Secret Key Rate Adaption for Multicarrier Continuous-Variable Quantum Key Distribution

Laszlo Gyongyosi^{1,2,3} · Sandor Imre²

Received: 6 June 2019 / Accepted: 24 September 2019 / Published online: 16 October 2019
© The Author(s) 2019

Abstract

A multicarrier continuous-variable quantum key distribution (CVQKD) protocol uses Gaussian subcarrier quantum continuous variables (CVs) for the transmission. Here, we define an iterative error-minimizing secret key adaption method for multicarrier CVQKD. The proposed method allows for the parties to reach a given target secret key rate with minimized error rate through the Gaussian sub-channels by a sub-channel adaption procedure. The adaption algorithm iteratively determines the optimal transmit conditions to achieve the target secret key rate and the minimal error rate over the sub-channels. The solution requires no complex calculations or computational tools, allowing for easy implementation for experimental scenarios.

Keywords Quantum key distribution · Quantum cryptography · Quantum continuous variables · CVQKD

Abbreviations

AMQD	Adaptive multicarrier quadrature division
AWGN	Additive white Gaussian noise
BER	Bit error rate
CV	Continuous variable
CVQFT	Continuous-variable quantum Fourier transform
CVQKD	Continuous-variable quantum key distribution
DV	Discrete variable
FFT	Fast Fourier transform
ICVQFT	Inverse CVQFT
IFFT	Inverse fast Fourier transform
MQA	Multiuser quadrature allocation
QFT	Quantum Fourier transform
QKD	Quantum key distribution
SNR	Signal-to-noise ratio

Introduction

Continuous-variable quantum key distribution (CVQKD) represents an important practical manifestation of the fundamentals of quantum mechanics [1, 2, 4–6, 11–17, 19–21, 37, 49, 50, 58, 59]. CVQKD does not require single-photon sources and detectors and can be implemented in an experimental scenario by standard devices [29–31, 39, 43–46, 48, 57, 60]. In a CVQKD setting, the information is carried by a continuous-variable quantum state that is defined in the phase space via the position and momentum quadratures. In an experimental CVQKD scenario, the CV quantum states have a Gaussian random distribution, and the quantum channel between the sender (Alice) and receiver (Bob) is also Gaussian, because the presence of an eavesdropper (Eve) adds a white Gaussian noise into the transmission [3, 7–10, 25, 26, 35, 40–42, 51, 54, 61–63].

The relevant performance attributes of experimental CVQKD (i.e., secret key rates, transmission distances, tolerable excess noise, etc.) still require significant improvements [6, 11–14, 17, 49, 58, 59]. The multicarrier CVQKD has been recently introduced through the adaptive quadrature division modulation (AMQD) [15]. The multicarrier CVQKD scheme injects several additional degrees of freedom into the transmission, which are not available for a standard (single carrier) CVQKD setting [15, 17, 18, 20–24, 27–31, 64, 65]. These results also made possible to utilize several significant phenomena for CVQKD that are unavailable in a standard CVQKD protocol [16–18, 21–23, 28, 29]. The secret key rates of multicarrier CVQKD confirm the

Parts of this work were presented in [15].

✉ Laszlo Gyongyosi
lasgy_ph@yahoo.com

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

² Department of Networked Systems and Services, Budapest University of Technology and Economics, Budapest 1117, Hungary

³ MTA-BME Information Systems Research Group, Hungarian Academy of Sciences, Budapest 1051, Hungary

multimode bounds of [7] (see the results on fundamental rate-loss scaling in quantum optical communications in [7]). Further information on the bounds of private quantum communications can be found in [8].

Here, a secret key adaption method is defined for multi-carrier CVQKD. The proposed secret key adaption successively utilizes private rate curves for the sub-channels. The curves also define an adaption region for each sub-channel. Particularly, the adaption region provides a base for the iterative, private rate increment method utilized by our secret key rate adaption algorithm. The iterative sub-channel selection procedure depends on the actual target private rate and the noise levels of the sub-channels. We demonstrate the results through the framework of AMQD and also extend the results to the multiple-access multicarrier CVQKD.

The novel contributions of our manuscript are as follows:

1. We define an iterative error-minimizing secret key adaption method for multicarrier CVQKD. The proposed secret key adaption algorithm iteratively determines the optimal transmit conditions at a given target secret key rate to realize minimal error transmission over the sub-channels.
2. The proposed method allows for the parties to reach a given target secret key rate with minimized error rate through the Gaussian sub-channels by a sub-channel adaption procedure.
3. At a given transmission rate of private classical information (private rate), the method determines and selects that sub-channel from the set of available sub-channels for the transmission of the quadratures which sub-channel provides a minimal error rate.
4. The scheme provably yields a minimized error rate transmission for all sub-channels while achieving the selected target secret key rate.
5. The solution requires no complex calculations or computational tools, allowing for easy implementation for experimental CVQKD scenarios.

This paper is organized as follows. In “Preliminaries”, preliminary findings are summarized. Section “Secret Key Rate Adaption with Minimized Error Rate” discusses the iterative secret key adaption scheme. Section “Secret Key Rate Adaption in Multiuser Multicarrier CVQKD” extends the results to a multiuser setting. In “Numerical Evidence”, a numerical evidence is proposed. Finally, Section “Conclusions” concludes the results. Supplemental material is included in the Appendix.

Preliminaries

The notations and basic terms of multicarrier CVQKD can be found in [15]. A brief summary is also included in Appendix 1.

Multiuser quadrature allocation (MQA)

In an MQA multiple access multicarrier CVQKD [20], a given user $U_k, k = 0, \dots, K - 1$, where K is the number of total users, is characterized via m subcarriers, formulating an $\mathcal{M}_{U_k}$ logical channel of U_k ,

$$\mathcal{M}_{U_k} = [\mathcal{N}_{U_k,0}, \dots, \mathcal{N}_{U_k,m-1}]^T, \quad (1)$$

where $\mathcal{N}_{U_k,i}$ is the i th sub-channel of $\mathcal{M}_{U_k}$. For a detailed description of MQA for multicarrier CVQKD, see [20].

Private Classical Rate Curves

The secret key adaption method utilizes $r + 2$ rate curves for the sub-channels, defined via set

$$\mathcal{S} = \{R_{\min}(\mathcal{N}_i), R(q), R_{\max}(\mathcal{N}_i)\}, q = 0 \dots r - 1. \quad (2)$$

Specifically, for all sub-channels $\mathcal{N}_i, i = 0, \dots, l - 1$ a given rate curve is selected from $\mathcal{S}$ (2) according to the sub-channel conditions.

In particular, a $R(q)$ rate curve refers to the transmission rate of private classical information (private rate) over $\mathcal{N}_i$, with the relation

$$R_{\min}(\mathcal{N}_i) < R(0) \dots < R(r - 1) < R_{\max}(\mathcal{N}_i), \quad (3)$$

where $R(q)$ is referred to as the target private rate at an $R(q - 1)$ actual private rate in an iteration procedure.

Assuming a reverse reconciliation [6], a given target private rate $R(q)$ is defined as

$$R(q) \leq P(\mathcal{N}_i) = \lim_{n \rightarrow \infty} \frac{1}{n} \max_{\rho_i} (\chi_{AB}(\mathcal{N}_i) - \chi_{BE}(\mathcal{N}_i)), \quad (4)$$

where $P(\mathcal{N}_i)$ is the private classical capacity of $\mathcal{N}_i$ [2, 34], and $\chi_{AB}(\mathcal{N}_i)$ and $\chi_{BE}(\mathcal{N}_i)$ are the Holevo information of Alice (transmitter) and Bob (receiver), and Bob and Eve (eavesdropper), respectively.

Secret Key Rate Adaption with Minimized Error Rate

Theorem 1 A given target secret key rate $S^*(\mathcal{N}) = \sum_{i=0}^{l-1} R_i(\mathcal{N}_i)$, where $R_i(\mathcal{N}_i)$ is the private rate of sub-channel $\mathcal{N}_i$, can be achieved over the l sub-channels such that the error rate of all sub-channels is minimized.

Proof The proof focuses on a single sub-channel $\mathcal{N}_i$ for the private transmission of a single quadrature component x_i (or p_i), which refers to a $x_i \in \mathcal{N}(0, \sigma_\omega^2)$ position or a $p_i \in \mathcal{N}(0, \sigma_\omega^2)$ momentum quadrature of the i th subcarrier, respectively.

Let

$$v_i(\mathcal{N}_i) = \frac{\sigma_{\mathcal{N}_i}^2}{|F(T_i(\mathcal{N}_i))|^2}, \quad (5)$$

of the i th, $i = 0, \dots, l-1$ sub-channel $\mathcal{N}_i$.

Let $R_{\min}(\mathcal{N}_i)$ and $R_{\max}(\mathcal{N}_i)$ be the minimal and maximal private classical information transmission rates selected for $\mathcal{N}_i$. The private rates are referring to the transmission of a given quadrature x_i .

These rate curves, $R(q) > R(q-1)$, allow us to reach a target secret key rate $S^*(\mathcal{N})$ over the sub-channels with a minimized error rate in a multicarrier CVQKD setting. Specifically, it requires a rigorously defined iterative condition on the selection of the sub-channels for each target rate $R(q)$.

From $R_{\min}(\mathcal{N}_i)$ and $R_{\max}(\mathcal{N}_i)$, an adaption region A can be characterized with r rate curves inside the region. Define r rate curves for the transmission of x_i in the region of A

$$A = [R_{\min}(\mathcal{N}_i), R_{\max}(\mathcal{N}_i)], \quad (6)$$

as

$$R(q), q = 0 \dots r-1, \quad (7)$$

such that (3) holds.

Precisely, at a given private rate $R(\mathcal{N}_i)$, (5) is referred to as $v_i(R(\mathcal{N}_i))$,

$$v_i(R(\mathcal{N}_i)) = \frac{\sigma_{R(\mathcal{N}_i)}^2}{|F(T(R(\mathcal{N}_i))))|^2}, \quad (8)$$

where $\sigma_{R(\mathcal{N}_i)}^2$ is the noise variance of $\mathcal{N}_i$ at $R(\mathcal{N}_i)$, while $F(T(R(\mathcal{N}_i))))$ is the transmittance coefficient of $\mathcal{N}_i$ at $R(\mathcal{N}_i)$. Note that in function of (8), after a scaling the rate curves of (7) are almost parallel to $R_{\min}(\mathcal{N}_i)$. By theory, at $R(\mathcal{N}_i) = 0$ (8) is directly defined from $\sigma_{\mathcal{N}_i}^2$ is the noise variance and $T_i(\mathcal{N}_i)$ is the transmittance coefficient of $\mathcal{N}_i$, as given in (5).

In function of $v_i(R(\mathcal{N}_i))$, the SNR of $\mathcal{N}_i$ at a given $R(\mathcal{N}_i)$ is expressed as [55]

$$\text{SNR}(R(\mathcal{N}_i)) = 10 \log_{10} \frac{1}{v_i(R(\mathcal{N}_i))}. \quad (9)$$

To step forward, we have to focus on the behavior of parameter $v_i(\cdot)$ at an increased transmission rate.

