Order statistics and random matrix theory of multicarrier continuous-variable quantum key distribution

Laszlo Gyongyosi

School of Electronics and Computer Science, University of Southampton, Southampton, UK
Department of Networked Systems and Services, Budapest University of Technology and Economics, Budapest, Hungary
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

Summary
In a multicarrier continuous-variable quantum key distribution (CVQKD) protocol, the information is granulated into Gaussian subcarrier CVs and the physical Gaussian link is divided into Gaussian sub-channels. Here, we propose a combined mathematical framework of order statistics and random matrix theory for multicarrier continuous-variable quantum key distribution. The analysis covers the study of the distribution of the sub-channel transmittance coefficients in the presence of a Gaussian noise and the utilization of the moment generation function (MGF) in the error analysis. We reveal the mathematical formalism of sub-channel selection and formulation of the transmittance coefficients and show a reduced complexity progressive sub-channel scanning method. We define a framework to evaluate the statistical properties of the information flowing processes in multicarrier CVQKD protocols. Using random matrix theory, we express the achievable secret key rates and study the efficiency of the adaptive multicarrier quadrature division-multiuser quadrature allocation (AMQD-MQA) multiple-access multicarrier CVQKD. The proposed combined framework is particularly convenient for the characterization of the physical processes of experimental multicarrier CVQKD.

KEYWORDS
cryptography, networking, quantum cryptography, quantum key distribution, security

1 | INTRODUCTION

The continuous-variable quantum key distribution (CVQKD) protocols allow the establishment of an unconditional secure communication over standard, currently established telecommunication networks. Another motivation behind the use of CVQKD is the development of the quantum Internet and quantum computers. In a CVQKD...
system, the information is carried by a continuous-variable quantum state that is defined in the phase space via the position and momentum quadratures. Since a Gaussian modulation is a reasonable modulation technique in an experiment, these CV quantum states have a Gaussian random distribution. Precisely, the presence of an eavesdropper on the quantum channel adds a white Gaussian noise into the transmission because the optimal attack against a CVQKD protocol is provably also Gaussian. Besides the attractive properties of CVQKD, the relevant performance attributes, such as secret key rates and transmission distances, still require significant improvements. For this purpose, the multicarrier CVQKD has been recently introduced through the adaptive quadrature division modulation (AMQD) scheme. The multicarrier CVQKD injects several additional degrees of freedom onto the transmission which is not available for a standard, single-carrier CVQKD setting. In particular, these extra benefits and resources not just allow the realization of higher secret key rates and higher amount of tolerable losses with unconditional security, but also make possible the introduction and defining of several new phenomena for CVQKD, such as singular layer transmission, enhanced security thresholds, multidimensional manifold extraction, subcarrier domain analysis, secret key rate adapting, or the utilization of inference methods. The benefits of multicarrier CVQKD has also been proposed for multiple-access multicarrier CVQKD via the AMQD-MQA (multiuser quadrature allocation). An adaptive quadrature detection technique has also been defined for multicarrier CVQKD, which uses a channel transmittance estimation to decode the continuous variables. The secret key rates of multicarrier CVQKD confirms the multimode bounds of a previous study (see the results on fundamental rate-loss scaling in quantum optical communications in a previous study). For an additional information on the bounds of private quantum communications, we suggest another work.

Here, we particularly focus on the characterization of the transmittance coefficients of the sub-channels through the statistical analysis of their distribution. We also define a random matrix formalism to describe the process of information flow via the Gaussian subcarrier CVs. We develop a combined framework that utilizes and integrates the results of distribution statistics and random matrix theory. The proposed combined framework provides a tool to characterize the physical distribution and transmission processes of information flowing in experimental multicarrier CVQKD scenarios.

First, we provide a distribution statistics framework for multicarrier CVQKD. The distribution statistics of multicarrier CVQKD utilizes the results of order statistics, which is an important subfield of statistical theory, with several applications—from mathematical statistics and engineering to the analysis of traditional communication systems. We reveal the statistical properties of the multicarrier transmission and define the statistical operators of sub-channel ordering, selection, and formulation of the single-carrier-level transmittance coefficients. We also define the conditions that are required for the simultaneous achievement of a maximal secret key rate and an unconditional security at diverse channel parameters. The proposed distribution statistics analysis covers the study of the distribution of the sub-channel transmittance coefficient in the presence of a Gaussian noise and the utilization of the moment generation function (MGF) in the error analysis, such as the distribution of the received Gaussian subcarriers.

Random matrix theory represents a useful mathematical tool with a widespread application—from physics, statistics, to engineering problems and communication theory. The popularity of random matrix theory is rooted in the fact that several problems can be directly interpreted and solved via the mathematical framework of random matrix formalism. In the second part, using the results of distributions statics, we define a random matrix formalism for multicarrier CVQKD. Using the framework provided by random matrix formalism, we characterize the statistical properties of the information transmission process, derive the achievable secret key rates, and study the multiuser efficiency of the AMQD-MQA multiple-access multicarrier CVQKD scheme.

The novel contributions of our manuscript are as follows:

1. We propose a mathematical framework of order statistics and random matrix theory for multicarrier continuous-variable quantum key distribution.
2. The order statistics analysis covers the study of the distribution of the sub-channel transmittance coefficients in the presence of a Gaussian noise and the utilization of the moment generation function (MGF) in the error analysis.
3. We reveal the mathematical formalism of sub-channel selection and show a reduced complexity progressive sub-channel scanning method.
4. We define a random matrix formalism for multicarrier CVQKD to evaluate the statistical properties of the information flowing process.
5. Using random matrix theory, we express the achievable secret key rates and study the efficiency of the adaptive multicarrier quadrature division–multiuser quadrature allocation (AMQD-MQA) multiple-access multicarrier CVQKD.
6. The proposed framework is particularly convenient for the characterization of the physical processes of experimental multichannel CVQKD.

This paper is organized as follows. In Section 2, some preliminary findings are summarized. Section 3 provides the distribution statistics of multichannel CVQKD. Section 4 discusses the random matrix formalism of multiple-access multichannel CVQKD via the analysis of AMQD-MQA. Finally, Section 5 concludes the results. Supplementary information is included in the Appendix.

2  |  PRELIMINARIES

This section briefly summarizes the notations and basic terms. For further information, see previous work.77

2.1  |  Terms and definitions

2.1.1  |  Multichannel CVQKD

First, we summarize the basic notations of AMQD.77 The following description assumes a single user, and the use of $n$ Gaussian sub-channels $\mathcal{N}_j$ for the transmission of the subcarriers, from which only $l$ sub-channels will carry valuable information.

