H\left(E\big|B\right) \\
&< \tilde{\chi}\left(B:E\right)_{\tilde{\gamma}} = H\left(E\right) - H\left(E\big|B\right)_{\tilde{\gamma}} \\
&\leq \chi\left(B:E\right)_{single} = H\left(E\right) - H\left(E\big|B\right)_{single},
\end{aligned}
\tag{107}
$$

and

$$
H\left(E\big|B\right) > H\left(E\big|B\right)_{\tilde{\gamma}} \geq H\left(E\big|B\right)_{single}.
\tag{108}
$$

The relation $H\left(E\big|B\right) > H\left(E\big|B\right)_{\tilde{\gamma}}$ holds for any $\tilde{\gamma}\left(\mathcal{N}\right) > 0$. The RHS of (108) is verified by the fact that a nonzero crosstalk has no relevance on the mutual information of Alice and Bob, i.e., communicating at a constant modulation variance $\sigma_{\omega}^2 < \sigma_{\omega_0}^2$ on the l sub-channels, the relation $H\left(B\big|A\right) = H\left(B\big|A\right)_{\tilde{\gamma}} = H\left(B\big|A\right)_{single}$ follows for an AMQD modulation. The first equality follows from the fact that the presence of any nonzero crosstalk does not change on the mutual information of the legally parties, while the second comes from that in an AMQD modulation the same amount of information transmitted than single-carrier CVQKD via lower modulation variance (see (75)), from which (108) is immediately concluded.

Finally, we show that the Gaussian collective attack is optimal in the AMQD modulation. Fixing the first and second moments, under an optimal Gaussian attack for all sub-channels $\mathcal{N}_i$, $i = 1\ldots n$, and with a nonzero crosstalk $\tilde{\gamma}\left(\mathcal{N}\right) > 0$, by the optimality consumption one obtains nonnegative $\Delta \geq 0$ for the difference of Eve's Holevo information that results from an optimal Gaussian and an arbitrary attack:

$$
\begin{aligned}
\Delta &= \tilde{\chi}\left(B:E\right)_{\tilde{\gamma}} - \tilde{\chi}\left(B':E'\right)_{\tilde{\gamma}} \\
&= \tfrac{1}{l}\left(\textstyle\sum_l \left(H\left(E_i\right) - H\left(E_i'\right)\right) - \sum_l \left(H\left(E_i\,\middle|\,B_i\right) - H\left(E_i'\,\middle|\,B_i'\right)\right)\right) \\
&\quad + \tfrac{1}{n}\textstyle\sum_n \left(\sum_{j\neq i}\left|T_{Eve,i}\right|^2 x_j \chi\left(A_j:B_j\right) - \sum_{j\neq i}\left|T_{Eve,i}\right|^2 x_j \chi'\left(A_j:B_j\right)\right) \\
&= \left(H\left(E\right) - H\left(E'\right)\right) - \left(H\left(E\,\middle|\,B\right) - H\left(E'\,\middle|\,B'\right)\right) \\
&\quad + \left(\left|T_{Eve}\right|^2 \tilde{\gamma}\left(\mathcal{N}\right) - \left|T_{Eve}\right|^2 \tilde{\gamma}'\left(\mathcal{N}\right)\right) \\
&= \left(H\left(AB\right) - H\left(A'B'\right)\right) - \left(H\left(AB\,\middle|\,X\right) - H\left(A'B'\,\middle|\,X'\right)\right) \\
&\quad + \left(\left|T_{Eve}\right|^2 \tilde{\gamma}\left(\mathcal{N}\right) - \left|T_{Eve}\right|^2 \tilde{\gamma}'\left(\mathcal{N}\right)\right) \\
&= \left(H\left(AB\right) - H\left(A'B'\right)\right) - \left(H\left(\overline{A}\,\overline{B}\right) - H\left(\overline{A}'\,\overline{B}'\right)\right) + \left(H\left(X\right) - H\left(X'\right)\right) \\
&\quad + \left(\left|T_{Eve}\right|^2 \tilde{\gamma}\left(\mathcal{N}\right) - \left|T_{Eve}\right|^2 \tilde{\gamma}'\left(\mathcal{N}\right)\right),
\end{aligned}
\tag{109}
$$

where $\tilde{\chi}\left(B':E'\right)_{\tilde{\gamma}}$ is Eve's average Holevo information in an AMQD modulation for an arbitrary attack, $\tilde{\chi}\left(B:E\right)_{\tilde{\gamma}}$ is evaluated by (105), while $\left|T_{Eve}\right|^2 \tilde{\gamma}\left(\mathcal{N}\right)$ and $\left|T_{Eve}\right|^2 \tilde{\gamma}'\left(\mathcal{N}\right)$ refer to the leaked valuable crosstalk information under an optimal Gaussian and an arbitrary attack, respectively.