Particularly, let $\underline{R}(\mathcal{N}_i)$ be the current private rate and $\tilde{R}(\mathcal{N}_i)$ be the target private rate for a sub-channel $\mathcal{N}_i$, such that $\underline{R}(\mathcal{N}_i) < R(\mathcal{N}_i) < \tilde{R}(\mathcal{N}_i)$. Then, let $\delta_{v_i}(R(\mathcal{N}_i))$ identify the cumulative $v_i(R(\mathcal{N}_i))$ parameter of $\mathcal{N}_i$ at an increased

(target) private rate $R(\mathcal{N}_i)$, evaluated via the following iteration:

$$\delta_{v_i}(R(\mathcal{N}_i)) = \delta_{v_i}(\underline{R}(\mathcal{N}_i)) + \Delta_{v_i}(R(\mathcal{N}_i), \tilde{R}(\mathcal{N}_i)), \quad (10)$$

where Δ_{v_i} identifies the difference of v_i at $R(\mathcal{N}_i)$ and $\tilde{R}(\mathcal{N}_i)$ as

$$\Delta_{v_i} = v_i(R(\mathcal{N}_i)) - v_i(\tilde{R}(\mathcal{N}_i)), \quad (11)$$

the iteration (10) at no transmission, $R(\mathcal{N}_i) = 0$, identifies $v_i(\mathcal{N}_i)$ as

$$\delta_{v_i}(R(\mathcal{N}_i) = 0) = v_i(\mathcal{N}_i), \quad (12)$$

while for any $R(\mathcal{N}_i) > \underline{R}(\mathcal{N}_i) > 0$,

$$v_i(R(\mathcal{N}_i)) < v_i(\underline{R}(\mathcal{N}_i)). \quad (13)$$

To conclude, from (10) follows that a rate increment from $\underline{R}(\mathcal{N}_i)$ to $R(\mathcal{N}_i)$ also increases $\delta_{v_i}(\underline{R}(\mathcal{N}_i))$ by $\Delta_{v_i}(R(\mathcal{N}_i), \tilde{R}(\mathcal{N}_i))$, thus for any $R(\mathcal{N}_i) > \underline{R}(\mathcal{N}_i)$, the following relation holds [55]:

$$\delta_{v_i}(R(\mathcal{N}_i)) > \delta_{v_i}(\underline{R}(\mathcal{N}_i)). \quad (14)$$

Let us then define r private transmission curves in the adaption region A of $\mathcal{N}_i$. The aim of the iterative secret key adaption scheme is to provide a rate increment in each step by selecting that sub-channel $\mathcal{N}_i$, for which (10) is minimal. Specifically, it is a convenient approach because this sub-channel provides the best condition for the transmission.

As we show, using this sub-channel, the increased rate $\tilde{R}$ can be achieved with a minimized error rate, but at the same time, it keeps the target secret key rate. Therefore, applying the sub-channel selection procedure with respect to the iterative condition of (10), a desired target secret key rate can be achieved such that the transmission is adapted to not just the sub-channel conditions, but also to yield a minimized error rate for all sub-channels.

Applying (10) for a $R_{\min}(\mathcal{N}_i)$ private rate is as follows. An $R_{\min}(\mathcal{N}_i)$ target private rate over $\mathcal{N}_i$, $\delta_{v_i}(R_{\min}(\mathcal{N}_i))$ is yielded via $v_i(\mathcal{N}_i)$ and $\Delta_{v_i}(R_{\min}(\mathcal{N}_i), R(0))$ derived from $R(0) \in A$ as

$$\delta_{v_i}(R_{\min}(\mathcal{N}_i)) = v_i(\mathcal{N}_i) + \Delta_{v_i}(R_{\min}(\mathcal{N}_i), R(0)). \quad (15)$$

Applying (10) to the r rate curves $R(q) \in A$, $q = 0 \dots r-2$ at a target rate $R(q)$ results in $\delta_{v_i}(R(q))$ as

$$\delta_{v_i}(R(q)) = \delta_{v_i}(R(q-1)) + \Delta_{v_i}(R(q), R(q+1)), \quad (16)$$

Specifically, in each step for a given target $R(q)$, the method selects that $\mathcal{N}_i$, for which (36) is minimal, because that sub-channel provides the best conditions. Thus, the secret key adaption is an iterative process and depends on the $\delta_{v_i}(R(q-1))$ parameter obtained at $R(q-1)$ and on $\Delta_{v_i}(R(q), R(q+1))$.

In particular, for $q = 0$, (16) yields

$$\begin{aligned} \delta_{v_i}(R(0)) &= \delta_{v_i}(R_{\min}(\mathcal{N}_i)) + \Delta_{v_i}(R(0), R(1)) \\ &= v_i(\mathcal{N}_i) + \Delta_{v_i}(R_{\min}(\mathcal{N}_i), R(0)) \\ &\quad + \Delta_{v_i}(R(0), R(1)), \end{aligned} \quad (17)$$

where $R(1) \in \mathcal{A}$. While, for $q = r-1$, (10) results in

$$\begin{aligned} \delta_{v_i}(R(r-1)) &= \delta_{v_i}(R(r-2)) + \Delta_{v_i}(R(r-1), R_{\max}(\mathcal{N}_i)) \\ &= \left(v_i(\mathcal{N}_i) + \Delta_{v_i}(R_{\min}(\mathcal{N}_i), R(0)) \right. \\ &\quad \left. + \sum_{k=0}^{r-2} \Delta_{v_i}(R(k), R(k+1)) \right) \\ &\quad + \Delta_{v_i}(R(r-1), R_{\max}(\mathcal{N}_i)), \end{aligned} \quad (18)$$

where $R(k) \in \mathcal{A}$, $k = 0 \dots r-2$. For $R_{\max}(\mathcal{N}_i)$, by definition $\delta_{v_i}(R_{\max}(\mathcal{N}_i)) = +\infty$ [55].

The distribution of a sample set $\delta_{v_i}(R(q))$ for m sub-channels, $i = 0, \dots, m-1$, in a low-SNR CVQKD

scenario is illustrated in Fig. 1a. The SNR in Fig. 1b is derived from the $\delta_{v_i}(R(q))$ set of the m sub-channels as $\text{SNR}(v_i(R(q))) = 10 \log_{10}(1/(v_i(R(q))))$.

Next, we show that for an arbitrary target private rate $R(\mathcal{N}_i) > 0$, the iterative condition on $\delta_{v_i}(R(\mathcal{N}_i))$ (see (16)) provides a minimized error rate over the selected $\mathcal{N}_i$.

Let $\mathcal{B}$ be the bit error rate (BER), and let $\mathcal{B}(R(q)_{\delta_{v_i}(R(q-1))})$ refer to the bit error rate of $\mathcal{N}_i$ at target private rate $R(q)$, at an actual rate $R(q-1)$, and $\delta_{v_i}(R(q-1))$. Then, at a given $R(q)$, selecting that $\mathcal{N}_i$, $i = 0, \dots, l-1$ from the total l , for which $\delta_{v_i}(R(q-1))$ is minimal, as

$$\xi(R(q-1)) = \min_{v_i} \delta_{v_i}(R(q-1)) \quad (19)$$

yields a minimized bit error rate at a given $R(q)$ over the selected $\mathcal{N}_i$ as

$$\mathcal{B}(R(q)_{\xi(R(q-1))}) = \mathcal{B}(R_{\min}(\mathcal{N}_i)_{\delta_{v_i}(R(q-1))}), \quad (20)$$

where $\mathcal{B}(R_{\min}(\mathcal{N}_i)_{\delta_{v_i}(R(q-1))})$ is defined as

$$\begin{aligned} \mathcal{B} \left(R_{\min}(\mathcal{N}_i)_{v_i(\mathcal{N}_i) + \left(\Delta_{v_i}(R_{\min}(\mathcal{N}_i), R(0)) + \sum_{k=0}^{q-1} \Delta_{v_i}(R(k), R(k+1)) \right)} \right) \\ = \frac{1}{2} \text{erfc} \mathcal{F} \left(v_i(\mathcal{N}_i) + \left(\Delta_{v_i}(R_{\min}(\mathcal{N}_i), R(0)) + \dots \right. \right. \\ \left. \left. + \Delta_{v_i}(R(q-1), R(q)) \right) \right), \end{aligned} \quad (21)$$

where function $\mathcal{F}(\cdot)$ is evaluated as

Fig. 1 **a** The distribution of a low-SNR set $\delta_{v_i}(R(q))$, $i = 0, \dots, m-1$, for $m = 1000$ sub-channels. **b** The SNR is derived from $\delta_{v_i}(R(q))$ for all sub-channels

$$\mathcal{F}(v_i(\mathcal{N}_i) + (\Delta_{v_i}(R_{\min}(\mathcal{N}_i), R(0)) + \dots + \Delta_{v_i}(R(q-1), R(q)))) \\ = \left[\sqrt{\text{SNR}(v_i(\mathcal{N}_i)) - [\text{SNR}(v_i(R(0))) - \text{SNR}(v_i(R_{\min}(\mathcal{N}_i)))]} \right. \\ \left. - \left(\sum_{k=0}^{q-1} [\text{SNR}(v_i(R(k+1))) - \text{SNR}(v_i(R(k)))] \right) \right] \quad (22)$$

where $\text{SNR}(v_i(R(x))) = 10 \log_{10} (1/(v_i(R(x))))$, while $\text{erfc}(\cdot)$ is the complementary error function

$$\text{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-t^2} dt. \quad (23)$$

The aim of the error minimization procedure is to achieve (20) for all $R(\cdot)$ via the selection of that $\mathcal{N}_i$ for which $\delta_{v_i}(R(q-1))$ is minimal.

Let $R(k+1)_{\delta_{v_i}(R(k))}$ refer to a private rate $R(k+1)$ over at $\delta_{v_i}(R(k))$ with respect to the transmission of a single quadrature component x_i (or p_i).

First, we apply (19) to the minimal rate $R_{\min}(\mathcal{N}_i)$ by the selection of that $\mathcal{N}_i$, for which $v_i(\mathcal{N}_i)$ is minimal, thus

$$\xi(0) = \min_{v_i} \delta_{v_i}(0) = \min_{v_i} v_i, \quad (24)$$

which yields

$$\mathcal{B}(R_{\min}(\mathcal{N}_i)_{\xi(0)}) = \mathcal{B}(R_{\min}(\mathcal{N}_i)_{v_i(\mathcal{N}_i)}). \quad (25)$$

Similarly, at $R(0)$, that sub-channel is selected for the $R(0)$ rate transmission, for which $\delta_{v_i}(R_{\min}(\mathcal{N}_i))$ is minimal.

In particular, due to the iterative determination of $\delta_{v_i}(R_{\min}(\mathcal{N}_i))$, the corresponding $\mathcal{B}(R(0)_{\xi(R_{\min}(\mathcal{N}_i))})$ is yielded as

$$\mathcal{B}(R(0)_{\xi(R_{\min}(\mathcal{N}_i))}) = \mathcal{B}(R_{\min}(\mathcal{N}_i)_{v_i(\mathcal{N}_i) + \Delta_{v_i}(R_{\min}(\mathcal{N}_i), R(0))}). \quad (26)$$

Precisely, for $R(q)$, $q = 1 \dots r-1$, therefore, in each step, that sub-channel selected for the transmission, for which $\xi(R(q-1))$ is minimal, ensures that the resulting $\mathcal{B}(R(q)_{\xi(R(q-1))})$ is evaluated as

$$\mathcal{B}(R(q)_{\xi(R(q-1))}) \\ = \mathcal{B}(R_{\min}(\mathcal{N}_i)_{\delta_{v_i}(R(q-2)) + \Delta_{v_i}(R(q-1), R(q))}). \quad (27)$$

Putting the pieces together, the utilization of (27) for $q = 1$ is as

$$\mathcal{B}(R(1)_{\xi(R(0))}) \\ = \mathcal{B}(R_{\min}(\mathcal{N}_i)_{\delta_{v_i}(R_{\min}(\mathcal{N}_i)) + \Delta_{v_i}(R(0), R(1))}), \quad (28)$$

while for $q = r-1$,

$$\mathcal{B}(R(r-1)_{\xi(R(r-2))}) \\ = \mathcal{B}(R_{\min}(\mathcal{N}_i)_{\delta_{v_i}(R(r-3)) + \Delta_{v_i}(R(r-2), R(r-1))}), \quad (29)$$

and, finally, for $R_{\max}(\mathcal{N}_i)_{\xi(R(r-1))}$, the corresponding error rate is

$$\mathcal{B}(R_{\max}(\mathcal{N}_i)_{\xi(R(r-1))}) \\ = \mathcal{B}(R_{\min}(\mathcal{N}_i)_{\delta_{v_i}(R(r-2)) + \Delta_{v_i}(R(r-1), R_{\max}(\mathcal{N}_i))}). \quad (30)$$

Fig. 2 The $\mathcal{B}$ bit error rates at $R_{\min}(\mathcal{N}_i)$, $R(0)$, $\dots$, $R(r-1)$, $R_{\max}(\mathcal{N}_i)$ in a low-SNR scenario for a given sub-channel $\mathcal{N}_i$ at **a** $v_i = [0.1, 0.3]$ and **b** $v_i = [0.3, 0.9]$

The $\mathcal{B}$ bit error rates at private rates, $R_{\min}(\mathcal{N}_i), R(0), \dots, R_{\min}(r-1), R_{\max}(\mathcal{N}_i)$, for a given sub-channel $\mathcal{N}_i$ in function of ν_i (low-SNR scenario) are summarized in Fig. 2 for the range $\nu_i = [0.1, 0.3]$ (Fig. 2a), and $\nu_i = [0.3, 0.9]$ (Fig. 2b).