In the single-carrier modulation scheme, the $j$th input single-carrier state $|\varphi_j\rangle = |x_j + ip_j\rangle$ is a Gaussian state in the phase space $S$, with i.i.d. Gaussian random position and momentum quadratures $x_j \in \mathcal{N}(0, \sigma_{x_0}^2)$, $p_j \in \mathcal{N}(0, \sigma_{p_0}^2)$, where $\sigma_{x_0}$ is the modulation variance of the quadratures. (For simplicity, $\sigma_{x_0}$ 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 multichannel scenario, the information is carried by Gaussian subcarrier CVs, $|\varphi_j\rangle = |x_j + ip_j\rangle$, $x_j \in \mathcal{N}(0, \sigma_{x_0}^2)$, $p_j \in \mathcal{N}(0, \sigma_{p_0}^2)$, where $\sigma_{x_0}$ is the modulation variance of the subcarrier quadratures, which are transmitted through a noisy Gaussian sub-channel $\mathcal{N}_i$. Each $\mathcal{N}_i$ Gaussian sub-channel is dedicated for the transmission of one Gaussian subcarrier CV from the $n$ subcarrier CVs. (Note: index $i$ refers to the subcarriers, while index $j$ to the single-carriers throughout the manuscript.) The single-carrier state $|\varphi_j\rangle$ in the phase space $S$ can be modeled as a zero-mean, circular symmetric complex Gaussian sub-channel $z_j \in \mathcal{N}(0, \sigma_{z_0}^2)$, with variance $\sigma_{z_0}^2 = \mathbb{E} [||z_j||^2]$, and with i.i.d. real and imaginary zero-mean Gaussian random components $\text{Re} (z_j) \in \mathcal{N}(0, \sigma_{z_0}^2)$, $\text{Im} (z_j) \in \mathcal{N}(0, \sigma_{z_0}^2)$.

In the multichannel 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

$$z = x + ip = (z_1, \ldots, z_n)^T \in \mathcal{N}(0, \mathbf{K}_x),$$

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

$$z_j \in \mathcal{N}(0, \sigma_{z_0}^2), \quad z_j = x_j + ip_j.$$  

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

$$f(x_j) = \frac{1}{\sigma_{x_0} \sqrt{2\pi}} e^{-\frac{x_j^2}{2\sigma_{x_0}^2}}, \quad f(p_j) = \frac{1}{\sigma_{p_0} \sqrt{2\pi}} e^{-\frac{p_j^2}{2\sigma_{p_0}^2}},$$

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

$$\mathbf{K}_x = \mathbb{E} [\mathbf{z}\mathbf{z}^\dagger],$$

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

For vector $\mathbf{z}$,

$$\mathbb{E} [\mathbf{z}] = \mathbb{E} [e^{i\mathbf{p}}\mathbf{z}] = \mathbb{E}e^{i\mathbf{p}} [\mathbf{z}]$$

holds and

$$\mathbb{E} [\mathbf{z}\mathbf{z}^T] = \mathbb{E} [e^{i\mathbf{p}}(e^{i\mathbf{p}}\mathbf{z})^T] = \mathbb{E}e^{i\mathbf{p}} [\mathbf{z}\mathbf{z}^T],$$

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

$$f(\mathbf{z}) = \frac{1}{\pi^n \det \mathbf{K}_z} e^{-\frac{1}{2} \mathbf{z}^T \mathbf{K}_z^{-1} \mathbf{z}}. \quad (7)$$

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

$$f(\mathbf{x}) = \frac{1}{(\sqrt{2\pi})^n \sqrt{\det (\mathbf{A} \mathbf{A}^T)}} e^{-\frac{1}{2} \mathbf{x}^T \mathbf{K}_z^{-1} \mathbf{x}}. \quad (8)$$

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

$$\mathbf{m} = F(\mathbf{v}) = e^{-\frac{\mathbf{m}^T \mathbf{A}^T \mathbf{A} \mathbf{m}}{2}} = e^{-\frac{1}{2} \sum (\sigma^2_m - \sigma^2_n)}, \quad (9)$$

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

$$\mathbb{R}e (d_i) = x_{d_i} \in \mathcal{N} (0, \sigma^2_{d_i}), \quad \mathbb{I}m (d_i) = p_{d_i} \in \mathcal{N} (0, \sigma^2_{d_i}), \quad (12)$$

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

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

$$\mathbf{T} (\mathcal{N}) = \left[ T_1 (\mathcal{N}_1), \ldots, T_n (\mathcal{N}_n) \right]^T \in \mathbb{C}^n. \quad (13)$$

where

$$T_i (\mathcal{N}_i) = \mathbb{R}e (T_i (\mathcal{N}_i)) + i \mathbb{I}m (T_i (\mathcal{N}_i)) \in \mathbb{C} \quad (14)$$

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

$$0 \leq \mathbb{R}e T_i (\mathcal{N}_i) \leq 1 / \sqrt{2} \quad (15)$$

and

$$0 \leq \mathbb{I}m T_i (\mathcal{N}_i) \leq 1 / \sqrt{2}. \quad (16)$$

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

$$\left| T_i (\mathcal{N}_i) \right|^2 = \mathbb{R}e T_i (\mathcal{N}_i)^2 + \mathbb{I}m T_i (\mathcal{N}_i)^2 \in \mathbb{R}, \quad (17)$$

where

$$\mathbb{R}e T_i (\mathcal{N}_i) = \mathbb{I}m T_i (\mathcal{N}_i). \quad (18)$$
The Fourier-transformed transmittance of the $i$th sub-channel $\mathcal{N}_i$ (resulted from CVQFT operation at Bob) is denoted by
\[
|F(T_i(\mathcal{N}_i))|^2.
\]
(19)

The $n$-dimensional zero-mean, circular symmetric complex Gaussian noise vector $\Delta \in \mathcal{CN}(0, \sigma^2_\Delta)\_n$ of the quantum channel $\mathcal{N}$, is evaluated as
\[
\Delta = (\Delta_1, \ldots, \Delta_n)^T \in \mathcal{CN}(0, K_\Delta),
\]
(20)
where
\[
K_\Delta = \mathbb{E}[\Delta \Delta^\dagger]
\]
(21)
with independent, zero-mean Gaussian random components
\[
\Delta_{x_i} \in \mathcal{N}\left(0, \sigma^2_{\mathcal{N}_i}\right)
\]
(22)
and
\[
\Delta_{p_i} \in \mathcal{N}\left(0, \sigma^2_{\mathcal{N}_i}\right),
\]
(23)
with variance $\sigma^2_\Delta$, for each $\Delta_i$ of a Gaussian sub-channel $\mathcal{N}_i$, which identifies the Gaussian noise of the $i$th sub-channel $\mathcal{N}_i$ on the quadrature components in the phase space $\mathbb{S}$.

