


## RESEARCH ARTICLE

# Diversity space of multicarrier continuous-variable quantum key distribution

Laszlo Gyongyosi<sup>1,2,3</sup>  | Sandor Imre<sup>2</sup>

<sup>1</sup> School of Electronics and Computer Science, University of Southampton, Southampton, UK

<sup>2</sup> Department of Networked Systems and Services, Budapest University of Technology and Economics, Budapest, Hungary

<sup>3</sup> MTA-BME Information Systems Research Group, Hungarian Academy of Sciences, Budapest, Hungary

## Correspondence

Laszlo Gyongyosi, School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, UK.  
Email: lasgy\_ph@yahoo.com

## Funding information

National Research Development and Innovation Office of Hungary, Grant/Award Number: 2017-1.2.1-NKP-2017-00001; Hungarian Scientific Research Fund, Grant/Award Number: OTKA K-112125; BME Artificial Intelligence FIKP, Grant/Award Number: EMMI (BMEFIKP-MI/SC)

## Summary

The diversity space of multicarrier continuous-variable quantum key distribution (CVQKD) is defined. The diversity space utilizes the resources that are injected into the transmission by the additional degrees of freedom of the multicarrier modulation. We prove that the exploitable extra degree of freedom in a multicarrier CVQKD scenario significantly extends the possibilities of single-carrier CVQKD. The manifold extraction allows for the parties to reach decreased error probabilities by utilizing those extra resources of a multicarrier transmission that are not available in a single-carrier CVQKD setting. We define the multidimensional manifold space of multicarrier CVQKD and the optimal tradeoff between the available degrees of freedom of the multicarrier transmission. We extend the manifold extraction for the multiple-access AMQD-MQA (multiuser quadrature allocation) multicarrier protocol. The additional resources of multicarrier CVQKD allow the achievement of significant performance improvements that are particularly crucial in an experimental scenario.

## KEYWORDS

cryptography, networking, quantum communication, quantum key distribution, security

## 1 | INTRODUCTION

The multicarrier CVQKD modulation has been proposed through the multicarrier transmission scheme of AMQD (adaptive multicarrier quadrature division).<sup>1-11</sup> The AMQD allows improved secret key rates and higher tolerable excess noise in comparison with standard (referred to as single-carrier<sup>1-4,8-35,36,37</sup> throughout) CVQKD. The multicarrier transmission granulates the information into several Gaussian subcarrier CVs, which are then transmitted through the Gaussian subchannels. Particularly, the AMQD divides the physical Gaussian channel into several Gaussian subchannels; each subchannel is dedicated for the conveying of a given Gaussian subcarrier CV. Similar to single-carrier CVQKD, a multicarrier CVQKD also provides an unconditional security against the most powerful attacks.<sup>2</sup> Specifically, the benefits

**Abbreviations:** AMQD, adaptive multicarrier quadrature division; AWGN, additive white Gaussian noise; BS, beam splitter; CV, continuous-variable; CVQFT, continuous-variable quantum Fourier transform; DV, discrete-variable; FFT, fast Fourier transform; IFFT, inverse fast Fourier transform; MQA, multiuser quadrature allocation; QKD, quantum key distribution; SNR, signal-to-noise ratio; SVD, singular value decomposition.

Parts of this work were presented in conference proceedings.<sup>1,6</sup>

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2019 The Authors International Journal of Communication Systems Published by John Wiley & Sons Ltd.

of AMQD can be extended by SVD-assistance (singular value decomposition) through the SVD-assisted AMQD.<sup>7,8</sup> Precisely, the SVD-assistance further injects an additional degree of freedom into the multicarrier transmission. The multicarrier CVQKD has been also proposed for a multiple-access scenario through the AMQD-MQA (multiuser quadrature allocation) scheme.<sup>3</sup> The AMQD-MQA allows for several legal parties to perform reliable simultaneous secret communication over a shared physical Gaussian link through the combination of a sophisticated allocation mechanism of the Gaussian subcarriers and the careful utilization of the Gaussian subchannels. The secret key rates and security thresholds of multicarrier transmission have been proven in Gyongyosi and Imre,<sup>2</sup> leading to enhanced secret key rates in both one- and two-way CVQKD.<sup>12,38–52</sup> For further information on the bounds of private quantum communications, we suggest Pirandola et al.<sup>48,49</sup> The common root of these improvements is that the additional degrees of freedom injected by the multicarrier transmission act as a resource, allowing for the parties to exceed significantly the possibilities of single-carrier CVQKD. We also further confirm this statement in this work through the utilization of these extra resources.<sup>6</sup>

In traditional communications, the diversity is an effective technique to improve the performance of communication over a noisy channel.<sup>53–57</sup> The diversity can be obtained through several different tools—most of these solutions are based on sophisticated information coding approaches. The diversity of classical communication channels represents an extra resource from which several benefits can be extracted to improve the performance of the transmission. The diversity in traditional telecommunications can be obtained via time, frequency, space, and coding.<sup>53–55</sup> Basically, in a communication scenario, the diversity provides a useful tool to improve the rates and the reliability.

Here, we show that similar benefits can be obtained for a multicarrier CVQKD scenario. The proposed solution is called manifold extraction. We propose the manifold extraction for multicarrier CVQKD, achieving an improved transmission by utilizing those available additional degrees of freedom in the Gaussian quantum channel that are obviously not available in a single-carrier CVQKD setting. In particular, the extractable manifold provided by the additional degrees of freedom of a multicarrier CVQKD transmission also allows for the parties in a multiple-access scenario to decrease much more significantly the error probabilities than it does presently in a single-carrier scheme. Specifically, the origin of these benefits is that the additional degrees of freedom of the multicarrier CVQKD provide an exploitable resource for the legal parties.<sup>1–11</sup>

The proposed manifold extraction uses a sophisticated phase space constellation for the Gaussian subchannels which provides a natural framework to exploit the manifold patterns of the subchannel transmittance coefficients. The manifold extraction can be applied for an arbitrary distribution of the subchannel transmittance coefficients and, by exploiting some properties of the phase space constellation, it does not require the use of a statistical model. The proposed phase space constellation offers an analogous criterion to an averaging over the statistics of the subchannel transmittance coefficients. We compare the achievable performance of manifold extraction of multicarrier and single-carrier CVQKD. We determine the optimal manifold-degree of freedom ratio tradeoff curve and define its attributes in a single and multicarrier CVQKD setting. We prove that the manifold extraction in a multicarrier scenario offers significantly decreased error probabilities, and through the sophisticated allocation of the Gaussian subcarrier CVs, this benefit can be extended to all legal users of a multiple-access multicarrier CVQKD. We characterize the multidimensional manifold space of multicarrier CVQKD and define the multidimensional optimal tradeoff function in a high-dimensional manifold space. We then study the manifold extraction for multicarrier CVQKD through AMQD, and multiple-access multicarrier CVQKD through AMQD-MQA, respectively.

The novel contributions of our manuscript are as follows:

1. *We define the framework of multidimensional manifold extraction for continuous-variable quantum key distribution.*
2. *The scheme utilizes the resources that are injected into the transmission by the additional degrees of freedom.*
3. *We prove that the exploitable degree of freedom in a multicarrier CVQKD scenario significantly extends the possibilities.*
4. *It allows for the parties to reach decreased error probabilities via the extra resources of a multicarrier transmission.*
5. *We define the multidimensional manifold space and the optimal tradeoff between the available degrees of freedom.*

This paper is organized as follows. Section 2 summarizes some preliminary findings. Section 3 defines the multidimensional manifold space for CVQKD. Section 4 proposes the manifold extraction of multicarrier CVQKD and multiple-access multicarrier CVQKD. Finally, Section 5 concludes the results. Supporting Information is included in Appendix A.

## 2 | PRELIMINARIES

### 2.1 | Multicarrier CVQKD

The basic terms and notations of multicarrier CVQKD are summarized in Appendix A. The detailed description of AMQD and AMQD-MQA can be found in Gyongyosi and Imre.<sup>1,3</sup> For the secret key rate formulas, see Gyongyosi and Imre.<sup>2</sup>

### 2.1.1 | SVD-assisted multicarrier CVQKD

We briefly summarize the SVD-assisted multicarrier CVQKD scheme.<sup>7</sup> Precisely, the singular layer consists of a preunitary  $F_1$  ( $U_1$ ) (scaled FFT operation (scaled CVQFT), independent from the IFFT (inverse Fast Fourier transform) operation  $f$  ( $U_1$ )) and a post-unitary  $U_2^{-1}$  (CVQFT operation, independent from the  $U$  CVQFT<sup>†</sup> operation) that perform the pre- and post-transform.

The pre-unitary  $F_1$  ( $U_1$ ) transforms such that the input will be sent through the  $\lambda_i$  eigenchannels of the Gaussian link, whereas  $U_2^{-1}$  performs its inverse. Note that the pre- $F_1$  ( $U_1$ ) and post- $U_2^{-1}$  unitaries are the not inverse of  $F$  and  $U$  but  $F_1^{-1}$  ( $U_1^{-1}$ ) and  $U_2$ , respectively. In particular, these unitaries define the set  $S_1$  of singular operators, as follows:

$$S_1 = \{F_1, U_2^{-1}\}. \quad (1)$$

Specifically, if each transmit user sends a single-carrier Gaussian CV signal to an encoder  $\mathcal{E}$ , then the pre-operator is the unitary  $U_1$ , the CVQFT operation, whereas the unitary post-operator is achieved by the inverse CVQFT operation  $U_2^{-1}$ , defining the set  $S_2$  of singular operators as

$$S_2 = \{U_1, U_2^{-1}\}. \quad (2)$$

The subindices of the operators  $\{F_1, U_2^{-1}\}$  and  $\{U_1, U_2^{-1}\}$  are different in each  $S_i$ ,  $i=1,2$  because these operators are not the inverse of each other.

These operators are determined by the SVD of  $F(\mathbf{T})$ , which is evaluated as

$$F(\mathbf{T}) = U_2 \Gamma F_1^{-1}, \quad (3)$$

where  $F_1^{-1}$ ,  $F_1 \in \mathbb{C}^{K_{in} \times K_{in}}$  and  $U_2$ ,  $U_2^{-1} \in \mathbb{C}^{K_{out} \times K_{out}}$ ,  $K_{in}$ , and  $K_{out}$  refer to the number of sender and receiver users such that

$$K_{in} \leq K_{out}, F_1^{-1} F_1 = F_1 F_1^{-1} = I, \quad (4)$$

and

$$U_2 U_2^{-1} = U_2^{-1} U_2 = I. \quad (5)$$

The term  $\Gamma \in \mathbb{R}$  is a diagonal matrix with nonnegative real diagonal elements

$$\lambda_1 \geq \lambda_2 \geq \dots \lambda_{n_{\min}}, \quad (6)$$

which are called the eigenchannels of  $F(\mathbf{T}) = U_2 \Gamma F_1^{-1}$ , where

$$n_{\min} = \min(K_{in}, K_{out}), \quad (7)$$

which equals to the rank of  $F(\mathbf{T})$ , where

$$K_{in} \leq K_{out}, \quad (8)$$

by an initial assumption. (Note that the eigenchannels are also called the ordered singular values of  $F(\mathbf{T})$ .) In terms of the  $\lambda_i$  eigenchannels,  $F(\mathbf{T})$  can be precisely rewritten as

$$F(\mathbf{T}) = \sum_{n_{\min}} \lambda_i U_{2,i} F_{1,i}^{-1}, \quad (9)$$

where  $\lambda_i U_{2,i} F_{1,i}^{-1}$  are rank-one matrices. In fact, the  $n_{\min}$  squared eigenchannels  $\lambda_i^2$  are the eigenvalues of the matrix

$$F(\mathbf{T}) F(\mathbf{T})^\dagger = U_2 \Gamma \Gamma^T U_2^{-1}, \quad (10)$$

where  $\Gamma^T$  is the transpose of  $\Gamma$ .

### 2.1.2 | Rate formulas of multicarrier CVQKD

The complete derivation of the secret key rate formulas can be found in Gyongyosi and Imre<sup>2</sup>; here, we give a brief overview on the transmission rates of multicarrier CVQKD.

In particular, the (real domain) classical capacity of a Gaussian subchannel  $\mathcal{N}_i$  in the multicarrier setting is

$$C(\mathcal{N}_i) = \frac{1}{2} \log_2 \left( 1 + \frac{\sigma_{\omega_i}^2 |F(T_i(\mathcal{N}_i))|^2}{\sigma_{\mathcal{N}_i}^2} \right), \quad (11)$$

while in the SVD-assisted AMQD,

$$C'(\mathcal{N}_i) = \frac{1}{2} \log_2 \left( 1 + \frac{\sigma_{\omega_i}^2 |F(T_i(\mathcal{N}_i))|^2}{\sigma_{\mathcal{N}_i}^2} \right), \quad (12)$$

where  $\sigma_{\omega_i}^2 = \sigma_{\omega}^2(1 + c) > \sigma_{\omega}^2$ .

Specifically, the SNR (signal to noise ratio) of  $\mathcal{N}_i$  is expressed as

$$\text{SNR}_i = \frac{\sigma_{\omega_i}^2}{\sigma_{\mathcal{N}_i}^2}, \quad (13)$$

while the SNR of  $\mathcal{N}$  at a constant modulation variance  $\sigma_{\omega}^2$  is  $\text{SNR} = \frac{\sigma_{\omega}^2}{\sigma_{\mathcal{N}}^2}$ .

Particularly, in the SVD-assisted AMQD, it referred to as

$$\text{SNR}'_i = \frac{\sigma_{\omega_i}^2}{\sigma_{\mathcal{N}_i}^2}, \quad (14)$$

and

$$\text{SNR}' = \frac{\sigma_{\omega}^2}{\sigma_{\mathcal{N}}^2}, \quad (15)$$

respectively. From (11) and (12), the (real domain) classical information transmission rates  $R_k(\mathcal{N})$  and  $R'_k(\mathcal{N})$  of user  $U_k$  through the  $l$   $\mathcal{N}_i$  Gaussian subchannels in AMQD and SVD-assisted AMQD are precisely as follows:

$$R_k(\mathcal{N}) \leq \max_{\forall i} \mathbb{E} \left[ \sum_l \frac{1}{2} \log_2 \left( 1 + \frac{\sigma_{\omega_i}^2 |F(T_i(\mathcal{N}_i))|^2}{\sigma_{\mathcal{N}}^2} \right) \right], \quad (16)$$

and

$$R'_k(\mathcal{N}) \leq \max_{\forall i} \mathbb{E} \left[ \sum_l \frac{1}{2} \log_2 \left( 1 + \frac{\sigma_{\omega_i}^2 |F(T_i(\mathcal{N}_i))|^2}{\sigma_{\mathcal{N}}^2} \right) \right]. \quad (17)$$

Precisely, the  $\text{SNR}_i^*$  (signal to noise ratio) of the  $i$ -th Gaussian subchannel  $\mathcal{N}_i$  for the transmission of private classical information (ie, for the derivation of the secret key rate) under an optimal Gaussian attack is expressed as  $\text{SNR}_i^* = \frac{\sigma_{\omega_i}^2}{\sigma_{\mathcal{N}_i^*}^2}$ ,

and  $\text{SNR}^* = \frac{\sigma_{\omega}^2}{\sigma_{\mathcal{N}^*}^2}$ , where  $\sigma_{\mathcal{N}_i^*}^2$  is precisely evaluated as follows<sup>2</sup>:

$$\sigma_{\mathcal{N}_i^*}^2 = \sigma_{\omega_i}^2 \left( \frac{\sigma_{\omega_i}^2 |F(T_i(\mathcal{N}_i))|^2 + \sigma_{\mathcal{X}_i}^2}{1 + \sigma_{\mathcal{X}_i}^2 \sigma_{\omega_i}^2 |F(T_i(\mathcal{N}_i))|^2} - 1 \right)^{-1}, \quad (18)$$

where

$$\sigma_{X_i}^2 = \sigma_0^2 + N_i, \quad (19)$$

and where  $\sigma_0^2$  is the vacuum noise and  $N_i$  is the excess noise of the Gaussian subchannel  $\mathcal{N}_i$  defined as

$$N_i = \frac{(W_i - 1) \left( |F(T_{Eve,i})|^2 \right)}{1 - |F(T_{Eve,i})|^2}, \quad (20)$$

where  $W_i$  is the variance of Eve's EPR state used for the attacking of  $\mathcal{N}_i$ , while

$$|T_{Eve,i}|^2 = 1 - |T_i|^2 \quad (21)$$

is the transmittance of Eve's beam splitter (BS), and  $|T_i|^2$  is the transmittance of  $\mathcal{N}_i$ .