The iterative secret key adapting method with the error minimization is detailed in Algorithm 1.

The proof is concluded here. $\square$

Algorithm 1 Iterative secret key rate adaption for multicarrier CVQKD.

Step 1. Let $R_{\min}(\mathcal{N}_i), R_{\max}(\mathcal{N}_i)$ be the minimal and maximal private transmission rates selected for all sub-channels $\mathcal{N}_i, i = 0, \dots, l-1$.

Step 2. For a given $\mathcal{N}_i$, let $\nu_i(\mathcal{N}_i) = \sigma_{\mathcal{N}_i}^2 / |F(T(\mathcal{N}_i))|^2$ at noise variance $\sigma_{\mathcal{N}_i}^2$ and transmission coefficient $F(T_i(\mathcal{N}_i))$. Define r curves $R(q), q = 0 \dots r-1$ in the adaption region $A = [R_{\min}(\mathcal{N}_i), R_{\max}(\mathcal{N}_i)]$, with relation $R_{\min}(\mathcal{N}_i) < R(0) \dots < R(r-1) < R_{\max}(\mathcal{N}_i)$.

Step 3. For target private rate $R_{\min}(\mathcal{N}_i)$, determine $\delta_{\nu_i}(R_{\min}(\mathcal{N}_i))$ as $\delta_{\nu_i}(R_{\min}(\mathcal{N}_i)) = \nu_i(\mathcal{N}_i) + \Delta_{\nu_i}(R_{\min}(\mathcal{N}_i), R(0))$. For the $R(q), q = 0 \dots r-2$ curves of the adaption region A , compute $\delta_{\nu_i}(R(q))$ as $\delta_{\nu_i}(R(q)) = \delta_{\nu_i}(R(q-1)) + \Delta_{\nu_i}(R(q), R(q+1))$. At $q = r-1$, use $\delta_{\nu_i}(R(r-1)) = \delta_{\nu_i}(R(r-2)) + \Delta_{\nu_i}(R(r-1), R_{\max}(\mathcal{N}_i))$. At $R_{\max}(\mathcal{N}_i)$, use $\delta_{\nu_i}(R_{\max}(\mathcal{N}_i)) = +\infty$.

Step 4. Utilize the adaption method: at a target rate $R(q), q = 0 \dots r-1$, select that sub-channel $\mathcal{N}_i$ for which $\delta_{\nu_i}(R(q-1))$ is minimal. At $R_{\min}(\mathcal{N}_i)$, select that $\mathcal{N}_i$ for which $\nu_i(\mathcal{N}_i)$ is minimal. At $R(0)$ select $\mathcal{N}_i$ for which $\delta_{\nu_i}(R_{\min}(\mathcal{N}_i))$ is minimal, while at $R_{\max}(\mathcal{N}_i)$, select $\mathcal{N}_i$ for which $\delta_{\nu_i}(R(r-1))$ is minimal.

Step 5. Repeat the steps until $S^*(\mathcal{N}) \leq \sum_{i=0}^{l-1} R_i(\mathcal{N}_i)$, where $S^*(\mathcal{N})$ is the desired secret key rate over the l sub-channels, and $R_i(\mathcal{N}_i)$ is the private transmission rate of $\mathcal{N}_i$ at a minimized $\mathcal{B}$ for all $\mathcal{N}_i$.

Fig. 3 The $\mathcal{B}$ bit error rate of secret key adapting for a sub-channel $\mathcal{N}_i$ in function of $\nu_i(R_i(x)) = 10^{-\text{SNR}(\nu_i(R_i(x)))/10}$. The adaption is made via r rate curves $R(q), q = 0 \dots r-1, R_{\min}(\mathcal{N}_i) < R(0) \dots < R(r-1) < R_{\max}(\mathcal{N}_i)$ in the $A = [R_{\min}(\mathcal{N}_i), R_{\max}(\mathcal{N}_i)]$ adaption region (shaded area)

The resulting $\mathcal{B}$ bit error rates of the secret key rate adapting method for a given sub-channel $\mathcal{N}_i$ in function of ν_i are summarized in Fig. 3. Parameter ν_i is scaled for the SNR with 5 dB steps in the range of $[15, -5]$ as $\nu_i(R_i(x)) = 10^{-\text{SNR}(\nu_i(R_i(x)))/10}$.

Secret Key Rate Adaption in Multiuser Multicarrier CVQKD

This section extends the results for a multiuser multicarrier CVQKD [20] scenario.

Lemma 1 *The secret key adaption can be extended to a $U_k, k = 0, \dots, K-1$ multiuser setting, where K is the number of users, to achieve target secret key rate $S^*(\mathcal{M}_{U_k})$ with minimized error rate over the m sub-channels of $\mathcal{M}_{U_k}$ of U_k , for $\forall k$.*

Proof The proof focuses on a given logical channel $\mathcal{M}_{U_k} = [\mathcal{N}_{U_k,0}, \dots, \mathcal{N}_{U_k,m-1}]^T$ of a user U_k , where $\mathcal{N}_{U_k,i}$, $i = 0, \dots, m-1$ is the i th sub-channel.

Let K be the number of transmit users and select a given $U_k, k = 0, \dots, K-1$. Let $S^*(\mathcal{M}_{U_k})$ be the target secret key rate of users over $\mathcal{M}_{U_k}$, and let $R(\mathcal{N}_{U_k,i})$ be the private rate of $\mathcal{N}_{U_k,i}$. The steps of the extension are summarized as follows.

Let

$$v_i(\mathcal{N}_{U_k,i}) = \frac{\sigma_{\mathcal{N}_{U_k,i}}^2}{|F(T(\mathcal{N}_{U_k,i}))|^2}, \quad (31)$$

where $\sigma_{\mathcal{N}_{U_k,i}}^2$ is the noise variance of $\mathcal{N}_{U_k,i}$, while $T_i(\mathcal{N}_{U_k,i})$ is the transmittance coefficient of $\mathcal{N}_{U_k,i}$. At a given rate curve $R(\mathcal{N}_{U_k,i}) > 0$,

$$v_i(R(\mathcal{N}_{U_k,i})) = \frac{\sigma_{R(\mathcal{N}_{U_k,i})}^2}{|F(T(R(\mathcal{N}_{U_k,i})))|^2}, \quad (32)$$

where $\sigma_{R(\mathcal{N}_{U_k,i})}^2$ is the noise variance at $R(\mathcal{N}_{U_k,i})$, while $T_i(R(\mathcal{N}_{U_k,i}))$ is the transmittance coefficient of $\mathcal{N}_{U_k,i}$ at $R(\mathcal{N}_{U_k,i})$, respectively. Apply the secret key rate adaption method over the set $\mathcal{M}_{U_k}$ of m $\mathcal{N}_{U_k,i}$, sub-channels of $\mathcal{M}_{U_k}$, until

$$S^*(\mathcal{M}_{U_k}) \leq \sum_{i=0}^{m-1} R(\mathcal{N}_{U_k,i}). \quad (33)$$

Apply the steps for all transmit users U_k for their $\mathcal{M}_{U_k}$ sets of m sub-channels. Therefore, one can utilize (27) at a given $R(\mathcal{N}_{U_k,i}) = R_i(q)$, where $R_i(q)$ refers to the $R(q)$ curve of $\mathcal{N}_{U_k,i}$, and from (12) follows $\delta_{v_i}(R(\mathcal{N}_{U_k,i}) = 0) = v_i(\mathcal{N}_{U_k,i})$, which yields the error rate for $\mathcal{N}_{U_k,i}$ of $\mathcal{M}_{U_k}$ as

$$\begin{aligned} & \mathcal{B}(R(\mathcal{N}_{U_k,i})_{\xi(R(q-1))}) \\ &= \mathcal{B}\left(R_{\min}(\mathcal{N}_{U_k,i})_{v_i(\mathcal{N}_{U_k,i})} + (\Delta_{v_i}(R_{\min}(\mathcal{N}_{U_k,i}), R_i(0)) + \sum_{k=0}^{q-1} \Delta_{v_i}(R_i(k), R_i(k+1)))\right). \end{aligned} \quad (34)$$

□

Variance Adaption for an Equalized Error Rate

In this section, we propose a modulation variance adaption method to achieve an equally minimized error rate for the sub-channels of a given user. The results can be extended to an arbitrary number of users.

Theorem 2 For all $U_k, k = 0, \dots, K-1$, the error rate of the $\mathcal{N}_{U_k,i}, i = 0, \dots, m-1$ sub-channels of $\mathcal{M}_{U_k}$ of user U_k can be equally minimized via a $\tilde{\sigma}_{\omega}^2 = \sigma_{\omega}^2 + \Delta_{\sigma_{\omega_i}^2}$ modulation variance correction, where $\Delta_{\sigma_{\omega_i}^2} > 0$.

Proof Let

$$R(\mathcal{N}_{U_k,i}) = R_i(q-1), q = 0, \dots, r-1, \quad (35)$$

and $R(\mathcal{N}_{U_k,i})$ be the target private rate,

$$R(\mathcal{N}_{U_k,i}) = R_i(q), \quad (36)$$

where $R_i(q)$ refers to the $R(q)$ curve of $\mathcal{N}_{U_k,i}$, with relation to $R_i(q-1) < R_i(q)$, and let us identify $R_i(-1) = R_{\min}(\mathcal{N}_{U_k,i})$ and $R_i(r) = R_{\max}(\mathcal{N}_{U_k,i})$.

Precisely, for a given U_k at $R(\mathcal{N}_{U_k,i})$, the minimal $\delta_{v_i}(R(\mathcal{N}_{U_k,i}))$ parameter for the $\mathcal{N}_{U_k,i}, i = 0, \dots, m-1$ sub-channels of the set $\mathcal{M}_{U_k}$ is evaluated as

$$\xi_{U_k} = \min_{\forall i \in \mathcal{M}_{U_k}} \delta_{v_i}(R(\mathcal{N}_{U_k,i})). \quad (37)$$

Let σ_{ω}^2 refer to the input modulation variance of the i th sub-carrier of U_k . Specifically, using the expression of ξ_{U_k} in (37), the σ_{ω}^2 modulation variance of the i th subcarrier is corrected by $\Delta_{\sigma_{\omega_i}^2}$ as

$$\Delta_{\sigma_{\omega_i}^2} = \delta_{v_i}(R(\mathcal{N}_{U_k,i})) - \xi_{U_k}, \quad (38)$$

yielding a modulation variance increment

$$\tilde{\sigma}_{\omega}^2 = \sigma_{\omega}^2 + \Delta_{\sigma_{\omega_i}^2} \quad (39)$$

for the input of $\mathcal{N}_{U_k,i}$.

In particular, using (39), the $\varphi_{\delta_{v_i}}(R(\mathcal{N}_{U_k,i}))$ resulting δ_{v_i} parameter for $\mathcal{N}_{U_k,i}$ at a target rate $R(\mathcal{N}_{U_k,i})$ is, therefore,

$$\varphi_{\delta_{v_i}}(R(\mathcal{N}_{U_k,i})) = \delta_{v_i}(R(\mathcal{N}_{U_k,i})) - \xi_{U_k}, \quad (40)$$

from which the $\Delta_{\text{SNR}}(\varphi_{\delta_{v_i}}(R(\mathcal{N}_{U_k,i})))$ SNR increment of $\mathcal{N}_{U_k,i}$ at a given $R(\mathcal{N}_{U_k,i}) = R(q)$ is as

$$\begin{aligned} & \Delta_{\text{SNR}}(\varphi_{\delta_{v_i}}(R(\mathcal{N}_{U_k,i}))) \\ &= 10 \log_{10} \frac{1}{\xi_{U_k}} - \mathcal{F}(v_i(\mathcal{N}_{U_k,i}) + (\Delta_{v_i}(R_{\min}(\mathcal{N}_{U_k,i}), R(0)) \\ & \quad + \dots + \Delta_{v_i}(R(q), R(q+1))))), \end{aligned} \quad (41)$$

where $\mathcal{F}(\cdot)$ is specified in (22).