The CVQFT-transformed noise vector can be rewritten as
\[
F(\Delta) = (F(\Delta_1), \ldots, F(\Delta_n))^T,
\]
(24)
with independent components $F(\Delta_{x_i}) \in \mathcal{N}\left(0, \sigma^2_{F(\mathcal{N}_i)}\right)$ and $F(\Delta_{p_i}) \in \mathcal{N}\left(0, \sigma^2_{F(\mathcal{N}_i)}\right)$ on the quadratures, for each $F(\Delta_i)$. It also defines an $n$-dimensional zero-mean, circular symmetric complex Gaussian random vector $F(\Delta) \in \mathcal{CN}(0, K_{F(\Delta)})$ with a covariance matrix
\[
K_{F(\Delta)} = \mathbb{E}[F(\Delta) F(\Delta)^\dagger],
\]
(25)
where $K_{F(\Delta)} = K_\Delta$, by theory. At a constant subcarrier modulation variance $\sigma^2_{\omega_0}$ for the $n$ Gaussian subcarrier CVs, the corresponding relation is
\[
\frac{1}{n} \sum_{i=1}^{n} \sigma^2_{\omega_0} = \sigma^2_{\omega_0},
\]
(26)
where $\sigma^2_{\omega_0}$ is the modulation variance of the quadratures of the subcarrier $|\phi_i\rangle$ transmitted by sub-channel $\mathcal{N}_i$. Assuming $l$ good Gaussian sub-channels from the $n$ with constant quadrature modulation variance $\sigma^2_{\omega_0}$, where $\sigma^2_{\omega_0} = 0$ for the $i$th unused sub-channel,
\[
\sum_{i=1}^{l} \sigma^2_{\omega_0} = l\sigma^2_{\omega_0} < n\sigma^2_{\omega_0},
\]
(27)
In particular, from the relation of (27), for the transmittance parameters, the following relation follows at a given modulation variance $\sigma^2_{\omega_0}$, precisely:
\[
\left|T_{AMQD}(\mathcal{N}_i)\right|^2 \sigma^2_{\omega_0} > \left|T(\mathcal{N})\right|^2 \sigma^2_{\omega_0},
\]
(28)
where $\left|T(\mathcal{N})\right|^2$ is the transmittance of $\mathcal{N}$ in a single-carrier scenario and
\[
\left|T_{AMQD}(\mathcal{N}_i)\right|^2 = \frac{1}{l} \sum_{i=1}^{l} \left|F(T_i(\mathcal{N}_i))\right|^2.
\]
(29)
For the method of the determination of these $l$ Gaussian sub-channels, see previous study.77 The $i$th Gaussian subcarrier of Alice is expressed as
\[
|\phi_i\rangle = |d_i\rangle = |F^{-1}(z)\rangle.
\]
(30)
The complex \( A_j (\mathcal{N}_j) \in \mathbb{C} \) single-carrier channel coefficient is derived from the \( l \) Gaussian sub-channel coefficients as
\[
A_j (\mathcal{N}_j) = \frac{1}{l} \sum_{i=0}^{l-1} F (T_i (\mathcal{N}_j)).
\] (31)

3 DISTRIBUTION STATISTICS FOR MULTICARRIER CVQKD

First, we summarize some preliminary findings from order statistics from a previous work\(^87\) then evaluate the theorems and proofs. Note the proofs throughout Section 3 follow the notations of the previous work.\(^87\)

3.1 Moment-generating function

The M moment-generating function (MGF)-function\(^87\) of a nonnegative random variable \( x, x \geq 0 \) is
\[
M_x (c) = \int_0^\infty P (x) e^{cx} dx,
\] (32)
where \( c \) is a complex dummy variable, \( P (\cdot) \) is the probability density function (PDF) function, and
\[
\mathbb{E} [x^n] = \frac{d^n}{dc^n} M_x (c) \big|_{c=0}.
\] (33)
It can be shown that
\[
M_x (-c) = \mathcal{L} \{ P (x) \},
\] (34)
where \( \mathcal{L} \) is the Laplace transform.

Particularly, using the M-function, the \( Q (\cdot) \) Gaussian tail function of \( x > 0 \) can be expressed precisely as
\[
Q (x) = \frac{1}{\pi} \int_0^{\pi/2} e^{-\frac{x^2}{2\sin^2 \phi}} d\phi,
\] (35)
where \( \phi \in [0, 2\pi] \) and
\[
Q^2 (x) = \frac{1}{\pi} \int_0^{\pi/4} e^{-\frac{x^2}{2\sin^2 \phi}} d\phi.
\] (36)

Assuming an error rate \( R_{err} (x) \)
\[
R_{err} (x) = aQ \left( \sqrt{bx} \right),
\] (37)
where \( a \) and \( b \) are constants, the \( \overline{R_{err}} \) average error rate is yielded as
\[
\overline{R_{err}} = \int_0^\infty aQ \left( \sqrt{b\text{SNR}} \right) P_{\text{SNR}} (x) dx,
\] (38)
where \( P_{\text{SNR}} (\cdot) \) is the PDF of the signal to noise ratio (SNR), which can be rewritten as
\[
\overline{R_{err}} = \frac{a}{\pi} \int_0^{\pi/2} M_{\text{SNR}} \left( \frac{-b}{2\sin^2 \phi} \right) d\phi,
\] (39)
where \( M_{\text{SNR}} (\cdot) \) is the M-function of the SNR.
3.2 Sub-channel distribution statistics

3.2.1 Marginal, joint, and conditional distributions of the sub-channels

Let the normalized independent, ordered transmittance coefficients of the \( l \) sub-channels be

\[
\frac{1}{l} \left| F \left( T_i \left( \mathcal{N}_i \right) \right) \right|^2, \quad i = 0, \ldots, l - 1, \tag{40}
\]

given in a descending order such that

\[
\frac{1}{l} \left| F \left( T_0 \left( \mathcal{N}_0 \right) \right) \right|^2 \geq \frac{1}{l} \left| F \left( T_1 \left( \mathcal{N}_1 \right) \right) \right|^2 \geq \ldots \geq \frac{1}{l} \left| F \left( T_{l-1} \left( \mathcal{N}_{l-1} \right) \right) \right|^2. \tag{41}
\]

The \( \frac{1}{l} \left| F \left( \tilde{T}_1 \left( \mathcal{N}_1 \right) \right) \right|^2 \) unordered variables are identically distributed with common PDF and cumulative distribution function (CDF), \( P_c(x) \) and \( f_c(x) \), respectively.