Precisely, in the SVD-assisted multicarrier CVQKD,

$$(\text{SNR}'_i)^* = \frac{\sigma_{\omega_i''}^2}{\sigma_{\mathcal{N}_i^*}^2}, \quad (22)$$

and

$$(\text{SNR}')^* = \frac{\sigma_{\omega''}^2}{\sigma_{\omega^*}^2}, \quad (23)$$

for  $\mathcal{N}_i$  and  $\mathcal{N}$ , respectively.

Particularly, from (18) the  $P(\mathcal{N}_i)$  private classical capacity (real domain) is expressed as

$$P(\mathcal{N}_i) = \frac{1}{2} \log_2 \left( 1 + \frac{\sigma_{\omega_i}^2 |F(T_i(\mathcal{N}_i))|^2}{\sigma_{\mathcal{N}_i^*}^2} \right). \quad (24)$$

The SVD-assisted  $P'(\mathcal{N}_i)$  from (22) is then yielded precisely as

$$P'(\mathcal{N}_i) = \frac{1}{2} \log_2 \left( 1 + \frac{\sigma_{\omega_i''}^2 |F(T_i(\mathcal{N}_i))|^2}{\sigma_{\mathcal{N}_i^*}^2} \right). \quad (25)$$

Assuming  $l$  Gaussian subchannels, the (real domain) secret key rate  $S(\mathcal{N})$  of AMQD and  $S'(\mathcal{N})$  of SVD-assisted AMQD are as follows:

$$S(\mathcal{N}) \leq P(\mathcal{N}) = \max_{\forall i} \mathbb{E} \left( \sum_l \log_2 \left( 1 + \frac{\sigma_{\omega_i}^2 |F(T_i(\mathcal{N}_i))|^2}{\sigma_{\mathcal{N}_i^*}^2} \right) \right), \quad (26)$$

$$S'(\mathcal{N}) \leq P'(\mathcal{N}) = \max_{\forall i} \mathbb{E} \left( \sum_l \log_2 \left( 1 + \frac{\sigma_{\omega_i''}^2 |F(T_i(\mathcal{N}_i))|^2}{\sigma_{\mathcal{N}_i^*}^2} \right) \right). \quad (27)$$

## 2.2 | Manifold extraction

In a multicarrier CVQKD scenario, the term manifold is interpreted as follows. Let the  $i$ -th component  $p_{j,i}$  of a given private random codeword  $\mathbf{p}_j = (p_{j,1}, \dots, p_{j,l})^T$  to be transmitted through  $\mathcal{N}_i$ , where each Gaussian subchannel is characterized by an independent transmittance coefficient  $|T_i(\mathcal{N}_i)|^2$ . As a first approach, the number  $l$  of the Gaussian

subchannels is identified as the manifold of  $\mathcal{N}$ . Precisely, the information is granulated into subcarriers, which are dispersed by the inverse Fourier transform, and each  $p_{j,i}$  component is identified by independent transmittance coefficients. A more detailed formula will be concluded in the further sections.

Specifically, the transmission can be utilized by a permutation phase space constellation  $\mathcal{C}_s^P(\mathcal{N})$ . Using  $P_i$ ,  $i=2,\dots,l$  random permutation operators,  $\mathcal{C}_s^P(\mathcal{N})$  can be defined for the multicarrier transmission as

$$\begin{aligned}\mathcal{C}_s^P(\mathcal{N}) &= (\mathcal{C}_s(\mathcal{N}_1), \dots, \mathcal{C}_s(\mathcal{N}_l)) \\ &= (\mathcal{C}_s(\mathcal{N}_1), P_2\mathcal{C}_s(\mathcal{N}_1), \dots, P_l\mathcal{C}_s(\mathcal{N}_1)),\end{aligned}\quad (28)$$

where  $d_{\mathcal{C}_s(\mathcal{N}_i)} = d_{\mathcal{C}_s(\mathcal{N}_j)}$  is the cardinality of  $\mathcal{C}_s(\mathcal{N}_i)$ . Using  $\mathcal{C}_s^P(\mathcal{N})$ , the available degrees of freedom in the Gaussian link can be utilized, and the random permutation operators inject correlation between the  $\mathcal{N}_i$  subchannels via  $P_i\mathcal{C}_s(\mathcal{N}_1)$ .

In particular, for each Gaussian subchannel, the distance between the phase space constellation points is evaluated by  $\delta_i$ , the normalized difference function. Assuming two  $l$ -dimensional input random private codewords  $\mathbf{p}_A = (p_{A,1}, \dots, p_{A,l})^T$  and  $\mathbf{p}_B = (p_{B,1}, \dots, p_{B,l})^T$  and two Gaussian subchannels  $\mathcal{N}_i$  and  $\mathcal{N}_j$ ,  $\delta_i$  is calculated precisely as follows:

$$\delta_i = \frac{1}{\sqrt{\frac{\sigma_{\omega''}^2}{\sigma_{\mathcal{N}''}^2}}} (p_{A,i} - p_{B,i}), \quad (29)$$

particularly, for the  $l$  Gaussian subchannels

$$|\delta_1 \dots l|^2 > \left( c \frac{1}{l2^{S'(\mathcal{N}_i)}} \right)^l, \quad (30)$$

where the term  $|\delta_1 \dots l|$  is referred to as the product distance.<sup>53-55</sup> The maximization of this term ensures the maximization of the extractable manifold, and determines the  $\tilde{p}_{err}$  pairwise worst-case error probabilities of  $\mathbf{p}_A, \mathbf{p}_B$ .

As we have shown in Section 3, by using  $\mathcal{C}_s^P(\mathcal{N})$  and (30), the  $\tilde{p}_{err}$  worst-case pairwise error probability can be decreased to the theoretical lower bound. We further reveal that in a multiuser CVQKD scenario, this condition can be extended simultaneously for all users.

Let us assume that the  $S'_k(\mathcal{N})$  secret key rate of user  $U_k$ , for  $\forall k$ , is fixed precisely as follows:

$$S'_k(\mathcal{N}) = \frac{\varsigma_k}{n_{\min}} P'(\mathcal{N}), \quad (31)$$

where  $\varsigma_k > 0$  is referred to as the degree of freedom ratio of  $U_k$ , while  $n_{\min}$  has been shown in (7). As one can immediately conclude from (31),  $S'_k(\mathcal{N}) \ll P'(\mathcal{N})$ .

Without loss of generality, for a given subchannel  $\mathcal{N}_i$ , we redefine  $S'_k(\mathcal{N}_i)$ ,  $\varsigma_{k,i} > 0$  precisely as

$$S'_k(\mathcal{N}_i) = \frac{\varsigma_{k,i}}{n_{\min}} P'(\mathcal{N}_i). \quad (32)$$

Note: From this point, we use the complex domain formulas throughout the manuscript and  $S'_k(\mathcal{N})$  and  $S'_k(\mathcal{N}_i)$  are fixed to (31) and (32).

For a given  $\mathcal{N}_i$ , an  $E_{err}$  error event<sup>53-55</sup> is identified as follows:

$$E_{err} \equiv \log_2 \left( 1 + |F(T_i(\mathcal{N}_i))|^2 (\text{SNR}'_i)^* \right) < S'(\mathcal{N}_i), \quad (33)$$

and the probability of  $E_{err}$  at a given  $S'(\mathcal{N}_i)$  is identified by the  $p_{err}$  error probability as follows:

$$E_{err} = p_{err}(S'_k(\mathcal{N}_i)) = \Pr \left( \log_2 \left( 1 + |F(T_i(\mathcal{N}_i))|^2 (\text{SNR}'_i)^* \right) < S'(\mathcal{N}_i) \right). \quad (34)$$

Particularly, by some fundamental argumentations on the statistical properties of a Gaussian random distribution,<sup>53-55</sup> for  $|F(T_i(\mathcal{N}_i))|^2 (\text{SNR}'_i)^* \rightarrow 0$ ,  $p_{err}(S'_k(\mathcal{N}_i))$  can be expressed as

$$p_{err}(S'_k(\mathcal{N}_i)) = \Pr\left(|F(T_i(\mathcal{N}_i))|^2 (\text{SNR}'_i)^* \log_2 e < S'(\mathcal{N}_i)\right), \quad (35)$$

while for  $|F(T_i(\mathcal{N}_i))|^2 (\text{SNR}'_i)^* \rightarrow \infty$ , the corresponding error probability is as

$$p_{err}(S'_k(\mathcal{N}_i)) = \Pr\left(\log_2\left(|F(T_i(\mathcal{N}_i))|^2 (\text{SNR}'_i)^*\right) < S'(\mathcal{N}_i)\right). \quad (36)$$

Let  $l=1$ , that is, let us consider a single-carrier CVQKD, with  $|F(T(\mathcal{N}))|^2$  of  $\mathcal{N}$ , with a secret key rate  $S'(\mathcal{N})$ . In this setting,  $p_{err}$  is expressed precisely as<sup>53</sup>

$$\begin{aligned} p_{err}^{single}(S'_k(\mathcal{N})) &= \Pr(\log_2(1 + |F(T(\mathcal{N}))|^2 (\text{SNR}')^*) < S'(\mathcal{N})) \\ &= \Pr\left(|F(T(\mathcal{N}))|^2 \frac{1}{(\text{SNR}')^*}\right) \\ &= \frac{1}{(\text{SNR}')^*}, \end{aligned} \quad (37)$$

by theory.

Specifically, assuming a multicarrier CVQKD scenario with  $l$  Gaussian subchannels and secret key rate  $S'(\mathcal{N}_i)$  per  $\mathcal{N}_i$ ,  $p_{err}^{AMQD}$  is derived as follows:

Without loss of generality, we construct the set  $\mathcal{T}$ , such that

$$\mathcal{T} : \min_{\forall i} \{|F(T_i(\mathcal{N}_i))|\}, \quad (38)$$

where for  $\forall i, i=1, \dots, l$  the following condition holds:

$$F(T_i(\mathcal{N}_i)) \geq \frac{1}{(\text{SNR}')^*} = . \quad (39)$$

In particular, the transmission through the Gaussian subchannels is evaluated via set  $\mathcal{T}$ , which refers to the worst-case scenario at which a  $S'(\mathcal{N}) > 0$  nonzero secret key rate is possible, by convention. Particularly, in (30), a given  $\partial_i$  identifies the minimum distance between the normalized  $2^{S'_k(\mathcal{N}_i)}$  points for the phase space constellation  $\mathcal{C}'_s(\mathcal{N}_i)$  of  $\mathcal{N}_i$ .

Precisely, by fundamental theory,<sup>53-55</sup> it can be proven that for an arbitrary distribution of the  $F(T_i(\mathcal{N}_i))$  Fourier transformed transmittance coefficient, the maximized product distance function of (30) can be derived by an averaging over the following statistic  $\mathcal{S}$ :

$$\mathcal{S} : F(T_i(\mathcal{N}_i)) \in \mathcal{CN}\left(0, \sigma_{F(T_i(\mathcal{N}_i))}^2\right), \quad (40)$$

where  $\sigma_{F(T_i(\mathcal{N}_i))}^2 = \mathbb{E}[|F(T_i(\mathcal{N}_i))|^2]$ , and  $F(T_i(\mathcal{N}_i))$  is a zero-mean, circular symmetric complex Gaussian random variable with i.i.d.  $\mathcal{N}\left(0, 0.5\sigma_{F(T_i(\mathcal{N}_i))}^2\right)$  zero-mean Gaussian random variables per quadrature components  $x_i$  and  $p_i$ , for the  $i$ -th Gaussian subcarrier CV.

As it has been shown in Gyongyosi,<sup>6</sup> the  $\delta$  manifold parameter picks up the following value in the single-carrier CVQKD setting:

$$\delta_{single} = 1, \quad (41)$$

while in the multicarrier CVQKD setting,

$$\delta_{AMQD} = l. \quad (42)$$



The result in (42) will be further sharpened in Section 3 since it significantly depends on the properties of the corresponding phase space constellation  $\mathcal{C}_s(\mathcal{N})$ . From (45), it clearly follows that the extractable manifold  $\delta$  determines the error probability of the transmission, and for higher  $\delta$ , the reliability of the transmission improves.

Particularly, in a multiple-access CVQKD scenario, there exists another degree of freedom in the channel, the number of information carriers allocated to a given user  $U$ . This type of degree of freedom is denoted by  $\varsigma$  and is referred to as the degree of freedom ratio. Without loss of generality, in the function of  $\varsigma > 0$  (41) and (42) precisely can be rewritten as

$$\delta_{\text{single}} = 1 - \varsigma, \quad (43)$$

while in the multicarrier CVQKD setting, it refers to the ratio of the subcarriers allocated to a given user,

$$\delta_{\text{AMQD}} = l(1 - \varsigma). \quad (44)$$

Thus, in a multicarrier CVQKD scenario with  $l$  Gaussian subchannels, for a given  $\varsigma > 0$ , the overall gain is  $l$ . As it can be verified, using (43) and (44), the error probabilities can be evaluated as (see also Gyongyosi<sup>6</sup>)

$$p_{\text{err}}^{\text{single}} = \frac{1}{\left((\text{SNR}')^*\right)^{\delta_{\text{single}}}} = \frac{1}{\left((\text{SNR}')^*\right)^{(1-\varsigma)}}, \quad (45)$$

$$p_{\text{err}}^{\text{AMQD}} = \frac{1}{\left((\text{SNR}')^*\right)^{\delta_{\text{AMQD}}}} = \frac{1}{\left((\text{SNR}')^*\right)^{l(1-\varsigma)}}. \quad (46)$$

The result in (46) is therefore a reduced error probability in comparison to the single-carrier CVQKD scenario (see (45)). Thus, the extra degree of freedom available in a multicarrier CVQKD setting allows us to decrease significantly the error probability. For a detailed derivation on (46), see Gyongyosi.<sup>6</sup>

In a multicarrier CVQKD protocol run, there exists an optimal tradeoff between  $\delta$  and  $\varsigma$ ; however, it requires to make some preliminary assumptions, as it is concluded in Lemma 1.