Therefore, the $\mathcal{B}(R(\mathcal{N}_{U_k,i})_{\xi_{U_k}})$ error rate for all $\mathcal{N}_{U_k,i}$ at an arbitrary $R(\mathcal{N}_{U_k,i})_{\delta_{v_i}(\underline{R}(\mathcal{N}_{U_k,i}))}$ is equally minimized by ξ_{U_k} via (21) as

$$\begin{aligned} \mathcal{B}(R(\mathcal{N}_{U_k,i})_{\xi_{U_k}}) &= \min_{\forall i \in \mathcal{M}_{U_k}} \mathcal{B}(R(\mathcal{N}_{U_k,i})_{\delta_{v_i}(\underline{R}(\mathcal{N}_{U_k,i}))}) \\ &= \mathcal{B}(R_{\min}(\mathcal{N}_{U_k,i})_{\delta_{v_i}(\underline{R}(\mathcal{N}_{U_k,i}))}), i = 0, \dots, m-1. \end{aligned} \quad (42)$$

The formula of (42) proves the minimal error rate at arbitrary $S^*(\mathcal{M}_{U_k})$ over $\mathcal{M}_{U_k}$ for all $\mathcal{N}_{U_k,i}$ sub-channels of U_k .

Without loss of generality, the results can be extended for all K users to achieve minimized equalized error rate over all $\mathcal{M}_{U_k}, k = 0, \dots, K-1$ logical channels.

In a single user setting, e.g., $K = 1$, the method provides an equal, minimized error rate over the l sub-channels.

The proof is concluded here. $\square$

Numerical Evidence

This section proposes numerical evidence to demonstrate the results through a multiuser multicarrier CVQKD environment (AMQD-MQA [20]). The numerical evidence serves demonstration purposes.

Parameters

To demonstrate the results of Section 4.1, let U_k be a given user with m sub-channels. The parameters of the numerical evidence are summarized as follows.

The single-carrier inputs of user U_k ,

$$x_{U_k,j} \in \mathcal{N}(0, \sigma_{\omega_0}^2), \quad (43)$$

have a modulation variance of $\sigma_{\omega_0}^2$ and formulate a d -dimensional input vector $\mathbf{x}_{U_k}$.

The j th single carrier is dedicated to a single-carrier channel $\mathcal{N}_{U_k,j}$. The single-carrier channel transmittance coefficient is depicted by $T(\mathcal{N}_{U_k,j})$, $j = 0, \dots, d-1$, where d is the dimension of the input vector.

The single carriers are granulated into m subcarriers, where the i th subcarrier is

$$x_{U_k,i} \in \mathcal{N}(0, \sigma_{\omega}^2), \quad (44)$$

and has a modulation variance of σ_{ω}^2 .

The m sub-channels,

$$\mathcal{N}_{U_k,i}, i = 0, \dots, m-1, \quad (45)$$

formulate the $\mathcal{M}_{U_k}$ logical channel of user U_k ,

$$\mathcal{M}_{U_k} = [\mathcal{N}_{U_k,0}, \dots, \mathcal{N}_{U_k,m-1}]^T. \quad (46)$$

The $\Delta_{x_i} \in \mathcal{N}(0, \sigma_{\mathcal{N}_{U_k,i}}^2)$ noise of $\mathcal{N}_{U_k,i}$ is added to the subcarriers, where $\sigma_{\mathcal{N}_{U_k,i}}^2$ is the noise variance of $\mathcal{N}_{U_k,i}$.

For a given sub-channel $\mathcal{N}_{U_k,i}$ of U_k , parameters $v_i(\mathcal{N}_{U_k,i})$ and $v_i(R(\mathcal{N}_{U_k,i}))$ are evaluated via (31) and (32), such that the $T(\mathcal{N}_{U_k,i})$ sub-channel transmittance coefficients are estimated in a pre-communication phase via the subcarrier spreading technique [30].

The $\delta_{v_i}(R(\mathcal{N}_{U_k,i}))$ of $\mathcal{N}_{U_k,i}$ parameters are determined from $v_i(\mathcal{N}_{U_k,i})$ for all sub-channels via the iterative method of Theorem 2.

Modulation Variance Adaption

The analysis focuses on a low-SNR CVQKD scenario. An initial low-SNR set of $\delta_{v_i}(R(\mathcal{N}_{U_k,i}))$, $i = 0, \dots, m-1$ of user U_k from a low-SNR scenario is illustrated in Fig. 4a. The minimum of the set is $\xi_{U_k} = \min_{\forall i \in \mathcal{M}_{U_k}} \delta_{v_i}(R(\mathcal{N}_{U_k,i}))$, from which the modulation variance correction for $\mathcal{N}_{U_k,i}$ is $\Delta_{\sigma_{\omega_i}^2} = \delta_{v_i}(R(\mathcal{N}_{U_k,i})) - \xi_{U_k}$. The corresponding $\Delta_{\sigma_{\omega_i}^2}$ (see (38)), $i = 0, \dots, m-1$ values determined from the $\delta_{v_i}(R(\mathcal{N}_{U_k,i}))$ elements are depicted in Fig. 4b.

In a low-SNR setting due to the value range of $\delta_{v_i}(R(\mathcal{N}_{U_k,i}))$, $i = 0, \dots, m-1$, the required $\Delta_{\sigma_{\omega_i}^2}$ variance correction for the subcarriers is, therefore, negligible.

The $x_{U_k,i}$, $i = 0, \dots, m-1$ input quadratures of user U_k with a constant variance σ_{ω}^2 are illustrated in Fig. 5a. Applying the result of $\Delta_{\sigma_{\omega_i}^2}$, the $\tilde{x}_{U_k,i}$, $i = 0, \dots, m-1$ input quadratures of user U_k at the $\tilde{\sigma}_{\omega_i}^2 = \sigma_{\omega}^2 + \Delta_{\sigma_{\omega_i}^2}$ increased variance are depicted in Fig. 5b.

The variance adaption of $x_{U_k,i}$, $i = 0, \dots, m-1$ requires only a moderate $\Delta_{\sigma_{\omega_i}^2}$ for all subcarriers to achieve an equalized, significantly lower error rate through the sub-channels.

SNR Differences

The effects of the $\Delta_{\sigma_{\omega_i}^2}$ variance correction and the resulting $\varphi_{\delta_{v_i}}(R(\mathcal{N}_{U_k,i}))$ can be expressed in terms of the resulting SNR change.

The $\Delta_{\text{SNR}}(\tilde{\sigma}_{\omega_i}^2) = \text{SNR}(\tilde{\sigma}_{\omega_i}^2) - \text{SNR}(\sigma_{\omega}^2)$, $i = 0, \dots, m-1$, SNR difference for the input quadratures $\{x_{U_k,i}, \tilde{x}_{U_k,i}\}$ at σ_{ω}^2 and $\tilde{\sigma}_{\omega_i}^2 = \sigma_{\omega}^2 + \Delta_{\sigma_{\omega_i}^2}$ is depicted in Fig. 6a. The $\Delta_{\text{SNR}}(\varphi_{\delta_{v_i}}(R(\mathcal{N}_{U_k,i})))$ SNR differences (see (41)) achieved

Fig. 4 An initial low-SNR set of $\delta_{v_i}(R(\mathcal{N}_{U_k,i}))$ of user U_k , $i = 0, \dots, m-1$, $m = 1000$. **a** The minimum of set $\delta_{v_i}(R(\mathcal{N}_{U_k,i}))$ (red solid line). **b** The resulting $\Delta_{\sigma_{\omega_i}^2}$ variance correction, $i = 0, \dots, m-1$, $m = 1000$ determined from the $\delta_{v_i}(R(\mathcal{N}_{U_k,i}))$ elements

Fig. 5 **a** The $x_{U_k,i}$, $i = 0, \dots, m-1$, $m = 1000$ input quadratures of user U_k at a constant variance $\sigma_{\omega}^2 = 64$. **b** The $\tilde{x}_{U_k,i}$, $i = 0, \dots, m-1$, $m = 1000$ input quadratures of user U_k at increased variance $\tilde{\sigma}_{\omega_i}^2 = \sigma_{\omega}^2 + \Delta_{\sigma_{\omega_i}^2}$

at a given $\varphi_{\delta_{v_i}}(R(\mathcal{N}_{U_k,i}))$, $i = 0, \dots, m-1$, are illustrated in Fig. 6b.

The $\Delta_{\text{SNR}}(\tilde{\sigma}_{\omega_i}^2)$ input SNR difference results in an improved $\Delta_{\text{SNR}}(\varphi_{\delta_{v_i}}(R(\mathcal{N}_{U_k,i})))$ parameter via $\varphi_{\delta_{v_i}}(R(\mathcal{N}_{U_k,i}))$ for all i .

Error Rate Minimization

The BER values for the initial low-SNR set and for the set of $\varphi_{\delta_{v_i}}(R(\mathcal{N}_{U_k,i}))$ are compared in Fig. 2. The BER of $\mathcal{N}_{U_k,i}$

at the initial low-SNR set of $\delta_{v_i}(R(\mathcal{N}_{U_k,i}))$, $i = 0, \dots, m-1$, is illustrated in Fig. 7a. The BER of the m sub-channels $\mathcal{N}_{U_k,i}$, $i = 0, \dots, m-1$, at $\varphi_{\delta_{v_i}}(R(\mathcal{N}_{U_k,i}))$, is depicted in Fig. 7b.

As follows, as ξ_{U_k} is determined and applied in the iteration procedure, the resulting BER is equally minimized for all $\mathcal{N}_{U_k,i}$ sub-channels of user U_k .

Fig. 6 **a** The $\Delta_{\text{SNR}}(\tilde{\sigma}_{\omega_i}^2)$, $i = 0, \dots, m-1$, $m = 1000$ parameter for $\{x_{U_k,i}, \tilde{x}_{U_k,i}\}$ at σ_{ω}^2 and $\tilde{\sigma}_{\omega_i}^2$. **b** The $\Delta_{\text{SNR}}(\varphi_{\delta_{\nu_i}}(R(\mathcal{N}_{U_k,i})))$ parameter, $i = 0, \dots, m-1$, $m = 1000$

Fig. 7 **a** The BER for the initial low-SNR set $\delta_{\nu_i}(R(\mathcal{N}_{U_k,i}))$, $i = 0, \dots, m-1$, $m = 1000$ (the minimum of the set is depicted by the green solid line). **b** The BER values for $\varphi_{\delta_{\nu_i}}(R(\mathcal{N}_{U_k,i}))$, $i = 0, \dots, m-1$, $m = 1000$

Conclusions

We defined an iterative secret key adaption method for multicarrier CVQKD. The scheme provides a minimized error rate using the utilization of an adaptive private classical information transmission through the sub-channels. The private classical transmission is realized through pre-defined private rate curves, which characterize an adaption region for each sub-channel to find the best conditions for the transmission at a given private classical rate. The method allows

us to reach a given target secret key rate with optimal transmit conditions and minimized error rate for all sub-channels.

Acknowledgements Open access funding provided by Budapest University of Technology and Economics (BME). The research reported in this paper has been supported by the National Research, Development and Innovation Fund (TUDFO/51757/2019-ITM, Thematic Excellence Program). This work was partially supported by the National Research Development and Innovation Office of Hungary (Project No. 2017-1.2.1-NKP-2017-00001), by the Hungarian Scientific Research Fund—OTKA K-112125 and in part by the BME Artificial Intelligence FIKP grant of EMMI (BME FIKP-MI/SC).

Author Contributions LGY designed the protocol and wrote the manuscript. LGY and SI analyzed the results. All authors reviewed the manuscript.

Funding We have no competing financial interests.

Data Availability This work does not have any experimental data.