The \( P_c(x_0, \ldots, x_{l-1}) \) common joint PDF of the unordered variables can be expressed as

\[
P_c(x_0, \ldots, x_{l-1}) = \prod_{i=0}^{l-1} P_c(x_i). \tag{42}
\]

Without loss of generality, the ordered variables are not identically distributed and have PDF and CDF functions

\[
P_{\frac{1}{l} \left| F \left( T_i \left( \mathcal{N}_i \right) \right) \right|^2}(x) \tag{43}
\]

and

\[
f_{\frac{1}{l} \left| F \left( T_i \left( \mathcal{N}_i \right) \right) \right|^2}(x). \tag{44}
\]

Then, let \( P_{\frac{1}{l} \left| F \left( T_i \left( \mathcal{N}_i \right) \right) \right|^2}(x) \) the PDF function of the \( i \)th ordered sub-channel coefficient, as

\[
P_{\frac{1}{l} \left| F \left( T_i \left( \mathcal{N}_i \right) \right) \right|^2}(x) = \frac{I!}{(I-i)! (I-1)!} f_c(x)^{I-1} (1-f_c(x))^{I-I} P_c(x), \tag{45}
\]

with

\[
P_{\frac{1}{l} \left| F \left( T_i \left( \mathcal{N}_i \right) \right) \right|^2}(x) = I f_c(x)^{I-1} P_c(x) \tag{46}
\]

and

\[
P_{\frac{1}{l} \left| F \left( T_{l-i} \left( \mathcal{N}_{l-i} \right) \right) \right|^2}(x) = I (1-f_c(x))^{I-1} P_c(x). \tag{47}
\]

The \( P_{\frac{1}{l} \left| F \left( T_i \left( \mathcal{N}_i \right) \right) \right|^2, \frac{1}{l} \left| F \left( T_m \left( \mathcal{N}_m \right) \right) \right|^2}(x, y) \) joint PDF of \( \frac{1}{l} \left| F \left( T_k \left( \mathcal{N}_k \right) \right) \right|^2, \frac{1}{l} \left| F \left( T_m \left( \mathcal{N}_m \right) \right) \right|^2, m > k \) is as

\[
P_{\frac{1}{l} \left| F \left( T_i \left( \mathcal{N}_i \right) \right) \right|^2, \frac{1}{l} \left| F \left( T_m \left( \mathcal{N}_m \right) \right) \right|^2}(x, y) = \frac{I!}{(k-1)! (m-k-1)! (I-m)!} P_c(x) \cdot (f_c(x) - f_c(y))^{m-k} P_c(y) \cdot (f_c(y))^{I-m}. \tag{48}
\]

Since the ordered variables are not identically distributed, the \( P_c(x_0, \ldots, x_{l-1}) \) common joint PDF of (42) can be rewritten as a joint PDF function

\[
P_{\frac{1}{l} \left| F \left( T_i \left( \mathcal{N}_i \right) \right) \right|^2, \ldots, \frac{1}{l} \left| F \left( T_{l-i} \left( \mathcal{N}_{l-i} \right) \right) \right|^2}(x_0, \ldots, x_{l-1}) = I \prod_{i=0}^{l-1} P_c(x_i), \quad x_0 \geq x_1 \geq \ldots \geq x_{l-1}. \tag{49}
\]
Assuming that there are \( l - i \) available sub-channels, the \( m \)th ordered sub-channel coefficient is referred to as

\[
\frac{1}{l - 1} \left| F\left( T_m^i \left( \mathcal{N}_m \right) \right) \right|^2, \ m = 0, \ldots, (l - i) - 1. \tag{50}
\]

Using the variable of (50), and further assuming that

\[
\frac{1}{l} \left| F \left( T_i \left( \mathcal{N}_i \right) \right) \right|^2 = y, \tag{51}
\]

the \( P_{\frac{1}{l}}[F(T_m^i(\mathcal{N}_m))]^2|F(T(\mathcal{N}_i))]^2 = y \) conditional PDF can be evaluated as

\[
P_{\frac{1}{l}}[F(T_m^i(\mathcal{N}_m))]^2|F(T(\mathcal{N}_i))]^2 = y \left( x, y \right) = \frac{P_{\frac{1}{l}}[F(T_m^i(\mathcal{N}_m))]^2|F(T(\mathcal{N}_i))]^2 \left( x, y \right)}{P_{\frac{1}{l}}[F(T(\mathcal{N}_i))]^2 \left( y \right)}
\]

\[
= \frac{(l - i)!}{(m - i)! \cdot (l - m)!} \left( \frac{1 - f_i(x)}{f_i(y)} \right)^{m - i - 1} \frac{P_i(x)}{f_i(y)}^{l - m} \cdot x \leq y. \tag{52}
\]

Without loss of generality, at \( l - 1 \) available sub-channels, (50) can be rewritten as

\[
\frac{1}{l - 1} \left| F \left( T_m^i \left( \mathcal{N}_m \right) \right) \right|^2, \ m = 0, \ldots, (l - 1) - 1, \tag{53}
\]

and (51) holds, the conditional PDF is expressed as

\[
P_{\frac{1}{l - 1}}[F(T_m^i(\mathcal{N}_m))]^2 \left( x \right) = P_{\frac{1}{l - 1}}[F(T_m^i(\mathcal{N}_m))]^2 \left( x \right), \tag{54}
\]

where the PDF of \( \frac{1}{l - 1} \left| F \left( T_m^i \left( \mathcal{N}_m \right) \right) \right|^2 \) is

\[
P_{\frac{1}{l - 1}}[F(T_m^i(\mathcal{N}_m))]^2 \left( x \right) = \frac{P_i(x)}{1 - f_i(y)^{l - 1}}, \ x \geq y. \tag{55}
\]