Since any nonzero crosstalk $\tilde{\gamma}\left(\mathcal{N}\right) > 0$ acts as a Gaussian noise for the receiver that is already included in the sub-channel noise variance $\sigma^2_{\mathcal{N}_i}$, see (64), the next equation is straightforward for the minimized mutual information under an optimal Gaussian collective attack:

$$
\begin{aligned}
I\left(A:B\right) - I\left(A':B'\right) &= \tfrac{1}{l}\left(\textstyle\sum_l I\left(A_j:B_j\right) - \sum_l I\left(A_j':B_j'\right)\right) \\
&= \tfrac{1}{l}\left(\textstyle\sum_l \left(H\left(A_j\right) - H\left(A_j'\right)\right) + \sum_l \left(H\left(B_j\right) - H\left(B_j'\right)\right)\right. \\
&\quad \left. - \textstyle\sum_l \left(H\left(A_j B_j\right) - H\left(A_j'B_j'\right)\right)\right) \\
&= \tfrac{1}{l}\left(\textstyle\sum_l \left(H\left(B_j\right) - H\left(B_j'\right)\right) - \sum_l \left(H\left(A_j B_j\right) - H\left(A_j'B_j'\right)\right)\right) \\
&\leq 0.
\end{aligned}
\tag{110}
$$

Thus, Eve's Gaussian collective attack remains optimal in an AMQD modulation (i.e., Eve's Holevo information is maximized), and the presence of a nonzero crosstalk has no effect on the mutual information between Alice and Bob.

On the other hand, Eve's Holevo information could be slightly improved by a nonzero crosstalk, to be precise by $\left|T_{Eve}\right|^2 \tilde{\gamma}\left(\mathcal{N}\right)$, however an AMQD modulation does not allow leaking of more information to Eve than the single-carrier CVQKD. The argumentation behind this is as follows. The inequality

$$
\begin{aligned}
\chi\left(B:E\right)_{single} - \tilde{\chi}\left(B:E\right)_{\tilde{\gamma}} &\geq 0 \\
\chi\left(B:E\right)_{single} - \left(\tilde{\chi}\left(B:E\right) + \left|T_{Eve}\right|^2 \tilde{\gamma}\left(\mathcal{N}\right)\right) &\geq 0
\end{aligned}
\tag{111}
$$

directly comes from (105), which combined with (108) leads to

$$
\chi\left(B:E\right)_{single} - \tilde{\chi}\left(B:E\right) \geq \left|T_{Eve}\right|^2 \tilde{\gamma}\left(\mathcal{N}\right),
\tag{112}
$$

which reveals that in an AMQD modulation, the degradation of Eve's Holevo information in comparison to the single-carrier CVQKD is always equal to or greater than the valuable information that is leaked from the crosstalk to Eve, thus

$$\tilde{\chi}\left(B:E\right) < \tilde{\chi}\left(B:E\right)_{\tilde{\gamma}} < \chi\left(B:E\right)_{single} - \left|T_{Eve}\right|^{2}\tilde{\gamma}\left(\mathcal{N}\right), \tag{113}$$

hence for any $\left|T_{Eve}\right|^{2}\tilde{\gamma}\left(\mathcal{N}\right)$, the inequality

$$\chi\left(B:E\right)_{\tilde{\gamma}} \leq \chi\left(B:E\right)_{single} \tag{114}$$

immediately follows.