Compliance with Ethical Standards

Conflict of Interest We have no competing interests.

Ethical Approval This work did not involve any active collection of human data.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

Appendix

Multicarrier CVQKD

First, we summarize the basic notations of AMQD [15]. The following description assumes a single user, and the use of n Gaussian sub-channels $\mathcal{N}_i$ for the transmission of the sub-carriers, from which only l sub-channels will carry valuable information.

In the single-carrier modulation scheme, the j th input single-carrier state $|\varphi_j\rangle = |x_j + ip_j\rangle$ is a Gaussian state in the phase space $\mathcal{S}$, with i.i.d. Gaussian random position and momentum quadratures $x_j \in \mathcal{N}(0, \sigma_{\omega_0}^2)$, $p_j \in \mathcal{N}(0, \sigma_{\omega_0}^2)$, where $\sigma_{\omega_0}^2$ is the modulation variance of the quadratures. (For simplicity, $\sigma_{\omega_0}^2$ is referred to as the single-carrier modulation variance, throughout.) Particularly, this Gaussian single carrier is transmitted through a Gaussian quantum channel $\mathcal{N}$. In the multicarrier scenario, the information is carried by Gaussian subcarrier CVs, $|\phi_i\rangle = |x_i + ip_i\rangle$, $x_i \in \mathcal{N}(0, \sigma_{\omega}^2)$, $p_i \in \mathcal{N}(0, \sigma_{\omega}^2)$, where σ_{ω}^2 is the modulation variance of the subcarrier quadratures, which are transmitted through a noisy Gaussian sub-channel $\mathcal{N}_i$. Each $\mathcal{N}_i$ Gaussian sub-channel is dedicated for the transmission of one Gaussian subcarrier CV from the n subcarrier CVs. (Note: index i refers to the subcarriers, while index j to the single carriers throughout the manuscript.) The single-carrier state $|\varphi_j\rangle$ in the phase space $\mathcal{S}$ can be modeled as a zero-mean, circular symmetric complex Gaussian random variable $z_j \in \mathcal{CN}(0, \sigma_{\omega_{z_j}}^2)$, with variance $\sigma_{\omega_{z_j}}^2 = \mathbb{E}[|z_j|^2]$, and with i.i.d. real and imaginary

zero-mean Gaussian random components $\text{Re}(z_j) \in \mathcal{N}(0, \sigma_{\omega_0}^2)$, $\text{Im}(z_j) \in \mathcal{N}(0, \sigma_{\omega_0}^2)$.

In the multicarrier CVQKD scenario, let n be the number of Alice's input single-carrier Gaussian states. The n input coherent states are modeled by an n -dimensional, zero-mean, circular symmetric complex random Gaussian vector

$$\mathbf{z} = \mathbf{x} + i\mathbf{p} = (z_1, \dots, z_n)^T \in \mathcal{CN}(0, \mathbf{K}_z) \quad (47)$$

where each z_j can be modeled as a zero-mean, circular symmetric complex Gaussian random variable

$$z_j \in \mathcal{CN}\left(0, \sigma_{\omega_{z_j}}^2\right), z_j = x_j + ip_j. \quad (48)$$

Specifically, the real and imaginary variables (i.e., the position and momentum quadratures) formulate n -dimensional real Gaussian random vectors, $\mathbf{x} = (x_1, \dots, x_n)^T$ and $\mathbf{p} = (p_1, \dots, p_n)^T$, with zero-mean Gaussian random variables with densities $f(x_j)$ and $f(p_j)$ as

$$f(x_j) = \frac{1}{\sigma_{\omega_0} \sqrt{2\pi}} e^{-\frac{x_j^2}{2\sigma_{\omega_0}^2}}, f(p_j) = \frac{1}{\sigma_{\omega_0} \sqrt{2\pi}} e^{-\frac{p_j^2}{2\sigma_{\omega_0}^2}}, \quad (49)$$

where $\mathbf{K}_z$ is the $n \times n$ Hermitian covariance matrix of $\mathbf{z}$:

$$\mathbf{K}_z = \mathbb{E}[\mathbf{z}\mathbf{z}^\dagger], \quad (50)$$

while $\mathbf{z}^\dagger$ is the adjoint of $\mathbf{z}$.

For vector $\mathbf{z}$,

$$\mathbb{E}[\mathbf{z}] = \mathbb{E}[e^{i\gamma} \mathbf{z}] = \mathbb{E}[e^{i\gamma} \mathbf{z}] \quad (51)$$

holds, and

$$\mathbb{E}[\mathbf{z}\mathbf{z}^T] = \mathbb{E}[e^{i\gamma} \mathbf{z} (e^{i\gamma} \mathbf{z})^T] = \mathbb{E}[e^{i2\gamma} \mathbf{z}\mathbf{z}^T], \quad (52)$$

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

$$f(\mathbf{z}) = \frac{1}{\pi^n \det \mathbf{K}_z} e^{-\mathbf{z}^\dagger \mathbf{K}_z^{-1} \mathbf{z}}. \quad (53)$$

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 $\mathcal{N}(0, 1)_n$. This vector is characterized by its covariance matrix $\mathbf{K}_x = \mathbb{E}[\mathbf{x}\mathbf{x}^T] = \mathbf{A}\mathbf{A}^T$, and has density

$$f(\mathbf{x}) = \frac{1}{(\sqrt{2\pi})^n \sqrt{\det(\mathbf{A}\mathbf{A}^T)}} e^{-\frac{\mathbf{x}^T \mathbf{x}}{2(\mathbf{A}\mathbf{A}^T)}}. \quad (54)$$

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

$$\mathbf{m} = F(\mathbf{v}) = e^{\frac{-\mathbf{m}^T \mathbf{A} \mathbf{A}^T \mathbf{m}}{2}} = e^{\frac{-\sigma_{\omega_0}^2 (m_1^2 + \dots + m_n^2)}{2}}. \quad (55)$$

In the first step of AMQD, Alice applies the inverse FFT (fast Fourier transform) operation to vector $\mathbf{z}$ (see (47)), which results in an n -dimensional zero-mean, circular symmetric complex Gaussian random vector $\mathbf{d}$, $\mathbf{d} \in \mathcal{CN}(0, \mathbf{K}_d)$, $\mathbf{d} = (d_1, \dots, d_n)^T$, as

$$\mathbf{d} = F^{-1}(\mathbf{z}) = e^{\frac{\mathbf{d}^T \mathbf{A} \mathbf{A}^T \mathbf{d}}{2}} = e^{\frac{\sigma_{\omega_0}^2 (d_1^2 + \dots + d_n^2)}{2}}, \quad (56)$$

where

$$d_i = x_{d_i} + ip_{d_i}, d_i \in \mathcal{CN}(0, \sigma_{d_i}^2), \quad (57)$$

where $\sigma_{\omega_{d_i}}^2 = \mathbb{E}[|d_i|^2]$ and the position and momentum quadratures of $|\phi_i\rangle$ are i.i.d. Gaussian random variables

$$\text{Re}(d_i) = x_{d_i} \in \mathcal{N}(0, \sigma_{\omega_i}^2), \text{Im}(d_i) = p_{d_i} \in \mathcal{N}(0, \sigma_{\omega_i}^2), \quad (58)$$

where $\mathbf{K}_d = \mathbb{E}[\mathbf{d}\mathbf{d}^T]$, $\mathbb{E}[\mathbf{d}] = \mathbb{E}[e^{i\gamma} \mathbf{d}] = \mathbb{E}[e^{i\gamma} \mathbf{d}]$, and $\mathbb{E}[\mathbf{d}\mathbf{d}^T] = \mathbb{E}[e^{i\gamma} \mathbf{d} (e^{i\gamma} \mathbf{d})^T] = \mathbb{E}[e^{i2\gamma} \mathbf{d}\mathbf{d}^T]$, for any $\gamma \in [0, 2\pi]$.

The $\mathbf{T}(\mathcal{N})$ transmittance vector of $\mathcal{N}$ in the multicarrier transmission is

$$\mathbf{T}(\mathcal{N}) = [T_1(\mathcal{N}_1), \dots, T_n(\mathcal{N}_n)]^T \in \mathbb{C}^n, \quad (59)$$

where

$$T_i(\mathcal{N}_i) = \text{Re}(T_i(\mathcal{N}_i)) + i\text{Im}(T_i(\mathcal{N}_i)) \in \mathbb{C}, \quad (60)$$

is a complex variable, which quantifies the position and momentum quadrature transmission (i.e., gain) of the i th Gaussian sub-channel $\mathcal{N}_i$, in the phase space $\mathcal{S}$, with real and imaginary parts

$$0 \leq \text{Re}T_i(\mathcal{N}_i) \leq 1/\sqrt{2}, \quad (61)$$

and

$$0 \leq \text{Im}T_i(\mathcal{N}_i) \leq 1/\sqrt{2}. \quad (62)$$

Particularly, the $T_i(\mathcal{N}_i)$ variable has the squared magnitude of

$$|T_i(\mathcal{N}_i)|^2 = \text{Re}T_i(\mathcal{N}_i)^2 + \text{Im}T_i(\mathcal{N}_i)^2 \in \mathbb{R}, \quad (63)$$

where

$$\text{Re}T_i(\mathcal{N}_i) = \text{Im}T_i(\mathcal{N}_i). \quad (64)$$

The Fourier-transformed transmittance of the i th sub-channel $\mathcal{N}_i$ (resulted from CVQFT operation at Bob) is denoted by

$$|F(T_i(\mathcal{N}_i))|^2. \quad (65)$$

The n -dimensional zero-mean, circular symmetric complex Gaussian noise vector $\Delta \in \mathcal{CN}(0, \sigma_{\Delta}^2)_n$ of the quantum channel $\mathcal{N}$, is evaluated as

$$\Delta = (\Delta_1, \dots, \Delta_n)^T \in \mathcal{CN}(0, \mathbf{K}_{\Delta}), \quad (66)$$

where

$$\mathbf{K}_{\Delta} = \mathbb{E}[\Delta\Delta^T]. \quad (67)$$

with independent, zero-mean Gaussian random components

$$\Delta_{x_i} \in \mathcal{N}(0, \sigma_{\mathcal{N}_i}^2), \quad (68)$$

and

$$\Delta_{p_i} \in \mathcal{N}(0, \sigma_{\mathcal{N}_i}^2), \quad (69)$$

with variance $\sigma_{\mathcal{N}_i}^2$, for each Δ_i of a Gaussian sub-channel $\mathcal{N}_i$, 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 can be rewritten as

$$F(\Delta) = (F(\Delta_1), \dots, F(\Delta_n))^T, \quad (70)$$

with independent components $F(\Delta_{x_i}) \in \mathcal{N}(0, \sigma_{F(\mathcal{N}_i)}^2)$ and $F(\Delta_{p_i}) \in \mathcal{N}(0, \sigma_{F(\mathcal{N}_i)}^2)$ on the quadratures, for each $F(\Delta_i)$.

It also defines an n -dimensional zero-mean, circular symmetric complex Gaussian random vector $F(\Delta) \in \mathcal{CN}(0, \mathbf{K}_{F(\Delta)})$ with a covariance matrix

$$\mathbf{K}_{F(\Delta)} = \mathbb{E}[F(\Delta)F(\Delta)^T], \quad (71)$$

where $\mathbf{K}_{F(\Delta)} = \mathbf{K}_{\Delta}$, by theory. At a constant subcarrier modulation variance $\sigma_{\omega_i}^2$ for the n Gaussian subcarrier CVs, the corresponding relation is

$$\frac{1}{n} \sum_{i=1}^n \sigma_{\omega_i}^2 = \sigma_{\omega}^2, \quad (72)$$

where $\sigma_{\omega_i}^2$ is the modulation variance of the quadratures of the subcarrier $|\phi_i\rangle$ transmitted by sub-channel $\mathcal{N}_i$. Assuming l good Gaussian sub-channels from the n with constant quadrature modulation variance $\sigma_{\omega_i}^2$, where $\sigma_{\omega_i}^2 = 0$ for the i th unused sub-channel

$$\sum_{i=1}^l \sigma_{\omega_i}^2 = l\sigma_{\omega}^2 < n\sigma_{\omega_0}^2. \quad (73)$$

In particular, from the relation of (73), for the transmittance parameters the following relation follows at a given modulation variance $\sigma_{\omega_0}^2$, precisely,

$$|T_{\text{AMQD}}(\mathcal{N}_i)|^2 \sigma_{\omega_0}^2 > |T(\mathcal{N})|^2 \sigma_{\omega_0}^2, \quad (74)$$

where $|T(\mathcal{N})|^2$ is the transmittance of $\mathcal{N}$ in a single-carrier scenario, and

$$|\phi_i\rangle = |d_i\rangle = |F^{-1}(z)\rangle. \quad (76)$$

$$|T_{\text{AMQD}}(\mathcal{N}_i)|^2 = \frac{1}{l} \sum_{i=1}^l |F(T_i(\mathcal{N}_i))|^2. \quad (75)$$

A.2 Notations

For the method of the determination of these l Gaussian sub-channels, see [15]. Alice's i th Gaussian subcarrier is expressed as

The notations of the manuscript are summarized in Table 1.