**Lemma 1.** (*Manifold extraction in multicarrier CVQKD*). For any  $S'_k(\mathcal{N}) > 0$  and  $\varsigma_k$ , where  $\varsigma_k = \frac{1}{P'(\mathcal{N})} S'_k(\mathcal{N}) n_{\min}$ ,  $\varsigma_k > 0$ , of user  $U_k, k=1, \dots, K_{\text{out}}$ , the  $\delta_k(\varsigma_k)$  extractable manifold is the ratio of  $p_{\text{err}}(S'_k(\mathcal{N}))$  error probability and the  $n_{\min}$ -normalized private classical capacity  $\frac{1}{n_{\min}} P'(\mathcal{N})$ , derived at the asymptotic limit of  $(\text{SNR}')^* \rightarrow \infty$ .

*Proof.* In particular, at a given  $\varsigma_k$  and  $S'_k(\mathcal{N})$  (see (31)), the  $\delta_k(\varsigma_k)$  manifold parameter of user  $U_k, k=1, \dots, K_{\text{out}}$  is as follows:

$$\delta_k(\varsigma_k) = \lim_{(\text{SNR}')^* \rightarrow \infty} \frac{-\log_2 p_{\text{err}}(S'_k(\mathcal{N}))}{\frac{1}{n_{\min}}} P'(\mathcal{N}), \quad (47)$$

where  $p_{\text{err}}(S'_k(\mathcal{N}))$  is the error probability of  $U_k$  at  $S'_k(\mathcal{N})$ , while  $(\text{SNR}')^*$  is the SNR of  $\mathcal{N}$  in an SVD-assisted AMQD modulation for private information transmission (see (22)).

Specifically, assuming that the condition of

$$\frac{1}{l} \sum_i |F(T_i(\mathcal{N}_i))| \sqrt{(\text{SNR}')^*} \partial_k \geq c \quad (48)$$

holds, where  $c > 0$  is a constant and  $\partial_k$  is the minimum distance of the  $2^{S'_k(\mathcal{N})}$  normalized constellation points  $|\varphi_i\rangle, |\varphi_j\rangle, j \neq i$  in a phase space constellation  $\mathcal{C}'_s(\mathcal{N})$ ,  $\mathcal{C}'_s(\mathcal{N}) \subseteq \mathcal{C}_s(\mathcal{N})$ ,  $|\mathcal{C}'_s(\mathcal{N})| = 2^{S'_k(\mathcal{N})}$ , evaluated precisely as

$$\partial_k = \frac{1}{2^{S'_k(\mathcal{N})/2}}, \quad (49)$$



then at a given secret key rate  $S'_k(\mathcal{N})$ , the  $p_{err}(S'_k(\mathcal{N}))$  error probability of the transmission of  $U_k$  decays as

$$\begin{aligned} p_{err}(S'_k(\mathcal{N})) &= Q\left(\sqrt{\frac{1}{l}\sum_l |F(T_i(\mathcal{N}_i))|^2 \frac{(\text{SNR}')^*}{2} \partial_k^2}\right) \\ &= \frac{2^{S'_k(\mathcal{N})} - 1}{(\text{SNR}')^*}, \end{aligned} \quad (50)$$

where  $Q(\cdot)$  is the Gaussian tail function. Note that the condition of (48) follows from the fact that the separation (ie,  $\partial_k$ ) of the constellation points of  $\mathcal{C}_s(\mathcal{N})$  has to be significantly larger than  $\sigma_{\mathcal{N}}$ ; otherwise, the  $Q(\cdot)$  Gaussian tail function yields in high error probabilities.<sup>53</sup> Without loss of generality, for an  $\mathcal{N}_i$  dedicated to  $U_k$  with  $S'_k(\mathcal{N}_i)$ , the phase space constellation is referred to as  $\mathcal{C}'_s(\mathcal{N}_i)$ ,  $|\mathcal{C}'_s(\mathcal{N}_i)| = 2^{S'_k(\mathcal{N}_i)}$ , and  $\partial_{k,i} = \frac{1}{2^{S'_k(\mathcal{N}_i)/2}}$ , and

$$\begin{aligned} p_{err}(S'_k(\mathcal{N}_i)) &= Q\left(\sqrt{|F(T_i(\mathcal{N}_i))|^2 \frac{(\text{SNR}'_i)^*}{2} \partial_{k,i}^2}\right) \\ &= \frac{2^{S'_k(\mathcal{N}_i)} - 1}{(\text{SNR}'_i)^*}. \end{aligned} \quad (51)$$

Exploiting the argumentation of (40) on the averaging over the  $\mathcal{S}$  statistics of the channel transmittance coefficients, and the related result in (38), the  $p_{err}(S'_k(\mathcal{N}_i))$  of a given Gaussian subchannel  $\mathcal{N}_i$  at  $S'_k(\mathcal{N}_i)$  can be determined precisely as

$$p_{err}(S'_k(\mathcal{N}_i)) = 1 - e^{-\frac{(2^{S'_k(\mathcal{N}_i)} - 1)}{(\text{SNR}'_i)^*}}, \quad (52)$$

which at  $(\text{SNR}'_i)^* \rightarrow \infty$  coincidences with (51).

Thus, using  $P_i \in \mathcal{U}$ ,  $i=2,\dots,l$  drawn from a  $\mathcal{U}$  uniform distribution, the private permutation phase space constellation  $\mathcal{C}'_s^P, \mathcal{C}'_s^P(\mathcal{N}) \subseteq \mathcal{C}'_s(\mathcal{N})$ ,  $|\mathcal{C}'_s^P(\mathcal{N})| = 2^{S'_k(\mathcal{N})}$  can be defined for the private multicarrier transmission as

$$\begin{aligned} \mathcal{C}'_s^P(\mathcal{N}) &= (\mathcal{C}'_s(\mathcal{N}_1), \dots, \mathcal{C}'_s(\mathcal{N}_l)) \\ &= (\mathcal{C}'_s(\mathcal{N}_1), P_2\mathcal{C}'_s(\mathcal{N}_1), \dots, P_l\mathcal{C}'_s(\mathcal{N}_1)), \end{aligned} \quad (53)$$

where  $d_{\mathcal{C}'_s(\mathcal{N}_i)} = d_{\mathcal{C}'_s(\mathcal{N}_j)}$  is the cardinality of  $\mathcal{C}'_s(\mathcal{N}_i)$ .

The private permutation phase space constellation of (53) can be used as a corresponding  $\mathcal{C}'_s(\mathcal{N}_i)$ , for each  $\mathcal{N}_i$  subchannels.

In particular, assuming the use of  $\mathcal{S}(F(T_i(\mathcal{N}_i)))$  in (40), the  $p_{err}(S'_k(\mathcal{N}_i))$  of a given subchannel  $\mathcal{N}_i$  with secret key rate  $S'_k(\mathcal{N}) = \frac{S_k}{n_{\min}} P'(\mathcal{N})$  can be rewritten precisely as

$$\begin{aligned} p_{err}(S'_k(\mathcal{N}_i)) &= \Pr\left(\log_2\left(1 + |F(T_i(\mathcal{N}_i))|^2 \left(\text{SNR}'_i\right)^*\right) < S'_k(\mathcal{N}_i)\right) \\ &= \Pr\left(|F(T_i(\mathcal{N}_i))|^2 < \frac{\left(\left(\text{SNR}'_i\right)^*\right)^{S_{k,i}} - 1}{\left(\text{SNR}'_i\right)^*}\right) \\ &\approx \frac{1}{\left(\left(\text{SNR}'_i\right)^*\right)^{1-S_{k,i}}} = \frac{1}{\left(\left(\text{SNR}'_i\right)^*\right)^{\delta_{k,i}(S_{k,i})}}, \end{aligned} \quad (54)$$

where  $\Pr(|F(T_i(\mathcal{N}_i))|^2 < x) \approx x$ , by theory at the distribution of (40),<sup>53-55</sup> and  $\delta_{k,i}(\varsigma_{k,i}) = 1 - \varsigma_{k,i}$ . Specifically, if  $F(T_i(\mathcal{N}_i)) \in \mathcal{CN}(0, \sigma_{F(T_i(\mathcal{N}_i))}^2)$  for all  $\mathcal{N}_i$ , then for the  $S'(\mathcal{N})$  secret key rate in the low SNR regimes the following result yields, precisely:

$$\begin{aligned} S'(\mathcal{N}) &\leq \mathbb{E} \left( \log_2 \left( 1 + \frac{\sigma_{\omega''}^2 \max_i |F(T_i(\mathcal{N}_i))|^2}{\sigma_{\mathcal{N}^*}^2} \right) \right) \\ &\approx \mathbb{E} \left( \frac{\sigma_{\omega''}^2 \max_i |F(T_i(\mathcal{N}_i))|^2}{\sigma_{\mathcal{N}^*}^2} \right) \log_2 e \approx \frac{\sigma_{\omega''}^2}{\sigma_{\mathcal{N}^*}^2} \log_2 e, \end{aligned} \quad (55)$$

while in the high SNR regimes

$$\begin{aligned} S'(\mathcal{N}) &\leq \mathbb{E} \left( \log_2 \left( \frac{\sigma_{\omega''}^2 \max_i |F(T_i(\mathcal{N}_i))|^2}{\sigma_{\mathcal{N}^*}^2} \right) \right) \\ &\approx \log_2 \frac{\sigma_{\omega''}^2}{\sigma_{\mathcal{N}^*}^2} + \mathbb{E} \left( \log_2 \left( \max_i |F(T_i(\mathcal{N}_i))|^2 \right) \right), \end{aligned} \quad (56)$$

and from the law of large numbers<sup>53</sup>:

$$\frac{1}{l} \left( \sum_l \log_2 \left( 1 + \frac{\sigma_{\omega''}^2 |F(T_i(\mathcal{N}_i))|^2}{\sigma_{\mathcal{N}_i^*}^2} \right) \right) = \mathbb{E} \left( \log_2 \left( 1 + \frac{\sigma_{\omega''}^2 \max_i |F(T_i(\mathcal{N}_i))|^2}{\sigma_{\mathcal{N}^*}^2} \right) \right). \quad (57)$$

At  $F(T_i(\mathcal{N}_i)) \in \mathcal{CN}(0, \sigma_{F(T_i(\mathcal{N}_i))}^2)$ , the density of (52) is depicted in Figure 1.

Note that for the transmission of classical (ie, nonprivate) information,  $\mathcal{C}_s$  has a cardinality of  $|\mathcal{C}_s| = 2^{R'_k}$  at a given  $R'_k(\mathcal{N})$ , with a corresponding SNR' and  $\partial_k = \frac{1}{2^{R'_k(\mathcal{N})/2}}$ .

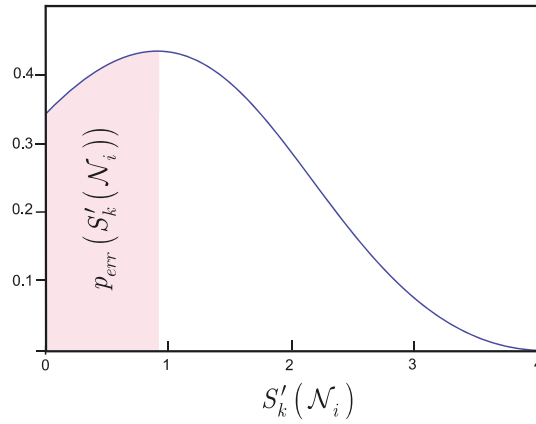
An error event  $E_{err}$  of (33) for a subchannel  $\mathcal{N}_i$  can be rewritten as

$$E_{err} \cdot \frac{1}{l} \sum_l |F(T_i(\mathcal{N}_i))|^2 < \frac{2^{S'_k(\mathcal{N})} - 1}{(\text{SNR}')^*}; \quad (58)$$

thus, introducing  $Z > 1$  which brings up by the use of a corresponding  $\mathcal{C}_s$ , a typical error probability is precisely expressed as follows:

$$\begin{aligned} p_{err}(S'_k(\mathcal{N}_i)) &= \Pr \left( \frac{1}{l} \sum_l \log_2 \left( 1 + |F(T_i(\mathcal{N}_i))|^2 (\text{SNR}'_i)^* \right) < S'_k(\mathcal{N}_i) \right) \\ &= \Pr \left( \frac{1}{l} \sum_l \log_2 \left( 1 + |F(T_i(\mathcal{N}_i))|^2 (\text{SNR}'_i)^* \right) < \frac{\varsigma_{k,i}}{n_{\min}} P'(\mathcal{N}_i) \right) \\ &= \Pr \left( \frac{1}{l} \sum_l |F(T_i(\mathcal{N}_i))|^2 < \frac{((\text{SNR}')^*)^{\varsigma_k} - 1}{(\text{SNR}')^*} \right) \\ &= \frac{1}{((\text{SNR}')^*)^{1-\varsigma_k}} = \frac{1}{((\text{SNR}')^*)^{Z(1-\varsigma_k)}} \\ &= \left( \frac{((\text{SNR}')^*)^{\varsigma_k} - 1}{(\text{SNR}')^*} \right)^Z, \end{aligned} \quad (59)$$

where  $\Pr(|F(T_i(\mathcal{N}_i))|^2 < x) \approx x^Z$  as  $\left( \frac{((\text{SNR}')^*)^{\varsigma_k} - 1}{(\text{SNR}')^*} \right) \rightarrow 0$ , by theory. (Note that in (59), the  $T_i$  transmittance coefficients are arbitrarily distributed, in contrast to (54)). As one immediately can conclude,



**FIGURE 1** At the distribution of the  $S$  statistics of (40), the shaded area under the curve gives the  $p_{err}$  error probability at a given  $S'_k(\mathcal{N}_i)$  for a Gaussian subchannel  $\mathcal{N}_i$

the phase space constellation  $\mathcal{C}_s$  provides a further decreased  $p_{err}$  in comparison to (46). Putting the pieces together, the optimal manifold-degree of freedom ratio tradeoff curve<sup>53</sup>  $f$  for a single-carrier scheme (eg, if  $l=1$  we trivially have a single-carrier scheme) can be expressed as

$$f(\mathcal{N}_i): \delta_k(\zeta_k) = Z(1 - \zeta_k), \quad (60)$$

where  $0 < \zeta_k \leq 1$ .

Specifically, some calculations then straightforwardly reveal that any phase space constellation  $\mathcal{C}_s(\mathcal{N})$  that satisfies the condition of

$$\partial_k^2 = q \frac{1}{2^{S_k(\mathcal{N})}} \quad (61)$$

achieves the optimal  $f$  tradeoff curve, for any constant  $q > 0$ . The recently proposed permutation phase space constellation  $\mathcal{C}_s^p(\mathcal{N})$  for SVD-assisted AMQD provably satisfies this condition.

Without loss of generality, assuming a constant  $g > 0$ ,  $p_{err}$  can be rewritten precisely as

$$\begin{aligned} p_{err}^g(S'_k(\mathcal{N}_i)) &: \Pr\left(\frac{1}{l} \sum_l \log_2 \left(1 + |F(T_i(\mathcal{N}_i))|^2 \left((\text{SNR}'_i)^*\right)^{1-g}\right) < S'_k(\mathcal{N}_i)\right) \\ &= \Pr\left(\frac{1}{l} \sum_l |F(T_i(\mathcal{N}_i))|^2 < \frac{\left(\left((\text{SNR}'_i)^*\right)^{1-g}\right)^{S_k} - 1}{\left((\text{SNR}'_i)^*\right)^{1-g}}\right) \\ &= \frac{\left(\left((\text{SNR}'_i)^*\right)^{S_k(1-g)} - 1\right)}{\left((\text{SNR}'_i)^*\right)^{1-g}}. \end{aligned} \quad (62)$$

Thus, for  $E_{err}^g$ , the manifold parameter is  $\delta_k^g(\zeta_k)$  as

$$\delta_k^g(\zeta_k) = \delta_k(\zeta_k) \cdot (1 - g) \geq \lim_{(\text{SNR}')^* \rightarrow \infty} \frac{-\log_2 p_{err}(S'_k(\mathcal{N}))}{\frac{1}{n_{\min}}} P'(\mathcal{N}). \quad (63)$$

In Section 3, we give a proof on the multicarrier CVQKD scenario and show that there exists an optimal tradeoff between  $\zeta_k$  and  $\delta_k$  for any  $U_k$ . We further reveal that in a multicarrier setting, the manifold extraction significantly exceeds the possibilities of a single-carrier CVQKD scenario.