These results lead to the S_{AMQD} secret key rates for reverse reconciliation at an AMQD modulation, under an optimal Gaussian collective attack:

$$S_{AMQD} = I\left(A:B\right) - \tilde{\chi}\left(B:E\right)_{\tilde{\gamma}}, \tag{115}$$

and, if Bob is allowed to perform a collective measurement, then the secret key rate is

$$S_{AMQD} = \chi\left(A:B\right) - \tilde{\chi}\left(B:E\right)_{\tilde{\gamma}}. \tag{116}$$

For the rigorous proofs of the achievable secret key rates of AMQD at a homodyne and heterodyne measurement, see the derivations of [24]. For an adaptive quadrature measurement scheme for multicarrier CVQKD, see [27].

These results prove the unconditional security of AMQD against optimal Gaussian collective attacks, which concludes the proof.

∎

7 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

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] William Shieh and Ivan Djordjevic. *OFDM for Optical Communications.* Elsevier (2010).

[20] Miguel Navascues, Frederic Grosshans, and Antonio Acin. Optimality of Gaussian Attacks in Continuous Variable Quantum Cryptography, *Phys. Rev. Lett. 97, 190502* (2006).

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

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

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

[24] L. Gyongyosi, Security Thresholds of Multicarrier Continuous-Variable Quantum Key Distribution, *arXiv:1404.7109* (2014).

[25] L. Gyongyosi, Multidimensional Manifold Extraction for Multicarrier Continuous-Variable Quantum Key Distribution, *arXiv:1405.6948* (2014).

[26] L. Gyongyosi, Subcarrier Domain of Multicarrier Continuous-Variable Quantum Key Distribution, *arXiv:1406.6949* (2014).

[27] L. Gyongyosi, Adaptive Quadrature Detection for Multicarrier Continuous-Variable Quantum Key Distribution, *arXiv:1408.6493* (2014).

[28] L. Gyongyosi, S. Imre, Geometrical Analysis of Physically Allowed Quantum Cloning Transformations for Quantum Cryptography, *Information Sciences,* Elsevier, pp. 1-23, DOI: 10.1016/j.ins.2014.07.010 (2014).

[29] L. Gyongyosi ; S. Imre, Adaptive multicarrier quadrature division modulation for long-distance continuous-variable quantum key distribution, *Proc. SPIE 9123, Quantum Information and Computation XII*, 912307 (May 22, 2014); doi:10.1117/12.2050095, From Conference Volume 9123, Quantum Information and Computation XII, > Baltimore, Maryland, USA (2014).

Supplemental Information

S.1 Notations

The notations of the manuscript are summarized in Table S.1.

Table S.1. The summary of the notations.

Notation	Description
$F(\cdot) = \mathrm{CVQFT}(\cdot)$	The CVQFT transformation, applied on Bob's side, continuous variable U unitary operation.
$F^{-1}(\cdot) = \mathrm{IFFT}(\cdot)$	Inverse FFT transform, applied on Alice's side.
$\sigma^2_{\omega_0}$	Single-carrier modulation variance.
$\sigma^2_\omega = \frac{1}{l}\sum_l \sigma^2_{\omega_i}$	Multicarrier modulation variance. Average modulation variance of the l Gaussian sub-channels $\mathcal{N}_i$.
$\mathbf{z} = \mathbf{x} + i\mathbf{p} = (z_0, \ldots, z_{n-1})^T \in \mathcal{CN}(0, \mathbf{K_z})$	An n-dimensional, zero-mean, circular symmetric complex random Gaussian vector, $\mathbf{K_z} = \mathbb{E}\left[\mathbf{zz}^\dagger\right]$, where $z_i = x_i + ip_i$, $\mathbf{x} = (x_0, \ldots, x_{n-1})^T$ and $\mathbf{p} = (p_0, \ldots, p_{n-1})^T$, and $x_i \in \mathbb{N}(0, \sigma^2_{\omega_0})$, $p_i \in \mathbb{N}(0, \sigma^2_{\omega_0})$ are i.i.d. zero-mean Gaussian random variables.
$\mathbf{d} = F^{-1}(\mathbf{z}) \in \mathcal{CN}(0, \mathbf{K_d})$	An n-dimensional, zero-mean, circular symmetric complex random Gaussian vector, $\mathbf{K_d} = \mathbb{E}\left[\mathbf{dd}^\dagger\right]$, $\mathbf{d} = (d_0, \ldots, d_{n-1})^T$, $d_i = x_i + ip_i$, $x_i \in \mathbb{N}(0, \sigma^2_{\omega_F})$, $p_i \in \mathbb{N}(0, \sigma^2_{\omega_F})$ are i.i.d. zero-mean Gaussian random variables, $\sigma^2_{\omega_F} = 1/\sigma^2_{\omega_0}$. The i-th component is $d_i \in \mathcal{CN}(0, \sigma^2_{d_i})$, with variance $\sigma^2_{d_i} = \mathbb{E}\left[\left|d_i\right|^2\right]$.
$\left|\phi_i\right\rangle = \left|F^{-1}(z_i)\right\rangle = \left|d_i\right\rangle$	The i-th subcarrier Gaussian CV, where F^{-1} stands for the inverse FFT.
$\left|\varphi_i\right\rangle = F(\left|\phi_i\right\rangle) = \left|F(F^{-1}(z_i))\right\rangle = \left|z_i\right\rangle$	Bob's decoded Gaussian state, the CVQFT-