Table 1 Summary of notations

Notation	Description
i	Index for the i -th subcarrier Gaussian CV, $ \phi_i\rangle = x_i + ip_i$.
j	Index for the j -th Gaussian single-carrier CV, $ \varphi_j\rangle = x_j + ip_j$.
l	Number of Gaussian sub-channels $\mathcal{N}_i$ for the transmission of the Gaussian subcarriers. The overall number of the sub-channels is n . The remaining $n - l$ sub-channels do not transmit valuable information.
x_i, p_i	Position and momentum quadratures of the i -th Gaussian subcarrier, $ \phi_i\rangle = x_i + ip_i$.
x'_i, p'_i	Noisy position and momentum quadratures of Bob's i -th noisy subcarrier Gaussian CV, $ \phi'_i\rangle = x'_i + ip'_i$.
x_j, p_j	Position and momentum quadratures of the j -th Gaussian single-carrier $ \varphi_j\rangle = x_j + ip_j$.
x'_j, p'_j	Noisy position and momentum quadratures of Bob's j -th recovered single-carrier Gaussian CV $ \varphi'_j\rangle = x'_j + ip'_j$.
$x_{A,i}, p_{A,i}$	Alice's quadratures in the transmission of the i -th subcarrier.
$ \phi_i\rangle, \phi'_i\rangle$	Transmitted and received Gaussian subcarriers.
$\mathbf{z}$	A d -dimensional input CV vector to transmit valuable information, $z \in \mathcal{CN}(0, \mathbf{K}_z)$.
$\mathbf{z}^T$	A d -dimensional noisy output vector, $\mathbf{z}^T = \mathbf{A}^T \mathbf{z} + (F^d(\Delta))^T = (z'_0, \dots, z'_{d-1})$, where $z'_j = \left(\frac{1}{l} \sum_{i=0}^{l-1} F(T_{j,i}(\mathcal{N}_{j,i})) \right) z_j + F(\Delta) \in \mathcal{CN}\left(0, 2(\sigma_{\omega_0}^2 + \sigma_{\mathcal{N}}^2)\right)$.
M	Measurement operator, homodyne or heterodyne measurement.
$\mathcal{S}$	Set of private rates, identifies $r + 2$ rate curves for a given subchannel $\mathcal{N}_i$, as $\mathcal{S} = \{R_{\min}(\mathcal{N}_i), R(q), R_{\max}(\mathcal{N}_i)\}, q = 0 \dots r - 1$, where $R_{\min}(\mathcal{N}_i) < R(0) \dots < R(r - 1) < R_{\max}(\mathcal{N}_i)$.
$R(q)$	A target private rate, refers to a target transmission rate of private classical information over $\mathcal{N}_i$. Also identified by $\underline{R}(\mathcal{N}_i)$.
$R(q - 1)$	A current private rate, refers to a current transmission rate of private classical information over $\mathcal{N}_i$. Also identified by $\bar{R}(\mathcal{N}_i)$.
$P(\mathcal{N}_i)$	Private classical capacity of a sub-channel $\mathcal{N}_i$.
$\chi_{AB}(\mathcal{N}_i)$	Holevo information of Alice (transmitter) and Bob (receiver), with respect to sub-channel $\mathcal{N}_i$.
$\chi_{BE}(\mathcal{N}_i)$	Holevo information of Bob and Eve (eavesdropper), with respect to sub-channel $\mathcal{N}_i$.
$S^*(\mathcal{N})$	Target secret key rate $S^*(\mathcal{N}) = \sum_{i=0}^{l-1} R_i(\mathcal{N}_i)$, where $R_i(\mathcal{N}_i)$ is the private rate of sub-channel $\mathcal{N}_i$.
$\mathbf{A}$	Adaption region, $\mathbf{A} = [R_{\min}(\mathcal{N}_i), R_{\max}(\mathcal{N}_i)]$, contains r private rate curves for the iteration.
$\text{SNR}(R(\mathcal{N}_i))$	SNR (signal to noise ratio) of $\mathcal{N}_i$ at private rate $R(\mathcal{N}_i)$, $\text{SNR}(R(\mathcal{N}_i)) = 10 \log_{10} \frac{1}{v_i(R(\mathcal{N}_i))},$ where $v_i(R(\mathcal{N}_i)) = \sigma_{R(\mathcal{N}_i)}^2 / F(T(R(\mathcal{N}_i))) ^2$, $\sigma_{R(\mathcal{N}_i)}^2$ is the noise variance of $\mathcal{N}_i$ at $R(\mathcal{N}_i)$, while $F(T(R(\mathcal{N}_i)))$ is the transmittance coefficient of $\mathcal{N}_i$ at $R(\mathcal{N}_i)$.
$\delta_{v_i}(R(\mathcal{N}_i))$	Cumulative $v_i(R(\mathcal{N}_i))$ of $\mathcal{N}_i$ at an increased (target) private rate $R(\mathcal{N}_i)$, evaluated as $\delta_{v_i}(R(\mathcal{N}_i)) = \delta_{v_i}(\underline{R}(\mathcal{N}_i)) + \Delta_{v_i}(R(\mathcal{N}_i), \bar{R}(\mathcal{N}_i))$ where $\underline{R}(\mathcal{N}_i)$ is the current private rate, $R(\mathcal{N}_i)$ is the target private rate for $\mathcal{N}_i$, $\underline{R}(\mathcal{N}_i) < R(\mathcal{N}_i) < \bar{R}(\mathcal{N}_i)$.

Table 1 (continued)

Notation	Description
Δ_{v_i}	Difference of v_i at $R(\mathcal{N}_i)$ and $\tilde{R}(\mathcal{N}_i)$, $\tilde{R}(\mathcal{N}_i) > R(\mathcal{N}_i) > 0$, $\Delta_{v_i} = v_i(R(\mathcal{N}_i)) - v_i(\tilde{R}(\mathcal{N}_i))$.
$\mathcal{B}$	Bit error rate of $\mathcal{N}_i$. At target private rate $R(q)$ at a current rate $R(q-1)$, and $\delta_{v_i}(R(q-1))$, is expressed as $\mathcal{B}(R(q)_{\delta_{v_i}(R(q-1))})$.
$\xi(R(q-1))$	Identifies that $\mathcal{N}_i$, $i = 0, \dots, l-1$ from the total l , for which $\delta_{v_i}(R(q-1))$ is minimal at a given $R(q)$, $\xi(R(q-1)) = \min_{\forall i} \delta_{v_i}(R(q-1))$, where $\xi(0) = \min_{\forall i} \delta_{v_i}(0) = \min_{\forall i} v_i$.
$R(q)_{\delta_{v_i}(R(q-1))}$	A target private rate $R(q)$ over $\mathcal{N}_i$ at a current $\delta_{v_i}(R(q-1))$.
$\mathcal{B}(R_{\min}(\mathcal{N}_i)_{\delta_{v_i}(R(q-1))})$	Minimal bit error rate, achievable at $R_{\min}(\mathcal{N}_i)$, at a given $\delta_{v_i}(R(q-1))$.
$\mathcal{F}(\cdot)$	Function, evaluates SNR quantities from the input $v_i(\cdot)$ parameters, defined as $\mathcal{F}(v_i(\mathcal{N}_i) + (\Delta_{v_i}(R_{\min}(\mathcal{N}_i), R(0)) + \dots + \Delta_{v_i}(R(q-1), R(q))))$ $= \left(\sqrt{\frac{\text{SNR}(v_i(\mathcal{N}_i)) - [\text{SNR}(v_i(R(0))) - \text{SNR}(v_i(R_{\min}(\mathcal{N}_i)))]}{\sum_{k=0}^{q-1} [\text{SNR}(v_i(R(k+1))) - \text{SNR}(v_i(R(k)))]}} \right)$, where $\text{SNR}(v_i(R(x))) = 10 \log_{10} (1/(v_i(R(x))))$.
$\text{erfc}(\cdot)$	Complementary error function, $\text{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-t^2} dt$.
U_k	A k -th user, $k = 0, \dots, K-1$.
$\mathcal{M}_{U_k}$	Logical channel of user U_k , $k = 0, \dots, K-1$, where K is the number of total users, $\mathcal{M}_{U_k} = [\mathcal{N}_{U_k,0}, \dots, \mathcal{N}_{U_k,m-1}]^T$, and $\mathcal{N}_{U_k,i}$ is the i -th sub-channel of $\mathcal{M}_{U_k}$, m is the number of subcarriers dedicated to U_k .
$S^*(\mathcal{M}_{U_k})$	Target secret key rate of $\mathcal{M}_{U_k}$, $S^*(\mathcal{M}_{U_k}) = \sum_{i=0}^{m-1} R(\mathcal{N}_{U_k,i})$, where $R(\mathcal{N}_{U_k,i})$ is the private rate of $\mathcal{N}_{U_k,i}$.
$\underline{R}(\mathcal{N}_{U_k,i})$	A current private rate of $\mathcal{N}_{U_k,i}$, $\underline{R}(\mathcal{N}_{U_k,i}) = R_i(q-1)$.
$\underline{R}(\mathcal{N}_{U_k,i})$	A target private rate of $\mathcal{N}_{U_k,i}$, $\underline{R}(\mathcal{N}_{U_k,i}) = R_i(q)$ where $R_i(q)$ refers to the $R(q)$ rate of $\mathcal{N}_{U_k,i}$, with relation $R_i(q-1) < R_i(q)$, $R_i(-1) = R_{\min}(\mathcal{N}_{U_k,i})$, and $R_i(r) = R_{\max}(\mathcal{N}_{U_k,i})$.
$\delta_{v_i}(R_i(q))$	Parameter δ_{v_i} of $\mathcal{N}_{U_k,i}$ at private rate $\underline{R}(\mathcal{N}_{U_k,i})$.
ξ_{U_k}	Identifies the minimal $\delta_{v_i}(\underline{R}(\mathcal{N}_{U_k,i}))$ parameter for the $\mathcal{N}_{U_k,i}$, $i = 0, \dots, m-1$ subchannels of the set $\mathcal{M}_{U_k}$, as $\xi_{U_k} = \min_{\forall i \in \mathcal{M}_{U_k}} \delta_{v_i}(\underline{R}(\mathcal{N}_{U_k,i}))$.
$\Delta_{\sigma_{\omega_i}^2}$	Modulation variance adaption at rate $\underline{R}(\mathcal{N}_{U_k,i})$, $\Delta_{\sigma_{\omega_i}^2} = \delta_{v_i}(\underline{R}(\mathcal{N}_{U_k,i})) - \xi_{U_k}$.
$\bar{\sigma}_{\omega}^2$	A corrected modulation variance, $\bar{\sigma}_{\omega}^2 = \sigma_{\omega}^2 + \Delta_{\sigma_{\omega_i}^2}$, where σ_{ω}^2 is the initial input subcarrier modulation variance, and $\Delta_{\sigma_{\omega_i}^2} = \delta_{v_i}(\underline{R}(\mathcal{N}_{U_k,i})) - \xi_{U_k}$.
$\varphi_{\delta_{v_i}}(R(\mathcal{N}_{U_k,i}))$	The resulting δ_{v_i} parameter for $\mathcal{N}_{U_k,i}$ at a target rate $\underline{R}(\mathcal{N}_{U_k,i})$, $\varphi_{\delta_{v_i}}(R(\mathcal{N}_{U_k,i})) = \delta_{v_i}(\underline{R}(\mathcal{N}_{U_k,i})) - \xi_{U_k}$.
$\Delta_{\text{SNR}}(\varphi_{\delta_{v_i}}(\underline{R}(\mathcal{N}_{U_k,i})))$	SNR increment of $\mathcal{N}_{U_k,i}$, achieved by $\Delta_{\sigma_{\omega_i}^2}$ at a given $\underline{R}(\mathcal{N}_{U_k,i}) = R(q)$.
$\mathcal{B}(\underline{R}(\mathcal{N}_{U_k,i})_{\xi_{U_k}})$	An equally minimized bit error rate for all $\mathcal{N}_{U_k,i}$ at an arbitrary $\underline{R}(\mathcal{N}_{U_k,i})_{\delta_{v_i}(\underline{R}(\mathcal{N}_{U_k,i}))}$.
F	Fourier transform (FFT).