In particular, focusing on the case that the \( l \) sub-channels are selected via operator \( \Lambda \) from a set of \( n \) variables \( S = \left\{ \frac{1}{l} \left| F \left( T_i \left( \mathcal{N}_i \right) \right) \right|^2 \right\}_{i=0}^{n-1} \), the joint PDF function is yielded as

\[
P_S(x_0, \ldots, x_{l-1}) = \frac{n!}{(n - l)!} f_c(x_{l-1})^{n-l} \prod_{i=0}^{l-1} P_c(x_i), x_0 \geq x_1 \geq \ldots \geq x_{l-1}. \tag{56}
\]

The model of the \( \Lambda_U \) order-and-sum (selection) operator of user \( U_k \) with single-carrier channel \( \mathcal{N}_{U_k} \) is depicted in Figure 1. Operator \( \Lambda_U \) is decomposed as \( \Lambda_U = \Omega_S \), where \( \Lambda_U \) first selects \( l \) sub-channels from the total \( n \) via an ordering operation \( O \), which uses the normalized, unordered \( \frac{1}{l} \left| F \left( T_i \left( \mathcal{N}_i \right) \right) \right|^2 \) coefficients; then, \( \Lambda_U \) evaluates \( A_j \left( \mathcal{N}_{U_k} \right) = \left( 1 / l \right) \sum_{i=0}^{l-1} F \left( T_i \left( \mathcal{N}_i \right) \right) \) from the ordered coefficients via the sum-operator \( \Sigma \) to yield \( A_j \left( \mathcal{N}_{U_k} \right) \).

### 3.2.2 Partial sum distributions of ordered sub-channels

**Proposition 1.** (PDF of the partial sum of sub-channel coefficients). The PDF function of single carrier transmittance \( A_j \left( \mathcal{N}_j \right) \) is \( P \left[ A_j \left( \mathcal{N}_j \right) \right] \left( x \right) = P_{\frac{1}{l}} \left[ F \left( T_i \left( \mathcal{N}_i \right) \right) \right]^2, \) where \( \Gamma_1 = \frac{1}{l} \sum_{i=0}^{l-2} \left| F \left( T_i \left( \mathcal{N}_i \right) \right) \right|^2 \) and \( \Gamma_2 = \frac{1}{l} \left| F \left( T_{l-1} \left( \mathcal{N}_{l-1} \right) \right) \right|^2 \) are two random correlated variables that identify the normalized, ordered sub-channel coefficients such that \( \frac{1}{l} \left| F \left( T_g \left( \mathcal{N}_g \right) \right) \right|^2 \geq \frac{1}{l} \left| F \left( T_{g+1} \left( \mathcal{N}_{g+1} \right) \right) \right|^2 \geq \ldots \geq \frac{1}{l} \left| F \left( T_{l-1} \left( \mathcal{N}_{l-1} \right) \right) \right|^2, \) is the minimum transmittance of the \( l \) sub-channels.
Proof. Let \(|A_j (\mathcal{N})|^2\) be identified as

\[ |A_j (\mathcal{N})|^2 = \frac{1}{l} \sum_{i=0}^{l-1} |F(T_i(\mathcal{N}))|^2, \tag{57} \]

and let the transmittances to be sorted in a descending order as

\[ \frac{1}{l} |F(T_0(\mathcal{N}))|^2 \geq \frac{1}{l} |F(T_1(\mathcal{N}))|^2 \geq \ldots \geq \frac{1}{l} |F(T_{l-1}(\mathcal{N}))|^2. \tag{58} \]

Particularly, the random variable in (57) can be decomposed to the sum of two correlated random variables as

\[ |A_j (\mathcal{N})|^2 = \Gamma_1 + \Gamma_2, \tag{59} \]

where

\[ \Gamma_1 = \frac{1}{l} \sum_{i=0}^{l-2} |F(T_i(\mathcal{N}))|^2 \tag{60} \]

and

\[ \Gamma_2 = \frac{1}{l} |F(T_{l-1}(\mathcal{N}))|^2. \tag{61} \]

Precisely, from (59), it follows that the PDF function of \(|A_j (\mathcal{N})|^2\) can be evaluated via two random correlated variables as

\[ P_{|A_j (\mathcal{N})|^2}(x) = P_{\Gamma_1, \Gamma_2}(x-y, y) dy. \tag{62} \]

Specifically, exploiting the Bayesian formula, it follows that

\[ P_{\Gamma_1, \Gamma_2}(x, y) = P_{\Gamma_2}(x) \times P_{\Gamma_1 | \Gamma_2 = x}(y), \tag{63} \]

where \(P_{\Gamma_2}(x)\) is the PDF of the \(l\)th (ordered) sub-channel transmittance coefficient while \(P_{\Gamma_1 | \Gamma_2 = x}(y)\) is the conditional PDF of the sum of the first \(l-1\) ordered sub-channel coefficients, at \(\frac{1}{l} |F(T_{l-1}(\mathcal{N}))|^2 = x\).

Then, let us assume that there are \(l-1\) available sub-channels, and let the \(i\)th sub-channel's quantity be referred to as \(\frac{1}{l} |F(T_i(\mathcal{N}))|^2\), \(i = 0, \ldots, l-2\).
Without loss of generality, for this quantity, the following relation holds:

$$P_{T_1, \tau_2=y}(x) = P_{t-2}^{1-\sum_{i=0}^{l-1}|F(T_i(N_i))|^2}(x), \tag{64}$$

where $P_{t-2}^{1-\sum_{i=0}^{l-1}|F(T_i(N_i))|^2}(x)$ is as

$$P_{t-2}^{1-\sum_{i=0}^{l-1}|F(T_i(N_i))|^2}(x) = \frac{P_\tau(x)}{1 - f_\tau(x)}, x \geq y. \tag{65}$$