### 3 | MULTIDIMENSIONAL MANIFOLD SPACE

**Theorem 1.** (Multidimensional manifold space for multicarrier CVQKD). For any  $K_{in}, K_{out}$  and  $\varsigma_k > 0$ , the  $\mathcal{M}$  manifold is a  $\dim(\mathcal{M}) = K_{in}\varsigma_k + (K_{out} - \varsigma_k)\varsigma_k$  dimensional space. The number  $N_{\dim^\perp}$  of dimensions orthogonal to  $\mathcal{M}$  in the  $\dim(S(F(\mathbf{T}(\mathcal{N})))) = K_{in}K_{out}$  dimensional space  $S(F(\mathbf{T}(\mathcal{N})))$  is  $N_{\dim^\perp} = K_{in}K_{out} - (K_{in}\varsigma_k + (K_{out} - \varsigma_k)\varsigma_k) = (K_{in} - \varsigma_k)(K_{out} - \varsigma_k)$ , with  $p_{err}(\varsigma_k) = \frac{1}{((\text{SNR}')^*)^{N_{\dim^\perp}}}$ , and optimal tradeoff curve  $h(\mathcal{M}) : \delta_k(\varsigma_k) = N_{\dim^\perp}$ .

*Proof.* The proof assumes a  $K_{in}, K_{out}$  multiuser scenario. First we express  $p_{err}$  as follows:

$$p_{err} = \Pr\left(E_{err} = \sum_{i=1}^{n_{\min}} \log_2\left(1 + \frac{(\text{SNR}')^*}{K_{in}} \lambda_i^2\right) < \frac{\varsigma_k(r + K_{in} - 1)}{r} P'(\mathcal{N})\right), \quad (64)$$

where  $\lambda_i^2$  are the squared random singular values of  $F(\mathbf{T}(\mathcal{N}))$ .<sup>53-55</sup>

Assuming  $\varsigma_k > 0$ , the  $\lambda_i$  singular values can be decomposed into subsets  $s_0$  and  $s_1$  such that set

$$s_0 = \{\lambda_1, \dots, \lambda_{\varsigma_k}\} \quad (65)$$

contains the largest  $\varsigma_k$  singular values of  $F(\mathbf{T}(\mathcal{N}))$ ,  $\lambda_i < \lambda_{i+1}$ ,  $i=1, \dots, \varsigma_k$ , and where

$$\max_{\forall i} \{\lambda_1, \dots, \lambda_{\varsigma_k}\} \leq 1. \quad (66)$$

The remaining  $n_{\min} - \varsigma_k$  singular values formulate the subset  $s_1$ , as

$$s_1 = \{\lambda_{\varsigma_k+1}, \dots, \lambda_{n_{\min}}\}, \quad (67)$$

where

$$\max_{\forall i} \{\lambda_{\varsigma_k+1}, \dots, \lambda_{n_{\min}}\} \leq \frac{1}{(\text{SNR}')^*}. \quad (68)$$

In particular, from (65) and (67), for the rank of  $F(\mathbf{T}(\mathcal{N}))$ , the following relation identifies an error event  $E_{err}$ :

$$E_{err} : \text{rank}(F(\mathbf{T}(\mathcal{N}))) \leq \varsigma_k. \quad (69)$$

Thus, the  $p_{err}$  at a given  $\varsigma_k$  is precisely referred to as

$$p_{err}(\varsigma_k) = \Pr(\text{rank}(F(\mathbf{T}(\mathcal{N}))) \leq \varsigma_k). \quad (70)$$

Specifically, at  $\varsigma_k=0$ ,  $p_{err}(\varsigma_k)$  is evaluated as

$$\begin{aligned} p_{err}(\varsigma_k = 0) &= \Pr\left(F(\mathbf{T}(\mathcal{N})) : \max_{\forall i} \{\lambda_1, \dots, \lambda_{n_{\min}}\} \leq \frac{1}{(\text{SNR}')^*}\right) \\ &= \frac{1}{((\text{SNR}')^*)^{K_{in}K_{out}}}. \end{aligned} \quad (71)$$

At  $\varsigma_k \rightarrow 0$ , in (64) the corresponding relation is

$$\lambda_i \leq \frac{1}{(\text{SNR}')^*}, \quad (72)$$

thus for the sum of the  $n_{\min}$  squared eigenvalues  $\lambda_i$ ,

$$\sum_{i=1}^{n_{\min}} \lambda_i^2 = \sum_k |F(T(\mathcal{N}_{U_k}))|^2, \quad (73)$$

where  $\mathcal{N}_{U_k}$  refers to the logical channel of  $U_k$ , which consists of the allocated Gaussian subcarriers of that user.

As follows, (72) holds if only

$$|F(T(\mathcal{N}_{U_k}))|^2 \leq \frac{1}{(\text{SNR}')^*}, \quad (74)$$

thus,

$$\begin{aligned} p_{err}(\zeta_k \rightarrow 0) &= \Pr\left(|F(T(\mathcal{N}_{U_k}))|^2 < \frac{1}{(\text{SNR}')^*}\right) \\ &\approx \frac{1}{\left((\text{SNR}')^*\right)^{K_{in}K_{out}}} \\ &= \frac{1}{\left((\text{SNR}')^*\right)^{\dim(F(\mathbf{T}(\mathcal{N})))}}, \end{aligned} \quad (75)$$

since the dimension of the space  $S(F(\mathbf{T}(\mathcal{N})))$  for a  $K_{in}$ ,  $K_{out}$  multiple-access scenario is as follows<sup>53</sup>:

$$\dim(S(F(\mathbf{T}(\mathcal{N})))) = K_{in}K_{out}. \quad (76)$$

Particularly, the  $\mathcal{M}$  manifold space can be represented as a rank- $\zeta_k$  matrix  $M$  (see later (78)); thus, it precisely has a dimension of

$$\dim(\mathcal{M}) = K_{in}\zeta_k + (K_{out} - \zeta_k)\zeta_k. \quad (77)$$

Specifically, for any  $\zeta_k > 0$ ,

$$\begin{aligned} p_{err}(\zeta_k > 0) &= \Pr(\text{rank}(F(\mathbf{T}(\mathcal{N}))) \leq \text{rank}(M) = \zeta_k) \\ &= \frac{1}{\left((\text{SNR}')^*\right)^{N_{\dim^\perp}}}, \end{aligned} \quad (78)$$

where  $N_{\dim^\perp}$  refers to the  $\dim^\perp$  dimensions orthogonal to  $\mathcal{M}$  in the  $\dim(S(F(\mathbf{T}(\mathcal{N})))) = K_{in}K_{out}$  dimensional space  $S$  of  $F(\mathbf{T}(\mathcal{N}))$ , and  $M$  is a matrix with rank  $\zeta_k$ .

Thus, for  $\zeta_k > 0$ ,  $p_{err}(\zeta_k)$  is related to as the difference between matrix  $F(\mathbf{T}(\mathcal{N}))$  and a rank- $\zeta_k$  matrix  $M$ , since  $F(\mathbf{T}(\mathcal{N}))$  is a  $K_{in} \times K_{out}$  matrix with rank  $= \zeta_k$ ; that is, it has  $\zeta_k > 0$  linearly independent row vectors from the  $K_{out}$  rows.<sup>53-55</sup> Without loss of generality,  $M$  can be characterized by  $K_{in}\zeta_k + (K_{out} - \zeta_k)\zeta_k$  parameters by theory, from which (77) straightforwardly follows.

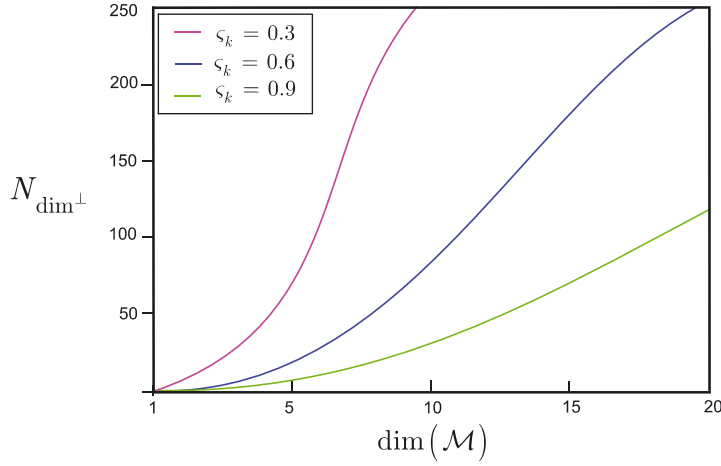
Putting the pieces together, the  $N_{\dim^\perp}$  number of  $\dim^\perp$  dimensions orthogonal to manifold space  $\mathcal{M}$  in the  $\dim(S(F(\mathbf{T}(\mathcal{N}))))$  dimensional space of  $F(\mathbf{T}(\mathcal{N}))$  is precisely

$$\begin{aligned} N_{\dim^\perp} &= K_{in}K_{out} - \dim(\mathcal{M}) \\ &= K_{in}K_{out} - (K_{in}\zeta_k + (K_{out} - \zeta_k)\zeta_k) \\ &= (K_{in} - \zeta_k)(K_{out} - \zeta_k). \end{aligned} \quad (79)$$

Particularly, from (78), the multidimensional optimal tradeoff function is yielded as

$$h(\mathcal{M}) : \delta(\zeta_k) = N_{\dim^\perp}. \quad (80)$$

The  $N_{\dim^\perp}$  in function of  $\dim(\mathcal{M})$ , at  $K_{in}=K_{out}-1$ ,  $\zeta_k=0,3;0.6;0.9$  is depicted in Figure 2.



**FIGURE 2** The values of  $N_{\dim^\perp}$  in function of  $\dim(\mathcal{M})$ , at  $K_{in}=K_{out}-1$ ,  $\varsigma_k=0.3,0.6,0.9$

#### 4 | MANIFOLD EXTRACTION FOR MULTICARRIER CVQKD

**Theorem 2.** (Manifold extraction for multicarrier CVQKD). For user  $U_k$ , the manifold extraction at  $l$  Gaussian subchannels leads to an optimal  $h$  tradeoff curve  $h: \delta_k(\varsigma_k) = lZ(1 - \varsigma_k) = lf$ , for any multicarrier scheme, where  $f$  is the optimal tradeoff curve of a single-carrier CVQKD protocol,  $f: \delta_k(\varsigma_k) = Z(1 - \varsigma_k)$ , and  $Z > 1$ .

*Proof.* In the first part of the proof, we assume the case  $l=1$ , which is analogous to a single-carrier transmission. In the second part of the proof, we study the multicarrier case for  $l$  Gaussian subchannels and reveal that a multicarrier case allows significantly improved manifold extraction.

In the single-carrier scenario, the phase space constellation  $\mathcal{C}'_s(\mathcal{N})$ ,  $\mathcal{C}'_s(\mathcal{N}) \subseteq \mathcal{C}_s(\mathcal{N})$ ,  $|\mathcal{C}'_s(\mathcal{N})| = 2^{S'_k(\mathcal{N})}$ , leads to  $\partial_k = \frac{1}{2^{S'_k(\mathcal{N})/2}}$ ,  $p_{err}(S'_k(\mathcal{N})) = \frac{2^{S'_k(\mathcal{N})} - 1}{(\text{SNR}')^*}$ , and  $f: \delta_k(\varsigma_k) = Z(1 - \varsigma_k)$ , as it has been already shown in the proof of Lemma 1. This is precisely the situation for  $l=1$ .

Specifically, for the multicarrier CVQKD case, let us assume that there are  $l$  Gaussian subchannels dedicated to the transmission of the  $d_i$ ,  $i=1, \dots, l$  Gaussian subcarriers, with  $(\text{SNR}'_i)^* = \frac{\sigma_{\omega_i}^2}{\sigma_{\mathcal{N}_i}^2}$  per  $\mathcal{N}_i$ , and secret key rate  $S'_k(\mathcal{N}_i)$  as

$$S'_k(\mathcal{N}_i) = \frac{S_{k,i}}{n_{\min}} P'(\mathcal{N}_i). \quad (81)$$

Without loss of generality, for the total constraint of SVD-assisted AMQD, one has precisely

$$\sum_{i=1}^l \log_2 \left( 1 + |F(T_i(\mathcal{N}_i))|^2 (\text{SNR}'_i)^* \right) \geq l S'_k(\mathcal{N}_i). \quad (82)$$

In particular, by further exploiting the results of SVD-assisted AMQD and following the derivations,<sup>2</sup> here, we determine the private random codeword difference for two  $l$ -dimensional input codewords

$\mathbf{p}_A = (p_{A,1}, \dots, p_{A,l})^T$  and  $\mathbf{p}_B = (p_{B,1}, \dots, p_{B,l})^T$ . The probability that  $\mathbf{p}_A$  is distorted onto  $\mathbf{p}_B$  conditioned on  $F(\mathbf{T}(\mathcal{N}))$  is evaluated precisely as follows:

$$\Pr(\mathbf{p}_A \rightarrow \mathbf{p}_B | F(\mathbf{T}(\mathcal{N}))) = Q \left( \sqrt{\frac{\sigma_{\omega_i}^2}{2\sigma_{\mathcal{N}_i}^2} \sum_l |F(T_i(\mathcal{N}_i))|^2 |\partial_i|^2} \right), \quad (83)$$

where  $\partial_i$  is the normalized difference of  $p_{A,i}$  and  $p_{B,i}$ , calculated as follows:

$$\partial_i = \frac{1}{\sqrt{\frac{\sigma_{\omega''}^2}{\sigma_{\mathcal{N}^*}^2}}} (p_{A,i} - p_{B,i}). \quad (84)$$

Assuming the case that in (83), the condition

$$\frac{\sigma_{\omega''}^2}{2\sigma_{\mathcal{N}^*}^2} \sum_l |F(T_i(\mathcal{N}_i))|^2 |\partial_i|^2 < 1 \quad (85)$$

holds, one obtains

$$|\partial_1 \dots \partial_l|^2 > c^l \frac{1}{l! 2^{S'_k(\mathcal{N}_i)l}}, \quad (86)$$

for any constant  $c > 0$  and for an arbitrary pair of  $\mathbf{p}_A$  and  $\mathbf{p}_B$ .

In particular, at a secret key rate  $S'_k$  per  $\mathcal{N}_i$ , the cardinality of  $\mathcal{C}'_s(\mathcal{N}_i)$  is as follows:

$$|\mathcal{C}'_s(\mathcal{N}_i)| = 2^{S'_k(\mathcal{N}_i)}. \quad (87)$$

Thus, in the private transmission each  $\mathcal{C}'_s(\mathcal{N}_i)$  is precisely defined with  $2^{S'_k(\mathcal{N}_i)}$  CV states  $|\phi_i$  for each  $\mathcal{N}_i$ , at an averaged  $\tilde{S}_k(\mathcal{N}_i)$  as

$$|\mathcal{C}'_s(\mathcal{N})| = 2^{\sum_l S'_k(\mathcal{N}_i)} \approx 2^{l\tilde{S}_k(\mathcal{N}_i)}. \quad (88)$$

Specifically, evaluating the  $Q(\cdot)$  Gaussian tail function at

$$\min_{\forall F(T_i(\mathcal{N}_i))} |F(T_i(\mathcal{N}_i))|^2 = \min_{\forall i} \frac{1}{\frac{\sigma_{\omega''}^2}{\sigma_{\mathcal{N}^*}^2}} \left( v_{Eve} \frac{1}{|\partial_i|^2} - 1 \right), \quad (89)$$

where  $v_{Eve}$  is Eve's corresponding security parameter in an optimal Gaussian attack.