Table 1 (continued)

Notation	Description
Φ_{U_k}	A d -dimensional input vector of user U_k , $k = 0, \dots, K-1$, $\Phi_{U_k} = (\varphi_{U_k,0}, \dots, \varphi_{U_k,d-1})^T$, where $\varphi_{U_k,j}$ refers to the j -th single-carrier CV, $\varphi_{U_k,j} = x_{U_k,j} + ip_{U_k,j}$, and $\{x_{U_k,j}, p_{U_k,j}\}$ are Gaussian random quadratures.
$\mathbf{x}_{U_k}$	A d -dimensional vector of U_k , $\mathbf{x}_{U_k} = (x_{U_k,0}, \dots, x_{U_k,d-1})^T$, where $x_{U_k,j}$ is the quadrature component of $\varphi_{U_k,j}$.
$x'_{U_k,i}$	Noisy subcarrier, discrete variable, $x'_{U_k,i} = M(\phi'_{U_k,i})$, where M is a measurement operator, and $\phi'_{U_k,i}$ is the i -th noisy Gaussian subcarrier CV of U_k .
z	The variable of a single-carrier Gaussian CV state, $ \varphi_i\rangle \in \mathcal{S}$, $z \in \mathcal{CN}(0, \sigma_z^2)$. Zero-mean, circular symmetric complex Gaussian random variable, $\sigma_z^2 = \mathbb{E}[z ^2] = 2\sigma_{\omega_0}^2$, with i.i.d. zero mean, Gaussian random quadrature components $x, p \in \mathcal{N}(0, \sigma_{\omega_0}^2)$, where $\sigma_{\omega_0}^2$ is the variance.
Δ	The noise variable of the Gaussian channel $\mathcal{N}$, $\Delta \in \mathcal{CN}(0, \sigma_\Delta^2)$, with i.i.d. zeromean, Gaussian random noise components on the position and momentum quadratures $\Delta_x, \Delta_p \in \mathcal{N}(0, \sigma_\Delta^2)$, $\sigma_\Delta^2 = \mathbb{E}[\Delta ^2] = 2\sigma_\Delta^2$.
d	The variable of a Gaussian subcarrier CV state, $ \phi_i\rangle \in \mathcal{S}$, $d \in \mathcal{CN}(0, \sigma_d^2)$. Zero-mean, circular symmetric Gaussian random variable, $\sigma_d^2 = \mathbb{E}[d ^2] = 2\sigma_\omega^2$, with i.i.d. zero mean, Gaussian random quadrature components $x_d, p_d \in \mathcal{N}(0, \sigma_\omega^2)$, where σ_ω^2 is the (constant) modulation variance of the Gaussian subcarrier CV state.
$F^{-1}(\cdot)$	The inverse CVQFT transformation, $F^{-1}(\cdot) = \text{CVQFT}^\dagger(\cdot)$, applied by the encoder, continuous-variable unitary operation.
$F(\cdot)$	The CVQFT transformation, $F(\cdot) = \text{CVQFT}(\cdot)$, applied by the decoder, continuous-variable unitary operation.
$F^{-1}(\cdot)$	Inverse FFT transform, $F^{-1}(\cdot) = \text{IFFT}(\cdot)$, applied by the encoder.
$\sigma_{\omega_0}^2$	Single-carrier modulation variance.
σ_ω^2	Multicarrier modulation variance, $\sigma_\omega^2 = \frac{1}{l} \sum_l \sigma_{\omega_i}^2$. Average modulation variance of the l Gaussian sub-channels $\mathcal{N}_i$.
$ \phi_i\rangle$	The i -th Gaussian subcarrier CV of user U_k , where IFFT stands for the Inverse Fast Fourier Transform, $ \phi_i\rangle \in \mathcal{S}$, $ \phi_i\rangle = \text{IFFT}(z_{k,i})\rangle = F^{-1}(z_{k,i})\rangle = d_i\rangle$, $d_i \in \mathcal{CN}(0, \sigma_{d_i}^2)$, $\sigma_{d_i}^2 = \mathbb{E}[d_i ^2]$, $d_i = x_{d_i} + ip_{d_i}$, $x_{d_i} \in \mathcal{N}(0, \sigma_{\omega_F}^2)$, $p_{d_i} \in \mathcal{N}(0, \sigma_{\omega_F}^2)$ are i.i.d. zeromean Gaussian random quadrature components, and $\sigma_{\omega_F}^2$ is the variance of the Fourier transformed Gaussian state.
$ \varphi_{k,i}\rangle$	The decoded single-carrier CV of user U_k from the subcarrier CV, $ \varphi_{k,i}\rangle = \text{CVQFT}(\phi_i\rangle)$, expressed as $F(d_i\rangle) = F(F^{-1}(z_{k,i}))\rangle = z_{k,i}\rangle$.
$\mathcal{N}$	Gaussian quantum channel.
$\mathcal{N}_i$	An i -th Gaussian sub-channel, $\mathcal{N}_i, i = 0, \dots, n-1$.
$T(\mathcal{N})$	Channel transmittance, normalized complex random variable, $T(\mathcal{N}) = \text{Re}T(\mathcal{N}) + i\text{Im}T(\mathcal{N}) \in \mathcal{C}$. The real part identifies the position quadrature transmission, the imaginary part identifies the transmittance of the position quadrature.
$T_i(\mathcal{N}_i)$	Transmittance coefficient of Gaussian subchannel $\mathcal{N}_i$, $T_i(\mathcal{N}_i) = \text{Re}(T_i(\mathcal{N}_i)) + i\text{Im}(T_i(\mathcal{N}_i)) \in \mathcal{C}$, quantifies the position and momentum quadrature transmission, with (normalized) real and imaginary parts $0 \leq \text{Re}T_i(\mathcal{N}_i) \leq 1/\sqrt{2}$, $0 \leq \text{Im}T_i(\mathcal{N}_i) \leq 1/\sqrt{2}$, where $\text{Re}T_i(\mathcal{N}_i) = \text{Im}T_i(\mathcal{N}_i)$.
T_{Eve}	Eve's transmittance, $T_{\text{Eve}} = 1 - T(\mathcal{N})$.
$T_{\text{Eve},i}$	Eve's transmittance for the i -th subcarrier CV.
$\mathbf{z}$	A d -dimensional, zero-mean, circular symmetric complex random Gaussian vector, $\mathbf{z} = \mathbf{x} + i\mathbf{p} = (z_0, \dots, z_{d-1})^T$, that models d Gaussian CV input states, $\mathcal{CN}(0, \mathbf{K}_z)$, $\mathbf{K}_z = \mathbb{E}[\mathbf{z}\mathbf{z}^\dagger]$, where $z_j = x_j + ip_j$, $\mathbf{x} = (x_0, \dots, x_{d-1})^T$, $\mathbf{p} = (p_0, \dots, p_{d-1})^T$, $x_j \in \mathcal{N}(0, \sigma_{\omega_0}^2)$, $p_j \in \mathcal{N}(0, \sigma_{\omega_0}^2)$ i.i.d. zeromean Gaussian random variables.
$\mathbf{d}$	An l -dimensional, zero-mean, circular symmetric complex random Gaussian vector, $\mathbf{d} = F^{-1}(\mathbf{z})$, $\mathcal{CN}(0, \mathbf{K}_d)$, $\mathbf{K}_d = \mathbb{E}[\mathbf{d}\mathbf{d}^\dagger]$, $\mathbf{d} = (d_0, \dots, d_{l-1})^T$, $d_i = x_i + ip_i$, $x_i, p_i \in \mathcal{N}(0, \sigma_{\omega_F}^2)$ are i.i.d. zero-mean Gaussian random variables. The i -th component is $d_i \in \mathcal{CN}(0, \sigma_{d_i}^2)$, $\sigma_{d_i}^2 = \mathbb{E}[d_i ^2]$.
$\mathbf{y}_k$	A d -dimensional zero-mean, circular symmetric complex Gaussian random vector, $\mathbf{y}_k \in \mathcal{CN}(0, \mathbb{E}[\mathbf{y}_k\mathbf{y}_k^\dagger])$.
$y_{k,m}$	The m -th element of the k -th user's vector $\mathbf{y}_k$, expressed as $y_{k,m} = \sum_l F(T_i(\mathcal{N}_i))F(d_i) + F(\Delta_i)$.

Table 1 (continued)

Notation	Description
$F(\mathbf{T}(\mathcal{N}))$	Fourier transform of $\mathbf{T}(\mathcal{N}) = [T_0(\mathcal{N}_0) \dots T_{l-1}(\mathcal{N}_{l-1})]^T \in \mathcal{C}^l$, the complex transmittance vector.
$F(\Delta)$	Complex vector, expressed as $F(\Delta) = e^{\frac{-F(\Delta)^T \mathbf{K}_{F(\Delta)} F(\Delta)}{2}}$, with covariance matrix $\mathbf{K}_{F(\Delta)} = \mathbb{E}[F(\Delta)F(\Delta)^\dagger]$.
$\mathbf{y}[j]$	AMQD block, $\mathbf{y}[j] = F(\mathbf{T}(\mathcal{N}))F(\mathbf{d})[j] + F(\Delta)[j]$.
τ	An exponentially distributed variable, $\tau = \ F(\mathbf{d})[j]\ ^2$, with density $f(\tau) = (1/2\sigma_\omega^2) e^{-\tau/2\sigma_\omega^2}$, $\mathbb{E}[\tau] \leq n2\sigma_\omega^2$.
$T_{Eve,i}$	Eve's transmittance on the Gaussian sub-channel $\mathcal{N}_i$, $T_{Eve,i} = \text{Re}T_{Eve,i} + i\text{Im}T_{Eve,i} \in \mathcal{C}$, $0 \leq \text{Re}T_{Eve,i} \leq 1/\sqrt{2}$, $0 \leq \text{Im}T_{Eve,i} \leq 1/\sqrt{2}$, $0 \leq T_{Eve,i} ^2 < 1$.
d_i	A d_i subcarrier in an AMQD block.
$v_{\min}$	The $\min\{v_0, \dots, v_{l-1}\}$ minimum of the v_i sub-channel coefficients, where $v_i = \sigma_{\mathcal{N}}^2 / F(T_i(\mathcal{N}_i)) ^2$ and $v_i < v_{Eve}$.
σ_ω^2	Constant modulation variance, $\sigma_\omega^2 = v_{Eve} - v_{\min} \mathcal{G}(\delta)_{p(x)}$, $v_{Eve} = \frac{1}{\lambda}$, $\lambda = F(T_{\mathcal{N}}^*) ^2 = \frac{1}{n} \sum_{i=0}^{n-1} \left \sum_{k=0}^{n-1} T_k^* e^{\frac{-i2\pi ik}{n}} \right ^2$ and $T_{\mathcal{N}}^*$ is the expected transmittance of the Gaussian sub-channels under an optimal Gaussian collective attack.