	transformed $\left\vert \phi_i \right\rangle$ subcarrier CV.
$\mathcal{N}$	Gaussian quantum channel in the single-carrier transmission.
$\mathcal{N}_i, i = 0,\ldots,n-1$	Gaussian sub-channels in the multicarrier transmission.
$T\left(\mathcal{N}\right) = \operatorname{Re} T\left(\mathcal{N}\right) + \mathrm{i}\operatorname{Im} T\left(\mathcal{N}\right) \in \mathcal{C}$	Channel transmittance, normalized complex variable. The real part identifies the position quadrature transmission, the imaginary part stand for the transmittance of the position quadrature.
$T\left(\mathcal{N}_i\right) = \operatorname{Re} T\left(\mathcal{N}_i\right) + \mathrm{i}\operatorname{Im} T\left(\mathcal{N}_i\right) \in \mathcal{C}$	Transmittance of the i-th sub-channel.
T_{Eve}	Eve's transmittance, $T_{Eve} = 1 - T\left(\mathcal{N}\right)$.
$T_{Eve,i}$	Eve's transmittance for the i-th subcarrier CV.
W	Variance of Eve's EPR ancilla used in the entangling cloner attack.
$\Delta \in \mathcal{CN}\left(0, \mathfrak{C}\left(\Delta\right)\right)$	Gaussian noise of the quantum channel $\mathcal{N}$, zero-mean, circular symmetric complex Gaussian random vector with variance $\mathfrak{C}\left(\Delta\right) = \mathbb{E}\left[\Delta\Delta^\dagger\right]$, and with quadrature components $\Delta_{x_i} \in \mathbb{N}\left(0, \sigma^2_{\mathcal{N}_i}\right)$, $\Delta_{p_i} \in \mathbb{N}\left(0, \sigma^2_{\mathcal{N}_i}\right)$.
$\left\vert \varphi'_i \right\rangle = \left\vert x'_i + \mathrm{i}p'_i \right\rangle = \left\vert z'_i \right\rangle$	Bob's Gaussian coherent state in the phase space. Modeled as a zero-mean, circular symmetric complex Gaussian random variable $z_i \in \mathcal{CN}\left(0, \sigma^2_{z_i}\right)$, $\sigma^2_{z_i} = \mathbb{E}\left[\left\vert z_i \right\vert^2\right]$, $z_i = x_i + \mathrm{i}p_i$, with quadrature components $x_i \in \mathbb{N}\left(0, \sigma^2_{\omega_0}\right)$, $p_i \in \mathbb{N}\left(0, \sigma^2_{\omega_0}\right)$, which are i.i.d. zero-mean Gaussian random variables.
$F\left(\mathbf{T}\left(\mathcal{N}\right)\right)$	The CVQFT transform of transmittance matrix $\mathbf{T}\left(\mathcal{N}\right) \in \mathcal{C}^n$, n dimensional complex vector.
$F\left(\Delta\right) \in \mathcal{CN}\left(0, \mathfrak{C}\left(F\left(\Delta\right)\right)\right)$	The CVQFT transform of vector Δ. An n-dimensional zero-mean, circular symmetric complex Gaussian random vector, where $\mathfrak{C}\left(F\left(\Delta\right)\right) = \mathbb{E}\left[F\left(\Delta\right)F\left(\Delta\right)^\dagger\right]$, and the quadrature components are $F\left(\Delta_{x_i}\right) \in \mathbb{N}\left(0, \sigma^2_{F\left(\mathcal{N}_i\right)}\right)$, $F\left(\Delta_{p_i}\right) \in \mathbb{N}\left(0, \sigma^2_{F\left(\mathcal{N}_i\right)}\right)$, where $\sigma^2_{F\left(\mathcal{N}\right)} < \sigma^2_{\mathcal{N}}$.