The result in (89) leads to a worst-case scenario precisely as

$$\tilde{p}_{err} = \Pr(\mathbf{p}_A \rightarrow \mathbf{p}_B | F(\mathbf{T}(\mathcal{N}))) = Q \left( \sqrt{\min_{\forall F(T_i(\mathcal{N}_i))} \frac{\frac{2}{\sigma_{\omega''}^2}}{2 \frac{\sigma_{\omega''}^2}{\sigma_{\mathcal{N}^*}^2}} \sum_l |F(T_i(\mathcal{N}_i))|^2 |\partial_i|^2} \right), \quad (90)$$

such that for the  $l$   $\mathcal{N}_i$  Gaussian subchannels, the following constraint is satisfied:

$$\log_2 \left( 1 + \frac{\sigma_{\omega''}^2 |F(T(\mathcal{N}))|^2}{\sigma_{\mathcal{N}^*}^2} \right) = \sum_l \log_2 \left( 1 + \frac{\sigma_{\omega''}^2 |F(T_i(\mathcal{N}_i))|^2}{\sigma_{\mathcal{N}^*}^2} \right) \geq l\tilde{S}_k(\mathcal{N}_i). \quad (91)$$

In particular, the optimal manifold extraction  $\delta_k(\zeta_k)$  requires the maximization of the product distance  $|\partial_1 \dots \partial_l|^{2/l}$  at (90); thus, without loss of generality, the optimizing condition at  $l$  Gaussian subchannels is a maximization as follows:

$$\delta_k(\zeta_k) : \max_{\forall i} |\partial_1 \dots \partial_l|^{2/l} > c \frac{1}{l 2^{S'_k(\mathcal{N}_i)}}. \quad (92)$$

Since for  $\mathcal{C}_s^p(\mathcal{N}_i)$  this condition is satisfied, by using the  $\mathcal{C}_s^p(\mathcal{N}_i)$  random permutation operators as  $\mathcal{C}_s(\mathcal{N}_i)$  for the Gaussian subchannels, the optimality of  $\delta_k(\zeta_k)$  can be satisfied. Using (84), the constraint of (91) can be rewritten as follows:



$$\sum_l \log_2 \left( 1 + \frac{\tilde{Q}_i(\mathcal{N}_i)}{|\partial_i|^2} \right) \geq l \tilde{S}'_k(\mathcal{N}_i), \quad (93)$$

where

$$\tilde{Q}_i(\mathcal{N}_i) = \frac{|F(T_i(\mathcal{N}_i))|^2 |\partial_i|^2 \sigma_{\omega''}^2}{\sigma_{\mathcal{N}^*}^2}, \quad (94)$$

and

$$\min_{\forall \tilde{Q}_i \geq 0} \frac{1}{2} \sum_l \tilde{Q}_i = \min_{\forall F(T_i(\mathcal{N}_i))} \frac{\sigma_{\omega''}^2}{2\sigma_{\mathcal{N}^*}^2} \sum_l |F(T_i(\mathcal{N}_i))|^2 |\partial_i|^2, \quad (95)$$

where

$$\min_{\forall F(T_i(\mathcal{N}_i))} \sum_l |F(T_i(\mathcal{N}_i))|^2 = \sum_l \frac{1}{\sqrt{\frac{\sigma_{\omega''}^2}{\sigma_{\mathcal{N}^*}^2}}} \left( v_{Eve} \frac{1}{|\partial_i|^2} - 1 \right). \quad (96)$$

Without loss of generality, from (95) and (96), the Gaussian tail function in (90) can be precisely rewritten as follows:

$$Q \left( \sqrt{\frac{1}{2} \sum_l (v_{Eve} - |\partial_i|^2)} \right), \quad (97)$$

and

$$\sum_l \log_2 \left( v_{Eve} \frac{1}{|\partial_i|^2} \right) = \sum_l \log_2 \left( 1 + \frac{\tilde{Q}_i(\mathcal{N}_i)}{|\partial_i|^2} \right) = l \tilde{S}'_k(\mathcal{N}_i). \quad (98)$$

Particularly, from these derivations, the manifold extraction for the multicarrier scenario is yielded as follows. The  $E_{err}$  error event can be rewritten as

$$E_{err}: \sum_{i=1}^l \log_2 \left( 1 + |F(T_i(\mathcal{N}_i))|^2 (\text{SNR}'_i)^* \right) < l \tilde{S}'_k(\mathcal{N}_i); \quad (99)$$

thus, for  $p_{err}(\tilde{S}'_k(\mathcal{N}))$ ,

$$\begin{aligned} p_{err}(\tilde{S}'_k(\mathcal{N})) &= \Pr \left( \sum_{i=1}^l \log_2 \left( 1 + |F(T_i(\mathcal{N}_i))|^2 (\text{SNR}'_i)^* \right) < l \tilde{S}'_k(\mathcal{N}_i) \right) \\ &= \Pr \left( \sum_{i=1}^l \log_2 \left( 1 + |F(T_i(\mathcal{N}_i))|^2 (\text{SNR}'_i)^* \right) < \frac{l \tilde{S}_{k,i}}{n_{\min}} P'(\mathcal{N}_i) \right). \end{aligned} \quad (100)$$

Specifically, it can be further evaluated as

$$\begin{aligned} p_{err}(\tilde{S}'_k(\mathcal{N})) &= \left( \Pr \left( \log_2 \left( 1 + |F(T_i(\mathcal{N}_i))|^2 (\text{SNR}'_i)^* \right) < \frac{\tilde{S}_{k,i}}{n_{\min}} P'(\mathcal{N}_i) \right) \right)^l \\ &= \left( \Pr \left( |F(T_i(\mathcal{N}_i))|^2 < \frac{((\text{SNR}'_i)^*)^{\tilde{S}_{k,i}} - 1}{(\text{SNR}'_i)^*} \right) \right)^l \\ &= \frac{1}{((\text{SNR}')^*)^{l(1-\tilde{S}_{k,i})}} = \left( \frac{((\text{SNR}'_i)^*)^{\tilde{S}_{k,i}} - 1}{(\text{SNR}'_i)^*} \right)^{l\tilde{S}_{k,i}}, \end{aligned} \quad (101)$$

and at  $\varsigma_{k,i}$ , the optimal manifold extraction for each  $\mathcal{N}_i$  is

$$\delta_{k,i}(\varsigma_{k,i}) = Z(1 - \varsigma_{k,i}) = Z(1 - \varsigma_k). \quad (102)$$

Thus, without loss of generality,

$$p_{err} = \frac{1}{\left((\text{SNR}')^*\right)^{lZ(1-\varsigma_k)}}. \quad (103)$$

As follows, from (103), the manifold extraction for the  $l$  Gaussian subchannels, and the optimal manifold-degree of freedom ratio tradeoff curve  $h^{53-55}$  for the multicarrier transmission, is precisely expressed as

$$h: \delta_k(\varsigma_k) = lZ(1 - \varsigma_k) = lf, \quad (104)$$

where  $0 \leq \varsigma_k$ .

The single-carrier and multicarrier tradeoff curves  $f$  and  $h$  are compared in Figure 3.

To conclude the results, the multicarrier CVQKD with  $l$  Gaussian subchannels provides an  $l$ -fold manifold gain over the single-carrier CVQKD protocols, for all  $\varsigma_k$ .

#### 4.1 | Manifold extraction for AMQD-MQA

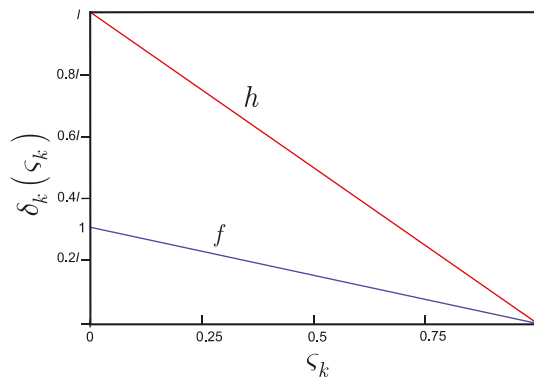
**Theorem 3.** (Manifold extraction in a multiple-access multicarrier CVQKD). For any  $K_{\text{in}}, K_{\text{out}}$  multiple-access multicarrier CVQKD scenario, the manifold extraction is maximized via  $\delta_k(\varsigma_k): \max_{\forall i} |\lambda_1 \dots \lambda_{n_{\min}}|^{2/n_{\min}}$ , where  $\lambda_i$  is the  $i$ -th smallest singular value of matrix  $\mathbf{M}_j = \frac{1}{\sqrt{(\text{SNR}')^*}}(\mathbf{p}_A - \mathbf{p}_B)$ , and  $\mathbf{p}_A, \mathbf{p}_B$  are 1-dimensional random private codewords.

*Proof.* Let us assume that  $\mathbf{p}_A, \mathbf{p}_B$  are  $l$ -dimensional inputs,  $\mathbf{p}_A = (p_{A,1}, \dots, p_{A,l})^T$  and  $\mathbf{p}_B = (p_{B,1}, \dots, p_{B,l})^T$ . The  $\Pr(\mathbf{p}_A \rightarrow \mathbf{p}_B | F(\mathbf{T}(\mathcal{N})))$  pairwise error probability can be evaluated as

$$\Pr(\mathbf{p}_A \rightarrow \mathbf{p}_B | F(\mathbf{T}(\mathcal{N}))) = \max_{\forall \eta} Q\left(\frac{F(\mathbf{T}(\mathcal{N})) \cdot (\mathbf{p}_A - \mathbf{p}_B)}{\sqrt{2}}\right), \quad (105)$$

where  $\eta$  is expressed as

$$\eta = F(\mathbf{T}(\mathcal{N})) : |F(\mathbf{T}(\mathcal{N}))|^2 > \frac{K_{\text{in}}(2^{S_k(\mathcal{N})} - 1)}{(\text{SNR}')^*}. \quad (106)$$



**FIGURE 3** Comparison of the optimal manifold-degree of freedom ratio tradeoff curves  $f$  and  $h$  for single-carrier and multicarrier CVQKD for a user  $U_k$

Without loss of generality, let  $\tilde{\lambda}$  be the smallest eigenvalue of  $\mathbf{M}_j$ ,

$$\tilde{\lambda} = \min_{\forall i}(\lambda_i), \quad (107)$$

where  $\mathbf{M}_j$  stands for the private codeword difference matrix,

$$\mathbf{M}_j = \frac{1}{\sqrt{(\text{SNR}')^*}}(\mathbf{p}_A - \mathbf{p}_B). \quad (108)$$

In particular, using (107) and (105) can be written precisely as

$$\Pr(\mathbf{p}_A \rightarrow \mathbf{p}_B | F(\mathbf{T}(\mathcal{N}))) = Q\left(\frac{1}{2}\tilde{\lambda}^2 K_{in} (2^{S'_k(\mathcal{N})} - 1)\right). \quad (109)$$

Precisely, the result of (109) follows from the fact that for a  $K_{in} \times K_{out}$  matrix  $\mathbf{M}_j$ , the following relation holds for  $\mathbf{M}_j$  and its smallest eigenvalue  $\tilde{\lambda}$ , by theory:

$$\tilde{\lambda}^2 = \min_{\forall |F(\mathbf{T}(\mathcal{N}))|} F(\mathbf{T}(\mathcal{N}))^\dagger \mathbf{M}_j \mathbf{M}_j^\dagger F(\mathbf{T}(\mathcal{N})). \quad (110)$$

Some calculations then straightforwardly reveal that for  $Q\left(\frac{1}{2}\tilde{\lambda}^2 K_{in} (2^{S'_k(\mathcal{N})} - 1)\right) > 1$ , the condition on  $\tilde{\lambda}$  is as follows:

$$\tilde{\lambda}^2 > \frac{1}{K_{in} (2^{S'_k(\mathcal{N})} - 1)} \simeq \frac{1}{K_{in} 2^{S'_k(\mathcal{N})}}. \quad (111)$$

Introducing a covariance matrix  $\mathbf{K}_o$  as

$$\mathbf{K}_o = (\text{SNR}')^* \frac{I_{K_{in}}}{K_{in}}, \quad (112)$$

where  $I_{K_{in}}$  is the  $K_{in} \times K_{in}$  identity matrix,  $E_{err}$  can be rewritten as

$$E_{err} = \log_2 \det \left( I_{K_{out}} + F(\mathbf{T}(\mathcal{N})) \mathbf{K}_o F(\mathbf{T}(\mathcal{N}))^\dagger \right) < S'(\mathcal{N}), \quad (113)$$

where without loss of generality,

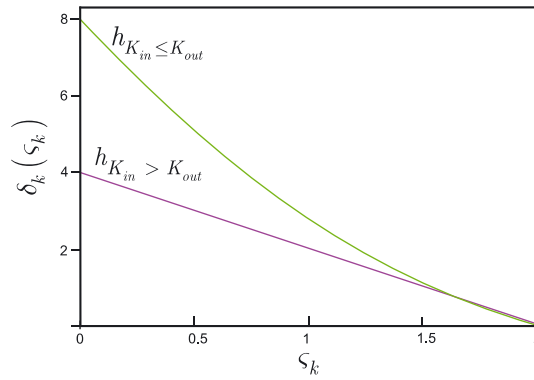
$$S'(\mathcal{N}) \leq P'(\mathcal{N}) = \max_{\forall i} \mathbb{E} \left( \sum_l \log_2 \left( 1 + \frac{\sigma_{\omega_i}^2 |F(T_i(\mathcal{N}_i))|^2}{\sigma_{\mathcal{N}_i}^2} \right) \right). \quad (114)$$

Let the SNIR (signal-to noise plus interference ratio) of  $\mathcal{N}_i$  be  $(\text{SNIR}'_i)^*$  in an SVD-assisted AMQD setting, then  $E_{err}$  can be rewritten precisely as

$$\begin{aligned} E_{err} &= \log_2 \det \left( I_{K_{out}} + F(\mathbf{T}(\mathcal{N})) \frac{(\text{SNR}')^*}{K_{in}} F(\mathbf{T}(\mathcal{N}))^\dagger \right) \\ &= \sum_{i=1}^{K_{in}} \left( 1 + (\text{SNIR}'_i)^* \right) < S'(\mathcal{N}). \end{aligned} \quad (115)$$

Then, let us assume that  $r$  subchannels are interfering with each other in the SVD-assisted multicarrier transmission. Specifically, at  $r$  interfering subchannels, after some calculations, it can be verified that the  $S'_k(\mathcal{N})$  secret key rate reduces to precisely

$$S'_k(\mathcal{N}) = r S'_k(\mathcal{N}) \frac{1}{(r + K_{in} - 1)}. \quad (116)$$



**FIGURE 4** The optimal tradeoff curves  $h_{K_{in} > K_{out}}$  for any  $K_{in} > K_{out}$ , and  $h_{K_{in} \leq K_{out}}$  at  $K_{in}=2, K_{out}=4$ . The  $h_{K_{in} > K_{out}}$  curve is maximized in  $\delta_k(\varsigma_k) = 4$  at  $\varsigma_k=0$ , and picks up the minimum  $\delta_k(\varsigma_k) = 0$  at  $\varsigma_k=2$ , for any  $K_{in} > K_{out}$ . For any  $K_{in} \leq K_{out}$ , the  $h_{K_{in} \leq K_{out}}$  curve has the max. in  $\delta_k(\varsigma_k) = K_{in}K_{out}$ ,  $\varsigma_k=0$ , and the min.  $\delta_k(\varsigma_k) = 0$  at  $\varsigma_k = \min(K_{in}, K_{out})$

Thus, the resulting  $p_{err}(S'_k(\mathcal{N}))$  error probability is<sup>53</sup>

$$p_{err}(S'_k(\mathcal{N})) = \Pr\left(\log_2 \det\left(I_{K_{out}} + F(\mathbf{T}(\mathcal{N})) \frac{(\text{SNR}')^*}{K_{in}} F(\mathbf{T}(\mathcal{N}))^\dagger\right) < \frac{\varsigma_k(r + K_{in} - 1)}{r} P'(\mathcal{N})\right), \quad (117)$$

where  $I_{K_{out}}$  is the  $K_{out} \times K_{out}$  identity matrix.