References

- Adcock MRA, Hoyer P, Sanders BC. Limitations on continuous-variable quantum algorithms with Fourier transforms. *N J Phys*. 2009;11:103035.
- Gyongyosi L, Imre S, Nguyen HV. A survey on quantum channel capacities. *IEEE Commun Surv Tut*. 2018;99:1. <https://doi.org/10.1109/COMST.2017.2786748>.
- Biamonte J, et al. Quantum machine learning. *Nature*. 2017;549:195–202.
- Garcia-Patron R, Cerf NJ. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Phys Rev Lett*. 2006;97:190503.
- Grosshans F. Collective attacks and unconditional security in continuous variable quantum key distribution. *Phys Rev Lett*. 2005;94:20504.
- Grosshans F, Cerf NJ, Wenger J, Tualle-Brouiri R, Grangier P. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quant Inf Comput*. 2003;3:535–52.
- Pirandola S, Laurenza R, Ottaviani C, Banchi L. Fundamental limits of repeaterless quantum communications. *Nat Commun*. 2017;8:15043. <https://doi.org/10.1038/ncomms15043>.
- Pirandola S, Braunstein SL, Laurenza R, Ottaviani C, Cope TPW, Spedalieri G, Banchi L. Theory of channel simulation and bounds for private communication. *Quantum Sci Technol*. 2018;3:35009. <https://doi.org/10.1088/2058-9565/aac394>.
- Pirandola S. Capacities of repeater-assisted quantum communications. 2016. [arXiv:1601.00966](https://arxiv.org/abs/1601.00966).
- Pirandola S. End-to-end capacities of a quantum communication network. *Commun Phys*. 2019;2:51.
- Pirandola S, Braunstein SL, Lloyd S. Characterization of collective gaussian attacks and security of coherent-state quantum cryptography. *Phys Rev Lett*. 2008;101:200504.
- Pirandola S, Garcia-Patron R, Braunstein SL, Lloyd S. Direct and reverse secret-key capacities of a quantum channel. *Phys Rev Lett*. 2009;102:50503.
- Pirandola S, Mancini S, Lloyd S, Braunstein SL. Continuous-variable quantum cryptography using two-way quantum communication. *Nat Phys*. 2008;4:726–30.
- Pirandola S, Serafini A, Lloyd S. Correlation matrices of two-mode bosonic systems. *Phys Rev A*. 2009;79:52327.
- Gyongyosi L, Imre S. Adaptive multicarrier quadrature division modulation for long-distance continuous-variable quantum key distribution. In: *Proc. SPIE 9123 Quantum Information and Computation XII*, “912307,” from Conference Volume 9123 Quantum Information and Computation XII, Baltimore, Maryland, USA 2014. <https://doi.org/10.1117/12.2050095>.
- Gyongyosi L, Imre S. Diversity space of multicarrier continuous-variable quantum key distribution. *Int J Commun Syst*. 2019. <https://doi.org/10.1002/dac.4003>.
- Gyongyosi L, Imre S. Gaussian quadrature inference for multicarrier continuous-variable quantum key distribution. *Quantum Stud Math Found*. 2019. <https://doi.org/10.1007/s40509-019-00183-9>.
- Gyongyosi L, Imre S. Statistical quadrature evolution by inference for multicarrier continuous-variable quantum key distribution. *Quantum Stud Math Found*. 2019. <https://doi.org/10.1007/s40509-019-00202-9>.
- Gyongyosi L, Imre S. Geometrical analysis of physically allowed quantum cloning transformations for quantum cryptography. *Inf Sci*. 2014;285:1–23. <https://doi.org/10.1016/j.ins.2014.07.010>.
- Gyongyosi L, Imre S. Multiple access multicarrier continuous-variable quantum key distribution. *Chaos, Solitons Fractals*. 2018;114:491–505. <https://doi.org/10.1016/j.chaos.2018.07.006>.
- Gyongyosi L, Imre S. Secret key rate proof of multicarrier continuous-variable quantum key distribution. *Int J Commun Syst*. 2018. <https://doi.org/10.1002/dac.3865>.
- Gyongyosi L. Singular value decomposition assisted multicarrier continuous-variable quantum key distribution. *Theor Comput Sci*. 2019. <https://doi.org/10.1016/j.tcs.2019.07.029>.
- Gyongyosi L, Imre S. Secret key rates of free-space optical continuous-variable quantum key distribution. *Int J Commun Syst*. 2019. <https://doi.org/10.1002/dac.4152>.
- Gyongyosi L, Imre S. Proceedings volume 8997 advances in photonics of quantum computing, memory, and communication “VII,” “89970C,”. 2014. <https://doi.org/10.1117/12.2038532>.
- Gyongyosi L, Imre S. Long-distance continuous-variable quantum key distribution with advanced reconciliation of a gaussian modulation. In: *Proceedings of SPIE Photonics West OPTO*. 2013; 2013.

26. Gyongyosi L, Imre S. Low-dimensional reconciliation for continuous-variable quantum key distribution. *Appl Sci*. 2018. <https://doi.org/10.3390/app8010087> (ISSN 2076-3417).
27. Gyongyosi L. Diversity extraction for multicarrier continuous-variable quantum key distribution. In: *Proceedings of the 2016 24th European Signal Processing Conference (EUSIPCO 2016)*, 2016.
28. Gyongyosi L, Imre S. Eigenchannel decomposition for continuous-variable quantum key distribution. In: *Proceedings Volume 9377 advances in photonics of quantum computing, memory, and communication "VIII;"* 937711. 2015. <https://doi.org/10.1117/12.2076532>.
29. Gyongyosi L, Imre S. Singular layer transmission for continuous-variable quantum key distribution. In: *IEEE Photonics Conference (IPC) 2014 IEEE*. 2014. <https://doi.org/10.1109/IPCCon.2014.6995246>.
30. Gyongyosi L, Imre S. Adaptive Gaussian quadrature detection for continuous-variable quantum key distribution. In: *SPIE advances in photonics of quantum computing memory and communication IX*, 2016.
31. Gyongyosi L, Imre S. Gaussian quadrature inference for multicarrier continuous-variable quantum key distribution. In: *SPIE quantum information and computation XIV*, 17–21 Apr 2016 Baltimore, Maryland, USA. 2016.
32. Gyongyosi L, Bacsardi L, Imre S. A survey on quantum key distribution. *Infocommun J*. 2019;XI(2):14–21.
33. Heinzel G, Rudiger A, Schilling R. Spectrum and spectral density estimation by the Discrete Fourier transform (DFT), including a comprehensive list of window functions and some new at-top windows. 2002. <http://hdl.handle.net/11858/00-001M-0000-0013-557A-5>.
34. Imre S, Gyongyosi L. *Advanced quantum communications—an engineering approach*. New Jersey: Wiley-IEEE Press; 2012 (ISBN-10: 1118002369 ISBN-13: 978-11180023).
35. Imre S, Balazs F. *Quantum computing and communications—an engineering approach*. Hoboken: Wiley; 2005 (ISBN 0-470-86902-X).
36. Jahromi OS. *Multirate statistical signal processing*. Berlin: Springer; 2007 (ISBN-10 1-4020-5316-9).
37. Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P, Diamanti E. Experimental demonstration of long-distance continuous-variable quantum key distribution. 2012. [arXiv:1210.6216v1](https://arxiv.org/abs/1210.6216v1).
38. Kay S. *Fundamentals of statistical signal processing, vol. I-III*. Upper Saddle River: Prentice Hall; 2013 (ISBN-13: 978-0133457117).
39. Kiktenko EO, Pozhar NO, Anufriev MN, Trushechkin AS, Yunusov RR, Kurochkin YV, Lvovsky AI, Fedorov AK. Quantum-secured blockchain. *Quantum Sci Technol*. 2018;3:35004.
40. Kimble HJ. The quantum Internet. *Nature*. 2008;453:1023–30. <https://doi.org/10.1038/nature07127>.
41. Laudenbach F, Pacher C, Fred Fung C-H, Poppe A, Peev M, Schrenk B, Hentschel M, Walther P, Hubel H. Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations. *Adv Quantum Technol*. 2018;1(1):1–37.
42. Laurenza R, Pirandola S. General bounds for sender-receiver capacities in multipoint quantum communications. *Phys Rev A*. 2017;96:32318.
43. Lloyd S. Capacity of the noisy quantum channel. *Phys Rev A*. 1997;55:1613–22.
44. Lloyd S, Mohseni M, Rebentrost P. Quantum algorithms for supervised and unsupervised machine learning. 2013. [arXiv:1307.0411](https://arxiv.org/abs/1307.0411).
45. Lloyd S, Mohseni M, Rebentrost P. Quantum principal component analysis. *Nat Phys*. 2014;10:631.
46. Lloyd S, Shapiro JH, Wong FNC, Kumar P, Shahriar SM, Yuen HP. Infrastructure for the quantum Internet. *ACM SIGCOMM Comput Commun Rev*. 2004;34:9–20.
47. Middleton D. *An introduction to statistical communication theory: an IEEE Press Classic Reissue, Hardcover*, IEEE, ISBN-10: 780311787 ISBN-13: 978-0780311787 1960.
48. Muralidharan S, Kim J, Lutkenhaus N, Lukin MD, Jiang L. Ultrafast and fault-tolerant quantum communication across long distances. *Phys Rev Lett*. 2014;112:250501.
49. Navascues M, Acin A. Security bounds for continuous variables quantum key distribution. *Phys Rev Lett*. 2005;94:20505.
50. Navascues M, Grosshans F, Acin A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys Rev Lett*. 2006;97:190502.
51. Petz D. *Quantum information theory and quantum statistics*. Heidelberg: Springer-Verlag; 2008 Hiv: 6.
52. Press WH, Teukolsky SA, Vetterling WT, Flannery BP. *Numerical recipes in C: the art of scientific computing*. Cambridge: Cambridge University Press; 1993 ISBN : 0-521-43108-5.
53. Shieh W, Djordjevic I. *OFDM for optical communications*. Amsterdam: Elsevier; 2010. p. 456 (Hardcover ISBN: 9780123748799, eBook ISBN: 9780080952062).
54. Shor PW. Scheme for reducing decoherence in quantum computer memory. *Phys Rev A*. 1995;52:R2493–6.
55. Rohling H, Fellenberg C. *Successive bit loading concept. OFDM concepts for future communication systems*. Berlin: Springer; 2011.
56. Tse D, Viswanath P. *Fundamentals of wireless communication*. Cambridge: Cambridge University Press; 2005 ISBN-13: 978-0521845274, ISBN-10: 521845270.
57. Van Meter R. *Quantum networking*. Hoboken: Wiley; 2014. p. 368 ISBN-13: 978-1848215375, ISBN-10: 9781848215375.
58. Weedbrook C, Pirandola S, Lloyd S, Ralph T. Quantum cryptography approaching the classical limit. *Phys Rev Lett*. 2010;105:110501.
59. Weedbrook C, Pirandola S, Garcia-Patron R, Cerf NJ, Ralph T, Shapiro J, Lloyd S. Gaussian quantum information. *Rev Mod Phys*. 2012;84:621.
60. Gyongyosi L, Imre S. Decentralized base-graph routing for the quantum internet. *Phys Rev A Am Phys Soc*. 2018. <https://doi.org/10.1103/PhysRevA.98.022310>.
61. Gyongyosi L, Imre S. Entanglement-gradient routing for quantum networks. *Sci Rep*. 2017. <https://doi.org/10.1038/s41598-017-14394-w>.
62. Gyongyosi L, Imre S. Entanglement availability differentiation service for the quantum internet. *Sci Rep Nat*. 2018. <https://doi.org/10.1038/s41598-018-28801-3>.
63. Bacsardi L. On the way to quantum-based satellite communication. *IEEE Commun Mag*. 2013;51(08):50–5.
64. Zhang H, Mao Y, Huang D, Li J, Zhang L, Guo Y. Security analysis of orthogonal-frequency-division-multiplexing-based continuous-variable quantum key distribution with imperfect modulation. *Phys Rev A*. 2018;97:52328.
65. Zhao W, Liao Q, Huang D, et al. Performance analysis of the satellite-to-ground continuous-variable quantum key distribution with orthogonal frequency division multiplexed modulation. *Quant Inf Proc*. 2019;18:39. <https://doi.org/10.1007/s11228-018-2147-8>.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.