### 3.2.3 Sub-channel selection with a complete scan

**Theorem 1.** (Sub-channel selection, $l$ from $n$). The M-function of $|F(T_i(N_i))|^2$ of the Gaussian sub-channel $N_i$ selection operator $\Lambda_0$ is

$$M_{|F(T_i(N_i))|^2}^{\Lambda_0}(x) = f\left(\frac{1}{l} |F(T_i'(N_i))|^2\right) + \int_{\frac{1}{l} |F(T_i(N_i))|^2}^{\infty} P\left(\frac{1}{l} |F(T_i(N_i))|^2\right) e^{\frac{1}{l} |F(T_i(N_i))|^2} d\left(\frac{1}{l} |F(T_i(N_i))|^2\right),$$

where $\frac{1}{l} |F(T_i'(N_i))|^2 \leq \frac{1}{l} |F(T_i(N_i))|^2$ is a threshold for all $N_i$, while $f(\cdot)$ and $P(\cdot)$ are the CDF and PDF functions of the ordered $\frac{1}{l} |F(T_i'(N_i))|^2$ coefficients. For $l$ Gaussian sub-channels with $\frac{1}{l} |F(T_i(N_i))|^2 \leq \frac{1}{l} |F(T_i'(N_i))|^2, i = 0, \ldots, l-1$, the M-function of $|A_i(N_i)|^2$ is

$$M_{|A_i(N_i)|^2}^{\Lambda_0}(x) = \prod_{i} f\left(\frac{1}{l} |F(T_i'(N_i))|^2\right) + \int_{\frac{1}{l} |F(T_i(N_i))|^2}^{\infty} P\left(\frac{1}{l} |F(T_i(N_i))|^2\right) e^{\frac{1}{l} |F(T_i(N_i))|^2} d\left(\frac{1}{l} |F(T_i(N_i))|^2\right).$$

**Proof.** First, let us assume that the operation of the selection of the $l$ sub-channels with the best $|T_i'(N_i)|^2$ coefficient from the total $n$ is depicted by operator $\Lambda_0$.

Assuming that the $l$ sub-channels are selected via $\Lambda_0$ at a $|F(T_i'(N_i))|^2$ threshold, the $P_{|A_i(N_i)|^2}^{\Lambda_0}$ PDF function can be expressed via the

$$P_{\frac{1}{l} \sum_{i=0}^{l-1}|F(T_i(N_i))|^2, \frac{1}{l} |F(T_{i-1}(N_{i-1}))|^2}(x - y, y) dy = P_{T_1, \tau_2}(x - y, y) dy \tag{66}$$

joint PDF function of the sub-channel $\frac{1}{l} F(T_i(N_i))$ as

$$P_{|A_i(N_i)|^2}^{\Lambda_0}(x) = \int_{0}^{\infty} P_{T_1, \tau_2}(x - y, y) dy. \tag{67}$$

The a priori fixed $|F(T_i'(N_i))|^2$ threshold is determined as

$$\frac{1}{l} |F(T_i'(N_i))|^2 \geq \frac{1}{l} |F(T_i(N_i))|^2, \tag{68}$$

for $i = 0, \ldots, l-1$, thus for all Gaussian sub-channels that carry valuable information.
The $\left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2$ threshold is derived from the security threshold $\nuEve = 1 / \lambda$ of the optimal Gaussian attack (see previous works\textsuperscript{77,78}), where $\lambda$ is the Lagrange multiplier as

$$\lambda = \left| F \left( T^*_N \right) \right|^2 = \frac{1}{l} \sum_{i=0}^{l-1} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 = \frac{1}{l} \sum_{k=0}^{l-1} \left| \sum \alpha^n_k e^{j2\pi k/n} \right|^2,$$

while $T^*_N$ is the expected transmittance of the $l$ sub-channels under an optimal Gaussian attack. For a detailed description, see previous study\textsuperscript{77}.

Without loss of generality, let us assume that the sub-channel transmittance coefficients are ordered in a descending order of (58).

Then, if $\frac{1}{l} \left| F \left( T_i (\mathcal{N}_i) \right) \right|^2 < \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2$, let

$$P^{\lambda_0}_{\frac{1}{l}|F(T_i(\mathcal{N}_i))|} \left( \frac{1}{l} \left| F \left( T_i (\mathcal{N}_i) \right) \right|^2 \right) = f^{\lambda_0}_{\frac{1}{l}|F(T_i(\mathcal{N}_i))|} \left( \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 \right) \delta_e \left( \frac{1}{l} \left| F \left( T_i (\mathcal{N}_i) \right) \right|^2 \right),$$

where $\delta_e (\cdot)$ is a random function, while for $\frac{1}{l} \left| F \left( T_i (\mathcal{N}_i) \right) \right|^2 \geq \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2$,

$$P^{\lambda_0}_{\frac{1}{l}|F(T_i(\mathcal{N}_i))|} \left( \frac{1}{l} \left| F \left( T_i (\mathcal{N}_i) \right) \right|^2 \right) = P^{\lambda_0}_{\frac{1}{l}|F(T_i(\mathcal{N}_i))|} \left( \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 \right).$$

After some calculations, the M-function of $\frac{1}{l} \left| F \left( T_i (\mathcal{N}_i) \right) \right|^2$ of sub-channel $\mathcal{N}_i$ is yielded as

$$M^{\lambda_0}_{\frac{1}{l}|F(T_i(\mathcal{N}_i))|} (\chi) = f^{\lambda_0}_{\frac{1}{l}|F(T_i(\mathcal{N}_i))|} \left( \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 \right)$$

$$+ \int_{\frac{1}{l}|F(T_i(\mathcal{N}_i))|^2}^{\infty} P^{\lambda_0}_{\frac{1}{l}|F(T_i(\mathcal{N}_i))|} \left( \frac{1}{l} \left| F \left( T_i (\mathcal{N}_i) \right) \right|^2 \right) e^{x \frac{1}{l}|F(T_i(\mathcal{N}_i))|^2} \frac{1}{l} \left| F \left( T_i (\mathcal{N}_i) \right) \right|^2 d \frac{1}{l} \left| F \left( T_i (\mathcal{N}_i) \right) \right|^2.$$ 

For $l$ Gaussian sub-channels with $\frac{1}{l} \left| F \left( T_i (\mathcal{N}_i) \right) \right|^2 \geq \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2$, $i = 0, \ldots, l-1$, the M-function of $\left| A_j (\mathcal{N}_j) \right|^2$ is

$$M^{\lambda_0}_{\left| A_j (\mathcal{N}_j) \right|^2} (\chi) = \prod_{i} M^{\lambda_0}_{\frac{1}{l}|F(T_i(\mathcal{N}_i))|} (\chi)$$

$$= \prod_{i} f^{\lambda_0}_{\frac{1}{l}|F(T_i(\mathcal{N}_i))|} \left( \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 \right)$$

$$+ \int_{\frac{1}{l}|F(T_i(\mathcal{N}_i))|^2}^{\infty} P^{\lambda_0}_{\frac{1}{l}|F(T_i(\mathcal{N}_i))|} \left( \frac{1}{l} \left| F \left( T_i (\mathcal{N}_i) \right) \right|^2 \right) e^{x \frac{1}{l}|F(T_i(\mathcal{N}_i))|^2} \frac{1}{l} \left| F \left( T_i (\mathcal{N}_i) \right) \right|^2 d \frac{1}{l} \left| F \left( T_i (\mathcal{N}_i) \right) \right|^2.$$ 