Then, by exploiting a union bound averaged over the  $\mathcal{S}$  statistics (see (40)) for each  $\mathcal{N}_i$ ,<sup>53,54</sup> the  $h_{K_{in} > K_{out}}$  optimal tradeoff curve is yielded as follows:

$$h_{K_{in} > K_{out}} : \delta_k(\varsigma_k) = 2(2 - \varsigma_k). \quad (118)$$

Assuming the situation  $K_{in} \leq K_{out}$ , some further results can also be derived.

By using (115) and the properties of the multidimensional manifold space  $\mathcal{M}$  (see Theorem 1), and by averaging over the  $\mathcal{S}$  statistics, the  $h_{K_{in} \leq K_{out}}$  tradeoff function<sup>53</sup> without loss of generality is

$$h_{K_{in} \leq K_{out}} : \delta_k(\varsigma_k) = (i, (K_{in} - i) \cdot (K_{out} - i)), i = 0, \dots, n_{\min}. \quad (119)$$

Putting the pieces together, for each function  $h_{K_{in} > K_{out}}$  and  $h_{K_{in} \leq K_{out}}$ , the manifold extraction is optimized via the maximization of the  $n_{\min}$  smallest singular values as  $\lambda_1 \dots n_{\min}$ , where for each  $0 \leq \lambda_i \leq 2\sqrt{K_{in}}$  and are determined from  $\mathbf{M}_j$  (see (108)).

Exploiting the argumentation of (86), the corresponding condition on  $|\lambda_1 \dots n_{\min}|$  for the optimal tradeoff curve  $h$  is precisely as

$$h : \max_{\forall i} |\lambda_1 \dots n_{\min}| > c^{\frac{1}{2}} n_{\min} \frac{1}{n_{\min}^{\frac{1}{2}} n_{\min}} 2^{\frac{1}{2}} S'_k(\mathcal{N}_i), \quad (120)$$

for any constant  $c > 0$ .

The results for any  $K_{in} > K_{out}$  and  $K_{in} \leq K_{out}$  at  $K_{in}=2, K_{out}=4$  are summarized in Figure 4.

## 5 | CONCLUSIONS

The additional degree of freedom injected by the multicarrier transmission represents a significant resource to achieve performance improvements in CVQKD protocols. The proposed manifold extraction exploits those extra resources brought in by the multicarrier CVQKD modulation and is unavailable in a single-carrier CVQKD scheme. We introduced the term of multidimensional manifold extraction and proved that it can significantly improve the reliability of the phase space transmission. We demonstrated the results through the AMQD multicarrier modulation and extended it to the multiple-access multicarrier scenario through the AMQD-MQA scheme. We studied the potential of a

multidimensional manifold space of multicarrier CVQKD and the optimized tradeoff curve between the manifold parameter and the additional degree of freedom ratio. The results confirm that the possibilities in a multicarrier CVQKD significantly exceed the single-carrier CVQKD scenario. The extra degrees of freedom allow the utilization of sophisticated optimization techniques for the aim of performance improvement. The available and efficiently exploitable extra resources have a crucial significance in experimental CVQKD, particularly in long-distance scenarios.

## ACKNOWLEDGEMENTS

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).

## FUNDING

No relevant funding.

## COMPETING INTERESTS

We have no competing interests.

## COMPETING FINANCIAL INTERESTS

We have no competing financial interests.

## AUTHORS' CONTRIBUTIONS

L.GY. designed the protocol and wrote the manuscript. L.GY. and S.I. analyzed the results. All authors reviewed the manuscript.

## ETHICS STATEMENT

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

## DATA ACCESSIBILITY STATEMENT

This work does not have any experimental data.

## ORIGINAL ARTICLE STATEMENT

This paper is a completely novel and completely independent submission has no any connection with any previously submitted papers. This manuscript is the authors' original work and has not been published nor has it been submitted simultaneously elsewhere. All authors have checked the manuscript and have agreed to the submission.

## ORCID

Laszlo Gyongyosi  <https://orcid.org/0000-0002-4209-7619>

## REFERENCES

1. 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; 2014;912307. From Conference Volume 9123, Quantum Information and Computation XII, Baltimore, Maryland, USA. <https://doi.org/10.1117/12.2050095>
2. Gyongyosi L, Imre S. Secret key rate proof of multicarrier continuous-variable quantum key distribution. *Int J Commun Syst.* 2018;32:e3865. <https://doi.org/10.1002/dac.3865>

3. 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>
4. Gyongyosi L, Imre S. Gaussian quadrature inference for multicarrier continuous-variable quantum key distribution. *Quantum Stud Math Found*. 2019. Springer Nature. <https://doi.org/10.1007/s40509-019-00183-9>
5. 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>
6. Gyongyosi L. Diversity extraction for multicarrier continuous-variable quantum key distribution. In: Proceedings of the 2016 24th European Signal Processing Conference (EUSIPCO 2016); 2016.
7. 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; 2015:937711. <https://doi.org/10.1117/12.2076532>
8. Gyongyosi L, Imre S. Singular layer transmission for continuous-variable quantum key distribution. In: IEEE Photonics Conference (IPC) IEEE; 2014:2014. <https://doi.org/10.1109/IPCon.2014.6995246>
9. Gyongyosi L, Imre S. Proc. SPIE 9377, Advances in Photonics of Quantum Computing, Memory, and Communication VIII, 937711. 2015. <https://doi.org/10.1117/12.2076532>
10. Gyongyosi L, Imre S. 2015. <http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=2195505>
11. Gyongyosi L, Imre S. Gaussian quadrature inference for multicarrier continuous-variable quantum key distribution. *SPIE Quantum Information and Computation XIV, 17 - 21 Apr 2016*. Baltimore, Maryland, USA: Springer; 2016.
12. Pirandola S, Mancini S, Lloyd S, Braunstein SL. Continuous-variable quantum cryptography using two-way quantum communication. *Nature Physics*. 2008;4:726-730.
13. Grosshans F, Cerf NJ, Wenger J, Tualle-Brouri R, Grangier P. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quant Info Comput*. 2003;3:535-552.
14. Navascues M, Acin A. Security bounds for continuous variables quantum key distribution. *Phys Rev Lett*. 2005;94:020505.
15. Gyongyosi L, Imre S, Nguyen HV. A survey on quantum channel capacities. *IEEE Commun Surv Tutor*. 2018;99:1. <https://doi.org/10.1109/COMST.2017.2786748>
16. Gyongyosi L, Imre S. A survey on quantum computing technology. *Comput Sci Rev*. 2018;31:51-71. <https://doi.org/10.1016/j.cosrev.2018.11.002>
17. Pirandola S, Garcia-Patron R, Braunstein SL, Lloyd S. *Phys Rev Lett*. 2009;102:050503.
18. Pirandola S, Serafini A, Lloyd S. *Phys Rev A*. 2009;79:052327.
19. Pirandola S, Braunstein SL, Lloyd S. *Phys Rev Lett*. 2008;101:200504.
20. Weedbrook C, Pirandola S, Lloyd S, Ralph T. *Phys Rev Lett*. 2010;105:110501.
21. Weedbrook C, Pirandola S, Garcia-Patron R, et al. *Rev Mod Phys*. 2012;84:621.
22. Gyongyosi L, Imre S. Geometrical analysis of physically allowed quantum cloning transformations for quantum cryptography. *Inform Sci*. 2014;285:1-3. Elsevier. <https://doi.org/10.1016/j.ins.2014.07.010>
23. Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P, Diamanti E. Experimental demonstration of long-distance continuous-variable quantum key distribution. arXiv:1210.6216v1; 2012.
24. Navascues M, Grosshans F, Acin A. Optimality of gaussian attacks in continuous-variable quantum cryptography. *Phys Rev Lett*. 2006;97:190502.
25. Garcia-Patron R, Cerf NJ. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Phys Rev Lett*. 2006;97:190503.
26. Grosshans F. Collective attacks and unconditional security in continuous variable quantum key distribution. *Phys Rev Lett*. 2005;94:020504.
27. Adcock MRA, Hoyer P, Sanders BC. Limitations on continuous-variable quantum algorithms with Fourier transforms. *New J Phys*. 2009;11:103035.
28. Lloyd S. Capacity of the noisy quantum channel. *Physical Rev A*. 1997;55:1613-1622.
29. 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.
30. Lloyd S, Mohseni M, Rebentrost P. Quantum algorithms for supervised and unsupervised machine learning. arXiv:1307.0411; 2013.
31. Lloyd S, Mohseni M, Rebentrost P. Quantum principal component analysis. *Nat Phys*. 2014;10:631.
32. 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.
33. Kiktenko EO, Pozhar NO, Anufriev MN, et al. *Quantum-secured blockchain*, Vol. 3; 2018:035004.
34. Gyongyosi L, Imre S. Decentralized base-graph routing for the quantum internet. *Phys Rev A*. 2018;98:10-20. American Physical Society.
35. Van Meter R. *Quantum Networking*. New York: John Wiley and Sons Ltd; 2014.

36. 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/s11128-018-2147-8>
37. 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.
38. Imre S, Balazs F. *Quantum Computing and Communications – An Engineering Approach*. Hoboken: John Wiley and Sons Ltd; 2005. ISBN 0-470-86902-X, 283 pages.
39. Petz D. Quantum information theory and quantum statistics. 2008. Hiv: 6.
40. 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.
41. Pirandola S. Capacities of repeater-assisted quantum communications. arXiv:1601.00966; 2016.
42. Gyongyosi L, Imre S. Entanglement-gradient routing for quantum networks. *Sci Rep*. 2017;7:14255. Nature.
43. Gyongyosi L, Imre S. Entanglement availability differentiation service for the quantum internet. *Sci Rep*. 2018. Nature. <https://doi.org/10.1038/s41598-018-28801-3>
44. Biamonte J, et al. Quantum machine learning. *Nat*. 2017;549:195-202.
45. Laudenbach F, Pacher C, Fred Fung C-H, et al. Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations, *Adv. Quantum Technol*. 2018;1800011.
46. Shor PW. Scheme for reducing decoherence in quantum computer memory. *Phys Rev A*. 1995;52:R2493-R2496.
47. Kimble HJ. The quantum Internet. *Nat*. 2008;453:1023-1030.
48. 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>
49. Pirandola S, Braunstein SL, Laurenza R, et al. Theory of channel simulation and bounds for private communication. *Quantum Sci Technol*. 2018;3:035009.
50. Laurenza R, Pirandola S. General bounds for sender-receiver capacities in multipoint quantum communications. *Phys Rev A*. 2017;96:032318.
51. Bacsardi L. On the way to quantum-based satellite communication. *IEEE Comm Mag*. 2013;51(08):50-55.
52. Gyongyosi L, Imre S. Low-dimensional reconciliation for continuous-variable quantum key distribution. *Appl Sci*. 2018;8:87. <https://doi.org/10.3390/app8010087>
53. Tse D, Viswanath P. *Fundamentals of Wireless Communication*. Cambridge: Cambridge University Press; 2005.
54. Middleton D. An Introduction to Statistical Communication Theory: An IEEE Press Classic Reissue, Hardcover, IEEE, ISBN-10: 0780311787, ISBN-13: 978-0780311787; 1960.
55. Kay S. *Fundamentals of Statistical Signal Processing*, Vol. I-III. Prentice Hall: New Jersey, USA; 2013.
56. Shieh W, Djordjevic I. *OFDM for Optical Communications*. Amsterdam: Elsevier; 2010.
57. Imre S, Gyongyosi L. *Advanced Quantum Communications - An Engineering Approach*. New Jersey, USA: Wiley-IEEE Press; 2012.

**How to cite this article:** Gyongyosi L, Imre S. Diversity Space of Multicarrier Continuous-Variable Quantum Key Distribution. *Int J Commun Syst*. 2019;e4003. <https://doi.org/10.1002/dac.4003>

## APPENDIX A

### A.1 | Multicarrier CVQKD

First, we summarize the basic notations of AMQD.<sup>1</sup> The following description assumes a single user, and the use of  $n$  Gaussian subchannels  $\mathcal{N}_i$  for the transmission of the subcarriers, from which only  $l$  subchannels 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  $\sigma_\omega^2$  is the modulation variance of the subcarrier quadratures, which are transmitted through a noisy Gaussian subchannel  $\mathcal{N}_i$ . Each  $\mathcal{N}_i$  Gaussian subchannel 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

$$\mathbf{z} = \mathbf{x} + i\mathbf{p} = (z_1, \dots, z_n)^T \in \mathcal{CN}(0, \mathbf{K}_z), \quad (\text{A1})$$

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

$$z_j \in \mathcal{CN}(0, \sigma_{\omega_{z_j}}^2), z_j = x_j + ip_j. \quad (\text{A2})$$

Specifically, the real and imaginary variables (ie, 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

$$f(x_j) = \frac{1}{\sigma_{\omega_0}\sqrt{2\pi}} e^{-\frac{x_j^2}{2\sigma_{\omega_0}^2}}, f(p_j) = \frac{1}{\sigma_{\omega_0}\sqrt{2\pi}} e^{-\frac{p_j^2}{2\sigma_{\omega_0}^2}}, \quad (\text{A3})$$

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

$$\mathbf{K}_z = \mathbb{E}[\mathbf{z}\mathbf{z}^\dagger], \quad (\text{A4})$$

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

For vector  $\mathbf{z}$ ,

$$\mathbb{E}[\mathbf{z}] = \mathbb{E}[e^{i\gamma}\mathbf{z}] = \mathbb{E}e^{i\gamma}[\mathbf{z}] \quad (\text{A5})$$

holds, and

$$\mathbb{E}[\mathbf{z}\mathbf{z}^T] = \mathbb{E}[e^{i\gamma}\mathbf{z}(e^{i\gamma}\mathbf{z})^T] = \mathbb{E}e^{i2\gamma}[\mathbf{z}\mathbf{z}^T], \quad (\text{A6})$$

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

$$f(\mathbf{z}) = \frac{1}{\pi^n \det \mathbf{K}_z} e^{-\mathbf{z}^\dagger \mathbf{K}_z^{-1} \mathbf{z}}. \quad (\text{A7})$$

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

$$f(\mathbf{x}) = \frac{1}{(\sqrt{2\pi})^n \sqrt{\det(\mathbf{A}\mathbf{A}^T)}} e^{-\frac{\mathbf{x}^T \mathbf{x}}{2(\mathbf{A}\mathbf{A}^T)}}. \quad (\text{A8})$$