$\mathbf{y}[j] = F\big(\mathbf{T}(\mathcal{N})\big)F(\mathbf{d})[j] + F(\Delta)[j],$ $j = 1,\dots,n.$	An AMQD block. Formulated by n Gaussian subcarrier continuous variables, where j is the index of the AMQD block, and $$\mathbf{y}[j] = \big(y_1[j],\dots,y_n[j]\big)^T$$ $$F(\mathbf{d})[j] = \big(F(d_1)[j],\dots,F(d_n)[j]\big)^T,$$ $$F(\Delta)[j] = \big(F(\Delta_1)[j],\dots,F(\Delta_n)[j]\big)^T.$$
$\tau = \big\|F(\mathbf{d})[j]\big\|^2$	Exponentially distributed variable, $\mathbb{E}[\tau] \leq n2\sigma_\omega^2$.
$\nu_i = \sigma_\mathcal{N}^2 \Big/ \big|F(T_i)\big|^2$	Ratio of noise variance and Fourier transformed channel transmittance, where $\big|F(T_i)\big|^2 = \Big|\sum_{k=0}^{n-1} T_k e^{\frac{-\mathrm{i}2\pi ik}{n}}\Big|^2$, $i = 0\dots n-1$.
$\nu_{Eve} = 1\big/\lambda$	Security bound of the optimal Gaussian attack, where λ is the Lagrange coefficient.
$\Omega = \Pr\Big(\sum_l \big|F(T_i)\big|^2 = l \max_{\forall i}\big|F(T_i)\big|^2\Big)$	The probability that the sum of the squared magnitudes of the Fourier transformed coefficients of the l Gaussian sub-channels picks up a maximum value.
$L = \big|F(T_{0\dots n-1})\big|^2$	Ordered list of the squared magnitudes so that $\big|F(T_i)\big|^2 \geq \big|F(T_{i+1})\big|^2$ and $\nu_i \leq \nu_{i+1}$.
$N_{single} = \dfrac{(W-1)\big(|T_{Eve}|^2\big)}{1-|T_{Eve}|^2}$	Excess noise at a single-carrier transmission, where T_{Eve} is Eve's transmittance, W is the variance of the EPR-ancilla.
$N_{AMQD} = \dfrac{(W-1)\big(\frac{1}{n}\sum_n |F(T_{Eve,i})|^2\big)}{1-\frac{1}{n}\sum_n |F(T_{Eve,i})|^2}$	The excess noise in the AMQD modulation scheme.
$\kappa = N_{single}\big/N_{AMQD} \geq 1$	Ratio of single-carrier and AMQD excess noise.
$N_{tol,AMQD} = \alpha N_{tol,single}$	Tolerable excess noise in AMQD modulation, where $\alpha = x\kappa \geq 1$.
$\eta_{single}, \eta_{AMQD}$	Single-carrier CVQKD and AMQD efficiency.
R	Transmission rate of classical information.
S	Secret key rate.

S.2 Abbreviations

AMQD	**Adaptive Multicarrier Quadrature Division**
AWGN	**Additive White Gaussian Noise**
BS	**Beam Splitter**

CV	Continuous-Variable
CVQFT	Continuous-Variable Quantum Fourier Transform
DR	Direct-Reconciliation
DV	Discrete-Variable
FFT	Fast Fourier Transform
FWHM	Full Width at Half Maximum
IFFT	Inverse Fast Fourier Transform
OFDM	Orthogonal Frequency-Division Multiplexing
RR	Reverse Reconciliation
SNR	Signal-to-Noise Ratio