In particular, the $\Pr^{\lambda_0} (\cdot)$ probability that $l$ sub-channels are selected from the $n$ is as

$$\Pr^{\lambda_0} (l) = \left( \frac{n}{l} \right) \left( 1 - f_c \left( \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 \right) \right) \left( f_c \left( \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 \right) \right)^{n-l}.$$ 

Note that in a worst-case scenario, the condition $\frac{1}{l} \left| F \left( T_i (\mathcal{N}_i) \right) \right|^2 \geq \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2$ may not be satisfied for the required number $l$ of sub-channels. In this case, the threshold $\frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2$ can be redefined as

$$\frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 = \mu \max_{l} \frac{1}{l} \left| F \left( T_i (\mathcal{N}_i) \right) \right|^2,$$

where $0 < \mu < 1$ is a real variable. The condition of (75) satisfies that, at least, the best sub-channel is selected via the sub-channel allocation procedure. It also allows us to reevaluate the M-function of the $l$ sub-channels as follows.
Presuming that for \( l \) sub-channels, (75) is satisfied, resulting in the ordered coefficients \( \frac{1}{T} \left| F \left( T_i \left( \mathcal{N}_i \right) \right) \right|^2 \geq \frac{1}{T} \left| F \left( T_{i+1} \left( \mathcal{N}_{i+1} \right) \right) \right|^2 \). Using the \( P_{\lambda_i} \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2 \cdots \frac{1}{T} \left| F (T_{i-1}(\mathcal{N}_{i-1})) \right|^2 \) joint PDF function, the \( M^\lambda_{\frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2} (\mathcal{X}) \)-function is precisely as

\[
M^\lambda_{\left| F (T_{i}(\mathcal{N}_i)) \right|^2} (\mathcal{X}) = l \left( \sum_{i=0}^{\infty} \int_{0}^{\mu} \int_{0}^{\mu} \int_{0}^{\mu} \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2 P \left( \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2 \right) \right)
\]

\[
\cdot \left( f \left( \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2 \right) \right) \left( M \left( x, \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2 \right) \right)
\]

\[
- M \left( x, \mu \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2 \right) \left( \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2 \right)^{l-1} \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2,
\]

which can be simplified into

\[
M^\lambda_{\left| F (T_{i}(\mathcal{N}_i)) \right|^2} (\mathcal{X}) = l \left( \sum_{i=0}^{\infty} \int_{0}^{\mu} \int_{0}^{\mu} \int_{0}^{\mu} \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2 P \left( \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2 \right) \right)
\]

\[
\cdot \left( f \left( \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2 \right) \right) \left( M \left( x, \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2 \right) \right)
\]

\[
- M \left( x, \mu \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2 \right) \left( \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2 \right)^{l-1} \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2,
\]

and the partial function is

\[
M^\lambda_{\frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2} (w, x) = \int_{x}^{\infty} P \left( \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2 \right) e^{w \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2} d \frac{1}{T} \left| F (T_{i}(\mathcal{N}_i)) \right|^2,
\]

by some fundamental theory.

The probability that \( k \) sub-channels are selected from \( n \) at condition (75) is expressed as

\[
\Pr(k) = \Pr \left( \sum_{i=0}^{\infty} \int_{x}^{\mu} \int_{x}^{\mu} \int_{x}^{\mu} P_{0,k,k+1}(x, y, z) dx dy dz \right),
\]

\[
= \int_{0}^{\mu} \int_{0}^{\mu} \int_{0}^{\mu} P_{0,k,k+1}(x, y, z) dx dy dz,
\]

\[
\sum_{i=0}^{\infty} \int_{x}^{\mu} \int_{x}^{\mu} \int_{x}^{\mu} P_{0,k,k+1}(x, y, z) dx dy dz.
\]
where
\[ P_{0,k-1,k}(x, y, z) = \frac{n!}{(k-2)! (n-k-1)!} P_c(x) \]
\[ \cdot (f_c(x) - f_c(y))^{k-2} P_c(y) \]
\[ \cdot P_c(z) (f_c(z))^{n-k-1}. \] (80)

The proof is concluded here. \( \square \)

### 3.3 Optimized complexity progressive scan

**Theorem 2.** (Progressive sub-channel selection). The average number of iterations needed for the selection of the sub-channel transmittance coefficients at a threshold per sub-channels) needed to derive \( |A_i|^2 \) is yielded as

\[ \kappa_{\Lambda_0} = \sum_{i=1}^{l} \left( \frac{n}{i} \right) \left( 1 - f_c \left( \frac{1}{2} \left| F \left( T_i^+ \left( \mathcal{N}_i \right) \right) \right| \right) \right)^i \left( f_c \left( \frac{1}{2} \left| F \left( T_i^+ \left( \mathcal{N}_i \right) \right) \right| \right) \right)^{n-i} \]
\[ \cdot \left( n + \sum_{i=1}^{l-i} (n - i - k) \right). \] (81)

Operator \( \Lambda_0 \) does require the scan of the total \( n \) sub-channels, which is practically inconvenient.

To resolve this problem, we introduce operator \( \Lambda \) which performs a progressive scan: it stops the iteration as the sub-channels have found and does not require to scan through all the sub-channels. Let \( \Lambda' \) a slightly modified version of \( \Lambda \) that also handles the situation when only \( k < l \) sub-channels are found, but \( l \) was required by the legal parties for the transmission. In this case, the progressive scan operator \( \Lambda' \) selects the remaining \( l - k \) sub-channels from the set \( B \left( \mathcal{N}_k, \ldots, \mathcal{N}_{l-1} \right) \) of bad sub-channels, and the Lagrange multiplier in (69) at \( \Lambda' \) is reevaluated as

\[ \lambda_{\Lambda'} = \left| F \left( \tilde{T}_{\lambda'} \right) \right|^2 = \left| F \left( T_i^+ \left( \mathcal{N}_i \right) \right) \right|^2 + \varphi, \] (82)

where \( \varphi \) is a nonnegative real variable, expressed as

\[ \varphi = \left| F \left( T_i^+ \left( \mathcal{N}_i \right) \right) \right|^2 - \min \left( \left| F \left( T \left( \mathcal{N}_k \right) \right) \right|^2, \ldots, \left| F \left( T \left( \mathcal{N}_{l-1} \right) \right) \right|^2 \right), \] (83)

where \( \left| F \left( T \left( \mathcal{N}_k \right) \right) \right|^2, \ldots, \left| F \left( T \left( \mathcal{N}_{l-1} \right) \right) \right|^2 \) are the corresponding coefficients of \( B \left( \mathcal{N}_k, \ldots, \mathcal{N}_{l-1} \right) \).