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 follows:

$$\mathbf{m} = F(\mathbf{v}) = e^{\frac{-\mathbf{m}^T \mathbf{A} \mathbf{A}^T \mathbf{m}}{2}} = e^{\frac{-\sigma_{\omega_0}^2 (m_1^2 + \dots + m_n^2)}{2}}. \quad (\text{A9})$$

In the first step of AMQD, Alice applies the inverse FFT (fast Fourier transform) operation to vector  $\mathbf{z}$  (see (A1)), 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

$$\mathbf{d} = F^{-1}(\mathbf{z}) = e^{\frac{\mathbf{d}^T \mathbf{A} \mathbf{A}^T \mathbf{d}}{2}} = e^{\frac{\sigma_{\omega_0}^2 (d_1^2 + \dots + d_n^2)}{2}}, \quad (\text{A10})$$

where

$$d_i = x_{d_i} + ip_{d_i}, \quad d_i \in \mathcal{CN}(0, \sigma_{d_i}^2), \quad (\text{A11})$$

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

$$\text{Re}(d_i) = x_{d_i} \in \mathcal{N}(0, \sigma_{\omega_i}^2), \quad \text{Im}(d_i) = p_{d_i} \in \mathcal{N}(0, \sigma_{\omega_i}^2), \quad (\text{A12})$$

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

$$\mathbf{T}(\mathcal{N}) = [T_1(\mathcal{N}_1), \dots, T_n(\mathcal{N}_n)]^T \in \mathbb{C}^n, \quad (\text{A13})$$

where

$$T_i(\mathcal{N}_i) = \text{Re}(T_i(\mathcal{N}_i)) + i\text{Im}(T_i(\mathcal{N}_i)) \in \mathbb{C}, \quad (\text{A14})$$

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

$$0 \leq \text{Re}T_i(\mathcal{N}_i) \leq 1/\sqrt{2}, \quad (\text{A15})$$

and

$$0 \leq \text{Im}T_i(\mathcal{N}_i) \leq 1/\sqrt{2}. \quad (\text{A16})$$

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

$$|T_i(\mathcal{N}_i)|^2 = \text{Re}T_i(\mathcal{N}_i)^2 + \text{Im}T_i(\mathcal{N}_i)^2 \in \mathbb{R}, \quad (\text{A17})$$

where

$$\text{Re}T_i(\mathcal{N}_i) = \text{Im}T_i(\mathcal{N}_i). \quad (\text{A18})$$

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

$$|F(T_i(\mathcal{N}_i))|^2. \quad (\text{A19})$$

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

$$\Delta = (\Delta_1, \dots, \Delta_n)^T \in \mathbb{CN}(0, \mathbf{K}_\Delta), \quad (\text{A20})$$

where

$$\mathbf{K}_\Delta = \mathbb{E}[\Delta \Delta^\dagger], \quad (\text{A21})$$

with independent, zero-mean Gaussian random components

$$\Delta_{x_i} \in \mathcal{N}(0, \sigma_{\mathcal{N}_i}^2), \quad (\text{A22})$$

and

$$\Delta_{p_i} \in \mathcal{N}(0, \sigma_{\mathcal{N}_i}^2), \quad (\text{A23})$$

with variance  $\sigma_{\mathcal{N}_i}^2$ , for each  $\Delta_i$  of a Gaussian subchannel  $\mathcal{N}_i$ , which identifies the Gaussian noise of the  $i$ -th subchannel  $\mathcal{N}_i$  on the quadrature components in the phase space  $\mathcal{S}$ .

The CVQFT-transformed noise vector can be rewritten as

$$F(\Delta) = (F(\Delta_1), \dots, F(\Delta_n))^T, \quad (\text{A24})$$

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  $F(\Delta) \in \mathbb{CN}(0, \mathbf{K}_{F(\Delta)})$  with a covariance matrix

$$\mathbf{K}_{F(\Delta)} = \mathbb{E}[F(\Delta)F(\Delta)^\dagger], \quad (\text{A25})$$

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

$$\frac{1}{n} \sum_{i=1}^n \sigma_{\omega_i}^2 = \sigma_\omega^2, \quad (\text{A26})$$

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

$$\sum_{i=1}^l \sigma_{\omega_i}^2 = l\sigma_\omega^2 < n\sigma_{\omega_0}^2. \quad (\text{A27})$$

In particular, from the relation of (A27), for the transmittance parameters the following relation follows at a given modulation variance  $\sigma_{\omega_0}^2$ , precisely,

$$|T_{AMQD}(\mathcal{N}_i)|^2 \sigma_{\omega_0}^2 > |T(\mathcal{N})|^2 \sigma_{\omega_0}^2, \quad (\text{A28})$$

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

$$|T_{AMQD}(\mathcal{N}_i)|^2 = \frac{1}{l} \sum_{i=1}^l |F(T_i(\mathcal{N}_i))|^2. \quad (\text{A29})$$

For the method of the determination of these  $l$  Gaussian subchannels, see Gyongyosi and Imre.<sup>1</sup> Alice's  $i$ -th Gaussian subcarrier is expressed as

$$|\phi_i\rangle = |d_i\rangle = |F^{-1}(z)\rangle. \quad (\text{A30})$$

## A.2 | Notations

The notations of the manuscript are summarized in Table A1.

**TABLE A1** Summary of notations

Notation	Description
$Q(\cdot)$	Gaussian tail function.
$\text{rank}(\cdot)$	Rank function.
$E$	An event.
$i$	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$ , where $x_j$ and $p_j$ are position and momentum quadratures of the $j$ -th Gaussian single-carrier.
$l$	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 $n-l$ subchannels 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.
$\text{SNR}_i$	The SNR of the $i$ -th Gaussian subchannel $\mathcal{N}_i$ , $\text{SNR}_i = \frac{\sigma_{\omega_i}^2}{\sigma_{\mathcal{N}_i}^2}$ .
$\text{SNR}'_i$	The SNR of the $i$ -th Gaussian subchannel $\mathcal{N}_i$ in the SVD-assisted multicarrier transmission, $\text{SNR}'_i = \frac{\sigma_{\omega_i''}^2}{\sigma_{\mathcal{N}_i}^2}$ .
$\text{SNR}$	The SNR of the Gaussian channel $\mathcal{N}$ , $\text{SNR} = \frac{\sigma_{\omega}^2}{\sigma_{\mathcal{N}}^2}$ .
$\text{SNR}'$	The SNR of the Gaussian channel $\mathcal{N}$ in an SVD-assisted protocol, $\text{SNR}' = \frac{\sigma_{\omega''}^2}{\sigma_{\mathcal{N}}^2}$ .
$\text{SNR}_i^*$	The SNR of the $i$ -th Gaussian sub-channel $\mathcal{N}_i$ in a private transmission, $\text{SNR}_i^* = \frac{\sigma_{\omega_i}^2}{\sigma_{\mathcal{N}_i^*}^2}$ .
$(\text{SNR}'_i)^*$	The SNR of the $i$ -th Gaussian sub-channel $\mathcal{N}_i$ in an SVD-assisted private transmission, $(\text{SNR}'_i)^* = \frac{\sigma_{\omega_i''}^2}{\sigma_{\mathcal{N}_i^*}^2}$ .
$\text{SNR}^*$	The SNR of the Gaussian channel $\mathcal{N}$ in a private transmission, $\text{SNR}^* = \frac{\sigma_{\omega}^2}{\sigma_{\mathcal{N}^*}^2}$ .
$(\text{SNR}')^*$	The SNR of the Gaussian channel $\mathcal{N}$ in an SVD-assisted private transmission, $(\text{SNR}')^* = \frac{\sigma_{\omega''}^2}{\sigma_{\mathcal{N}^*}^2}$ .
$P(\mathcal{N}_i)$	The private classical capacity of a Gaussian sub-channel $\mathcal{N}_i$ .
$P'(\mathcal{N}_i)$	The private classical capacity of a Gaussian sub-channel $\mathcal{N}_i$ at SVD-assistance.
$S(\mathcal{N}), S_k(\mathcal{N})$	The secret key rate in a multicarrier setting, and the secret key rate of user $U_k$ .

(Continues)

**TABLE A1** (Continued)

Notation	Description
$S'(\mathcal{N}), S'_k(\mathcal{N}_i)$	The secret key rate in an SVD-assisted multicarrier transmission, and the secret key rate of user $U_k$ . In the manifold extraction these are fixed as $S'_k(\mathcal{N}) = \frac{\zeta_k}{n_{\min}} P'(\mathcal{N})$ , and $S'_k(\mathcal{N}_i) = \frac{\zeta_{k,i}}{n_{\min}} P'(\mathcal{N}_i)$ , respectively.
$ \delta_1 \dots l $	Product distance derived for the $l$ Gaussian subchannels, $ \delta_1 \dots l ^2 > \left(c \frac{1}{l 2^{S'(\mathcal{N}_i)}}\right)^l$ , for any constant $c > 0$ and secret key rate $S'(\mathcal{N}_i) > 0$ per $\mathcal{N}_i$ .
$p_{err}$	Error probability.
$\mathbf{p}_A$	An $l$ -dimensional random private codeword, $\mathbf{p}_A = (p_{A,1}, \dots, p_{A,l})^T$ , where the $i$ -th component $p_i$ is dedicated to $\mathcal{N}_i$ .
$\mathcal{T}$	Set of transmittance coefficients, such that for $\forall j$ of $\mathcal{T}$ : $ F(T_j(\mathcal{N}_j))  = \min_{\forall i} \{ F(T_i(\mathcal{N}_i)) \}$ , where $F(T_i(\mathcal{N}_i)) \geq \frac{1}{(\text{SNR}')^*}$ . It refers to the worst-case scenario at which a $S'(\mathcal{N}) > 0$ nonzero secret key rate could exist.
$\mathcal{S}(\mathcal{N}_i)$	A statistical averaging over the distribution of the $T_i(\mathcal{N}_i)$ transmittance coefficients.
$\chi_{2l}^2$	Chi-square distribution with $2l$ degrees of freedom has a density $f(x) = \frac{1}{(l-1)!} x^{l-1} e^{-x}$ , where $x \geq 0$ .
$\zeta_k$	Degree of freedom ratio of user $U_k$ , $\zeta_k = \frac{1}{P'(\mathcal{N})} S'_k(\mathcal{N}) n_{\min}$ .
$\delta_k$	Manifold parameter, $\delta_k(\zeta_k) = \lim_{(\text{SNR}')^* \rightarrow \infty} \frac{-\log_2 p_{err} \left( \frac{S'_k(\mathcal{N})}{n_{\min}} \right)}{\frac{1}{n_{\min}}} P'(\mathcal{N})$ .
$p_{err}^{\text{single}}$	Error probability in a single-carrier transmission, $p_{err}^{\text{single}} = \frac{1}{((\text{SNR}')^*)^{\delta_{\text{single}}}}$ , where $\delta_{\text{single}} = 1 - \zeta$ .
$p_{err}^{\text{AMQD}}$	Error probability in a multicarrier transmission, $p_{err}^{\text{AMQD}} = \frac{1}{((\text{SNR}')^*)^{\delta_{\text{AMQD}}}}$ , $\delta_{\text{AMQD}} = l(1 - \zeta)$ .
$\partial_k, \partial_{k,i}$	Distance function for the phase space constellation $\mathcal{C}'_s(\mathcal{N})$ and $\mathcal{C}'_s(\mathcal{N}_i)$ of user $U_k$ , $\partial_i = \frac{1}{2^{S'_k(\mathcal{N}_i)/2}}$ , and $\partial_{k,i} = \frac{1}{2^{S'_k(\mathcal{N}_i)/2}}$ .
$f$	The optimal manifold-degree of freedom ratio tradeoff curve for a single-carrier transmission, $f: \delta_k(\zeta_k) = Z(1 - \zeta_k)$ , where $0 < \zeta_k \leq 1$ .
$h$	The optimal manifold-degree of freedom ratio tradeoff curve for multicarrier transmission, $f: \delta_k(\zeta_k) = lZ(1 - \zeta_k)$ , where $0 < \zeta_k \leq 1$ , at $l$ subchannels.
$r$	Number of interfering subchannels in an SVD-assisted multicarrier scenario.
$h(\mathcal{M})$	The multidimensional optimal manifold-degree of freedom ratio tradeoff curve over the multidimensional manifold space $\mathcal{M}$ .
$\mathcal{M}$	Multidimensional manifold space has dimension $\dim(\mathcal{M}) = K_{in} \zeta_k + (K_{out} - \zeta_k) \zeta_k$ .
$N_{\dim^\perp}$	The number of dimensions orthogonal to $\mathcal{M}$ in the space of $S(F(\mathbf{T}(\mathcal{N})))$ , $N_{\dim^\perp} = (K_{in} - \zeta_k)(K_{out} - \zeta_k)$ .
$S(F(\mathbf{T}(\mathcal{N})))$	The multidimensional space of $F(\mathbf{T}(\mathcal{N}))$ has dimension of $\dim(S(F(\mathbf{T}(\mathcal{N})))) = K_{in} K_{out}$ .
$\lambda_i^2$	The squared random singular values of $F(\mathbf{T}(\mathcal{N}))$ .
$\mathbf{K}_o$	An optimizing covariance matrix, defined as $\mathbf{K}_o = (\text{SNR}')^* \frac{I_{K_{in}}}{K_{in}}$ , where $I_{K_{in}}$ is the $K_{in} \times K_{in}$ identity matrix.
$\mathbf{M}_j$	The private codeword difference matrix, $\mathbf{M}_j = \frac{1}{\sqrt{(\text{SNR}')^*}} (\mathbf{p}_A - \mathbf{p}_B)$ .
$\tilde{\lambda} = \min_{\forall i}(\lambda_i)$	Smallest eigenvalue of the $\mathbf{M}_j$ private codeword difference matrix.
$\eta$	A maximization criteria over the distribution of $F(\mathbf{T}(\mathcal{N}))$ .
$S_1, S_2$	Sets of singular operators $S_1 = \{F_1, U_2^{-1}\}$ , $S_2 = \{U_1, U_2^{-1}\}$ .

(Continues)

TABLE A1 (Continued)

Notation	Description
$F(\mathbf{T})$	The SVD of $F(\mathbf{T})$ , $F(\mathbf{T}) = U_2 \Gamma F_1^{-1}$ , $F(\mathbf{T}) = U_2 \Gamma U_1^{-1}$ , where $F_1^{-1}$ , $F_1 \in \mathbb{C}^{K_{in} \times K_{in}}$ and $U_2$ , $U_2^{-1} \in \mathbb{C}^{K_{out} \times K_{out}}$ are unitary matrices, $K_{in}$ and $K_{out}$ refer to the number of sender and receiver users such that $K_{in} \leq K_{out}$ , $F_1^{-1} F_1 = F_1 F_1^{-1} = I$ , $U_2 U_2^{-1} = U_2^{-1} U_2 = I$ , and $\Gamma \in \mathbb{R}$ is a diagonal matrix with nonnegative real diagonal elements $\lambda_i$ , $F(\mathbf{T}) = \sum_{n_{\min}} \lambda_i U_{2,i} F_{1,i}^{-1}$ .
$\lambda_1 \geq \lambda_2 \geq \dots \lambda_{n_{\min}}$	The nonnegative real diagonal elements of the diagonal matrix $\Gamma \in \mathbb{R}$ , called the eigenchannels of $F(\mathbf{T}) = U_2 \Gamma F_1^{-1}$ .
$\lambda_i^2$	The $n_{\min}$ squared eigenchannels $\lambda_i^2$ are the eigenvalues of $F(\mathbf{T}) F(\mathbf{T})^\dagger = U_2 \Gamma \Gamma^T U_2^{-1}$ .
$n_{\min}$	$n_{\min} = \min(K_{in}, K_{out})$ , equals to the rank of $F(\mathbf{T})$ , where $K_{in} \leq K_{out}$ .
$\mathbf{s}$	Stream matrix, $\mathbf{s} = (s_1, \dots, s_{n_{\min}})^T \in \mathcal{CN}(0, \mathbf{K}_s)$ , defined by the unitary $F_1 (U_1)$ applied on $\mathbf{z} \in \mathcal{CN}(0, \mathbf{K}_z)$ .
$s_i$	A stream variable $s_i$ that identifies the CV state $ s_i\rangle$ in the phase space $\mathcal{S}$ . Expressed as $ s_i'\rangle = \lambda_i U_{2,i} F_{1,i}^{-1}  s_i\rangle$ , and $ \mathbf{s}'\rangle = F(\mathbf{T}) \mathbf{s} = \sum_{n_{\min}} \lambda_i U_{2,i} F_{1,i}^{-1}  s_i\rangle$ .
$U_2^{-1}(\gamma_i)$	The Fourier-transformed eigenchannel interference, $U_2^{-1}(\gamma_i) \in \mathcal{CN}(0, \mathbf{K}_{U_2^{-1}(\gamma_i)})$ , $\mathbf{K}_{U_2^{-1}(\gamma_i)} = \sigma_{\gamma_i}^2 = \mathbb{E}[ \gamma_i ^2]$ , $ U_2^{-1}(\gamma_i)\rangle = U_2^{-1} \left( \sum_{j \neq i}^{n_{\min}} \lambda_j U_{2,j} F_{1,j}^{-1} \right)  s_j\rangle$ . The variance $\sigma_{\gamma_i}^2 \rightarrow 0$ , in the low-SNR regimes.
$z \in \mathcal{CN}(0, \sigma_z^2)$	The variable of a single-carrier Gaussian CV state, $ \phi_i\rangle \in \mathcal{S}$ . 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.
$\Delta \in \mathcal{CN}(0, \sigma_\Delta^2)$	The noise variable of the Gaussian channel $\mathcal{N}$ , with i.i.d. zero-mean, Gaussian random noise components on the position and momentum quadratures $\Delta_x, \Delta_p \in \mathcal{N}(0, \sigma_{\Delta}^2)$ , $\sigma_\Delta^2 = \mathbb{E}[ \Delta ^2] = 2\sigma_{\mathcal{N}}^2$ .
$d \in \mathcal{CN}(0, \sigma_d^2)$	The variable of a Gaussian subcarrier CV state, $ \phi_i\rangle \in \mathcal{S}$ . 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 $\sigma_\omega^2$ is the 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.
$\sigma_\omega^2 = \frac{1}{l} \sum_l \sigma_{\omega_l}^2$	Multicarrier modulation variance. Average modulation variance of the $l$ Gaussian sub-channels $\mathcal{N}_l$ .
$ \phi_i\rangle$	The $i$ -th Gaussian subcarrier CV of user $U_k$ , $ \phi_i\rangle =  \text{IFFT}(z_{k,i})\rangle =  F^{-1}(z_{k,i})\rangle =  d_i\rangle$ , where IFFT stands for the Inverse Fast Fourier Transform, $ \phi_i\rangle \in \mathcal{S}$ , $d_i \in \mathcal{CN}(0, \sigma_{d_i}^2)$ , $\sigma_{d_i}^2 = \mathbb{E}[ d_i ^2]$ , $d_i = x_{d_i} + ip_{d_i}$ , $x_{d_i} \in \mathcal{N}(0, \sigma_{\omega_F}^2)$ , $p_{d_i} \in \mathcal{N}(0, \sigma_{\omega_F}^2)$ are i.i.d. zero-mean 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)$ , also expressed as $F( d_i\rangle) =  F(F^{-1}(z_{k,i}))\rangle =  z_{k,i}\rangle$ .
$\mathcal{N}$	Gaussian quantum channel.
$\mathcal{N}_i, i = 1, \dots, n$	Gaussian subchannels.

(Continues)

TABLE A1 (Continued)

Notation	Description
$T(\mathcal{N})$	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 sub-channel $\mathcal{N}_i$ , $T_i(\mathcal{N}_i) = \text{Re}(T_i(\mathcal{N}_i)) + i\text{Im}(T_i(\mathcal{N}_i)) \in \mathcal{C}$ , 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 $\text{Re}T_i(\mathcal{N}_i) = \text{Im}T_i(\mathcal{N}_i)$ .
$T_{\text{Eve}}$	Eve's transmittance, $T_{\text{Eve}} = 1 - T(\mathcal{N})$ .
$T_{\text{Eve},i}$	Eve's transmittance for the $i$ -th subcarrier CV.
$\mathcal{A} \subseteq K$	The subset of allocated users, $\mathcal{A} \subseteq K$ . Only the allocated users can transmit information in a given (particularly the $j$ -th) AMQD block. The cardinality of subset $\mathcal{A}$ is $ \mathcal{A} $ .
$U_k, k = 1, \dots,  \mathcal{A} $	An allocated user from subset $\mathcal{A} \subseteq K$ .
$\mathbf{z}$	A $d$ -dimensional, zero-mean, circular symmetric complex random Gaussian vector, $\mathbf{z} = \mathbf{x} + i\mathbf{p} = (z_1, \dots, z_d)^T$ , that models $d$ Gaussian CV input states, $\mathcal{CN}(0, \mathbf{K}_z)$ , $\mathbf{K}_z = \mathbb{E}[\mathbf{z}\mathbf{z}^\dagger]$ , where $z_i = x_i + ip_i$ , $\mathbf{x} = (x_1, \dots, x_d)^T$ , $\mathbf{p} = (p_1, \dots, p_d)^T$ , with $x_i \in \mathcal{N}(0, \sigma_{\omega_0}^2)$ , $p_i \in \mathcal{N}(0, \sigma_{\omega_0}^2)$ i.i.d. zero-mean Gaussian random variables.
$\mathbf{d} = F^{-1}(\mathbf{z})$	An $l$ -dimensional, zero-mean, circular symmetric complex random Gaussian vector of the $l$ Gaussian subcarrier CVs, $\mathcal{CN}(0, \mathbf{K}_d)$ , $\mathbf{K}_d = \mathbb{E}[\mathbf{d}\mathbf{d}^\dagger]$ , $\mathbf{d} = (d_1, \dots, d_l)^T$ , $d_i = x_i + ip_i$ , $x_i, p_i \in \mathcal{N}(0, \sigma_{\omega_F}^2)$ are i.i.d. zero-mean Gaussian random variables, $\sigma_{\omega_F}^2 = 1/\sigma_{\omega_0}^2$ . 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 $y_{k,m} = \sum_l F(T_i(\mathcal{N}_i))F(\mathbf{d}_i) + F(\Delta_i)$ .
$F(\mathbf{T}(\mathcal{N}))$	Fourier transform of $\mathbf{T}(\mathcal{N}) = [T_1(\mathcal{N}_1) \dots, T_l(\mathcal{N}_l)]^T \in \mathcal{C}^l$ , the complex transmittance vector.
$F(\Delta)$	Complex vector, expressed as $F(\Delta) = e^{\frac{-F(\Delta)^T K_{F(\Delta)} F(\Delta)}{2}}$ , with covariance matrix $K_{F(\Delta)} = \mathbb{E}[F(\Delta)F(\Delta)^\dagger]$ .
$\mathbf{y}[j]$	AMQD block, $\mathbf{y}[j] = F(\mathbf{T}(\mathcal{N}))F(\mathbf{d})[j] + F(\Delta)[j]$ .
$\tau = \ F(\mathbf{d})[j]\ ^2$	An exponentially distributed variable, with density $f(\tau) = (1/2\sigma_\omega^{2n})e^{-\tau/2\sigma_\omega^2}$ , $\mathbb{E}[\tau] \leq n2\sigma_\omega^2$ .
$T_{\text{Eve},i}$	Eve's transmittance on the Gaussian subchannel $\mathcal{N}_i$ , $T_{\text{Eve},i} = \text{Re}T_{\text{Eve},i} + i\text{Im}T_{\text{Eve},i} \in \mathcal{C}$ , $0 \leq \text{Re}T_{\text{Eve},i} \leq 1/\sqrt{2}$ , $0 \leq \text{Im}T_{\text{Eve},i} \leq 1/\sqrt{2}$ , $0 \leq  T_{\text{Eve},i} ^2 < 1$ .
$R_k$	Transmission rate of user $U_k$ .
$d_i$	A $d_i$ subcarrier in an AMQD block. For subset $\mathcal{A} \subseteq K$ with $ \mathcal{A} $ users and $n$ Gaussian subchannels for the transmission, $d_i = \frac{1}{\sqrt{n}} \sum_{k=0}^{ \mathcal{A} -1} z_k e^{\frac{-i2\pi ik}{n}}$ , $i = 0, \dots, n-1$ .
$\nu_{\min}$	The $\min\{\nu_1, \dots, \nu_l\}$ minimum of the $\nu_i$ subchannel coefficients, where $\nu_i = \sigma_{\mathcal{N}}^2 /  F(T_i(\mathcal{N}_i)) ^2$ and $\nu_i < \nu_{\text{Eve}}$ .
$\sigma_\omega^2$	Modulation variance, $\sigma_\omega^2 = \nu_{\text{Eve}} - \nu_{\min} \mathcal{G}(\delta)_{p(x)}$ , where $\nu_{\text{Eve}} = \frac{1}{\lambda}$ , $\lambda =  F(\mathbf{T}_{\mathcal{N}}^*) ^2 = \frac{1}{n} \sum_{i=0}^{n-1} \left  \sum_{k=0}^{n-1} T_k^* e^{\frac{-i2\pi ik}{n}} \right ^2$ and $T_{\mathcal{N}}^*$ is the expected transmittance of the Gaussian subchannels under an optimal Gaussian collective attack.
$\nu_\kappa$	Additional subchannel coefficient for the correction of modulation imperfections. For an ideal Gaussian modulation, $\nu_\kappa = 0$ , while for an arbitrary $p(x)$ distribution $\nu_\kappa = \nu_{\min} \left( 1 - \mathcal{G}(\delta)_{p(x)} \right)$ , where $\kappa = \frac{1}{\nu_{\text{Eve}} - \nu_{\min} \left( \mathcal{G}(\delta)_{p(x)} - 1 \right)}$ .
$\mathcal{N}_{U_k}[j]$	The set of $\mathcal{N}_i$ Gaussian subchannels from the set of $l$ good subchannels that transmit the $s$ subcarriers of user $U_k$ in the $j$ -th AMQD block, $\mathcal{N}_{U_k}[j] = [\mathcal{N}_1, \dots, \mathcal{N}_s]^T$ .

(Continues)



TABLE A1 (Continued)

Notation	Description
$\sigma_{\omega_i}^2$	The constant modulation variance $\sigma_{\omega_i}^2$ for eigenchannel $\lambda_i$ , evaluated as $\sigma_{\omega_i}^2 = \mu - \left( \sigma_{\mathcal{N}}^2 / \max_{n_{\min}} \lambda_i^2 \right) = \frac{1}{n_{\min}} \sigma_{\omega'}^2$ , with a total constraint $\sigma_{\omega'}^2 = \sum_{n_{\min}} \sigma_{\omega_i}^2 = \frac{1}{l} \sum_l \sigma_{\omega_l}^2 = \sigma_{\omega}^2$ .
$\sigma_{\omega''}^2$	The modulation variance of the AMQD multicarrier transmission in the SVD environment. Expressed as $\sigma_{\omega''}^2 = \nu_{Eve} - \left( \sigma_{\mathcal{N}}^2 / \max_{n_{\min}} \lambda_i^2 \right)$ , where $\lambda_i$ is the $i$ -th eigenchannel of $F(\mathbf{T})$ , $\max_{n_{\min}} \lambda_i^2$ is the largest eigenvalue of $F(\mathbf{T})F(\mathbf{T})^\dagger$ , with a total constraint $\frac{1}{l} \sum_l \sigma_{\omega_i}^2 = \sigma_{\omega''}^2 > \sigma_{\omega}^2$ .
$S(F(\mathbf{T}))$	The statistical model of $F(\mathbf{T})$ at a partial channel side information, $S(F(\mathbf{T})) = \xi_{K_{out}}^{-1} \Gamma \xi_{K_{in}}$ , where $\xi_{K_{out}}^{-1}$ and $\xi_{K_{in}}$ are unitaries that formulate the input covariance matrix $\mathbf{K}_s = \xi_{K_{in}} \mathcal{O} \xi_{K_{in}}^{-1}$ , while $\mathcal{O}$ is a diagonal matrix, $\mathbf{K}_s = Q \text{diag} \left\{ \sigma_{\omega_1}^2, \dots, \sigma_{\omega_{K_{in}}}^2 \right\} Q^\dagger$ .
$\mathcal{C}_s$	Phase space constellation $\mathcal{C}_s$ .
$\mathcal{C}_s^P(\mathcal{N})$	Random phase space permutation constellation for the transmission of the Gaussian subcarriers, expressed as $\mathcal{C}_s^P(\mathcal{N}) = \mathcal{C}_s^P(\mathcal{N}_1), \dots, \mathcal{C}_s^P(\mathcal{N}_l) = ( \phi_1 \dots d_{\mathcal{C}_s^P(\mathcal{N}_1)} \rangle, P_2  \phi_1 \dots d_{\mathcal{C}_s^P(\mathcal{N}_2)} \rangle, \dots, P_l  \phi_1 \dots d_{\mathcal{C}_s^P(\mathcal{N}_l)} \rangle)$ , where $ \phi_i \rangle$ are the Gaussian subcarrier CVs, $P_i, i=2, \dots, l$ is a random permutation operator, $d_{\mathcal{C}_s(\mathcal{N}_i)} = d_{\mathcal{C}_s(\mathcal{N}_j)}$ is the cardinality of $\mathcal{C}_s(\mathcal{N}_i)$ . The optimality function is $o(\mathcal{C}_s(\mathcal{N})) = \sum_l (\nu_{Eve} -  \delta_i ^2)$ .
$d_{\mathcal{C}_s^P(\mathcal{N}_i)}$	Cardinality of $\mathcal{C}_s(\mathcal{N}_i)$ .
$\delta_i$	The normalized difference of two Gaussian subcarriers $d_{A,i}$ and $d_{B,i}$ , $\delta_i = \frac{1}{\sqrt{\frac{\sigma_{\omega'}^2}{\sigma_{\mathcal{N}}^2}}} (d_{A,i} - d_{B,i})$ .
$\partial$	Difference function of Gaussian subcarriers (phase space symbols) $d_{A,i}$ and $d_{A,j}$ in constellations $\mathcal{C}_s^P(\mathcal{N}_k), k=1, \dots, l$ . For two Gaussian subchannels $\mathcal{N}_1$ and $\mathcal{N}_2$ , $\partial(\mathcal{C}_s^P(\mathcal{N}_1)) = \min_{\forall d_{A,i}} (d_{A,i} - d_{A,j}), \partial(\mathcal{C}_s^P(\mathcal{N}_2)) = \dots \partial(\mathcal{C}_s^P(\mathcal{N}_1))$ , where $\geq 2, j \neq i$ .