As follows, (82) allows to the legal parties to preserve the security conditions via a modified security threshold \( \nu_{\text{avg}} = 1 / \lambda_{\Lambda'} \).

The \( \kappa_{\Lambda} \) and \( \kappa_{\Lambda'} \) average number of iterations of operators \( \Lambda \) and \( \Lambda' \) are evaluated as follows. The \( \Lambda \) sub-channel selection operator models the situation if the iteration stops as the \( \frac{1}{2} \left| F \left( T_i \left( \mathcal{N}_i \right) \right) \right|^2 \geq \frac{1}{2} \left| F \left( T_i^+ \left( \mathcal{N}_i \right) \right) \right|^2 \) condition is satisfied for \( l \) sub-channels, that is, it is not needed to determine \( \frac{1}{2} \left| F \left( T_i \left( \mathcal{N}_i \right) \right) \right|^2 \) for the remaining \( i = l, \ldots, n - 1 \) sub-channels.

Specifically, the \( \Pr_{\Lambda}(k) \) probability of the availability of \( l \) sub-channels for \( k = l \),

\[ \Pr_{\Lambda}(k) = \sum_{h=1}^{n} \binom{n}{h} \left( 1 - f_c \left( \frac{1}{2} \left| F \left( T_h^+ \left( \mathcal{N}_k \right) \right) \right| \right) \right)^h \]
\[ \cdot \left( f_c \left( \frac{1}{2} \left| F \left( T_h^+ \left( \mathcal{N}_k \right) \right) \right| \right) \right)^{n-h}, \] (84)
and the probability that only \( k < l, k = 0, \ldots, l - 1 \) sub-channels are available is

\[
\Pr_A(k) = \binom{n}{k} \left( 1 - f_c \left( \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 \right) \right)^k \cdot \left( f_c \left( \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 \right) \right)^{n-k},
\]

(85)

and

\[
M_{A_i(\mathcal{N}_i)}^\Lambda \left( x \right) = \sum_{h=0}^{l-1} \left( \binom{n}{h} \left( 1 - P \left( \frac{1}{l} \left| F \left( T_h^* (\mathcal{N}_h) \right) \right|^2 \right) \right)^h \cdot \left( P \left( \frac{1}{l} \left| F \left( T_h^* (\mathcal{N}_h) \right) \right|^2 \right) \right)^{n-h} M_{A_i(\mathcal{N}_i)}^{\Lambda(h)} \left( x \right) + \sum_{g=1}^{l} \binom{n}{g} \left( 1 - P \left( \frac{1}{l} \left| F \left( T_g^* (\mathcal{N}_i) \right) \right|^2 \right) \right)^g \cdot \left( P \left( \frac{1}{l} \left| F \left( T_g^* (\mathcal{N}_i) \right) \right|^2 \right) \right)^{n-g} \frac{M_{A_i(\mathcal{N}_i)}^{\Lambda(2)}}{M_{A_i(\mathcal{N}_i)}^{\Lambda(1)^2}} \left( x \right)^{l-1},
\]

(87)

where

\[
M_{A_i(\mathcal{N}_i)}^{\Lambda(1)} \left( x \right) = \left( M_{A_i(\mathcal{N}_i)}^{\Lambda(2)} \left( x \right) \right)^h \left( M_{A_i(\mathcal{N}_i)}^{\Lambda(1)} \left( x \right) \right)^{l-h},
\]

(88)

which can be rewritten as

\[
M_{A_i(\mathcal{N}_i)}^\Lambda \left( x \right) = \left( 1 - f_c \left( \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 \right) \right) M_{A_i(\mathcal{N}_i)}^{\Lambda(1)} \left( x \right) + f_c \left( \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 \right) M_{A_i(\mathcal{N}_i)}^{\Lambda(2)} \left( x \right).
\]

(89)

After some calculations, the \( \kappa_\Lambda \) overall average number of the iterations to determine \( A_j \) is as

\[
\kappa_\Lambda = \sum_{i=1}^{n} \left( 1 - f_c \left( \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 \right) \right)^i \binom{n}{i} \frac{i-1}{i-1} \cdot \left( f_c \left( \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 \right) \right)^{i-1} + n \sum_{n-i+1}^{n} \binom{n}{i} \left( 1 - f_c \left( \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 \right) \right)^{i-1} \cdot \left( f_c \left( \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 \right) \right)^{n-i},
\]

(90)

Assuming the situation that the \( k \) available number of sub-channels is lower than the expected \( l \), the best \( l - k \) “bad” sub-channels with \( \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 < \frac{1}{l} \left| F \left( T_i^* (\mathcal{N}_i) \right) \right|^2 \), \( i = k, \ldots, l - 1 \) can be selected for transmission. This change is modeled via an extended \( \Lambda' \) operator that does modify the complexity and also leads to different functions and operators. Without loss of generality, if only \( k < l \) “good” sub-channels, \( \mathcal{G} = \{ \mathcal{N}_0, \ldots, \mathcal{N}_{k-1} \} \) are found and the
remaining \( l - k \) sub-channels are selected set \( B \) of the ordered coefficients, the \( f_{\Lambda, (\mathcal{N}_j)}^N \) CDF-function is as

\[
f_{\Lambda, (\mathcal{N}_j)}^N(x) = \Pr \left( \left| A_j (\mathcal{N}_j) \right|^2 < x \right) = \Pr(l) \Pr \left( \left| A_j (\mathcal{N}_j) \right|^2 < x \mid k \geq l \right) + \Pr \left( \left| A_j (\mathcal{N}_j) \right|^2 < x, k < l \right),
\] (91)

where \( \Pr(l) = \Pr\Lambda(l) = \Pr\Lambda_0(l) \).

Since at \( k \geq l, \left| A_j (\mathcal{N}_j) \right|^2 > \frac{1}{T} \sum_{t=0}^{l-1} F \left( T_t^* (\mathcal{N}_i) \right) \right| ^2 = \left| F \left( T_t^* (\mathcal{N}_i) \right) \right| ^2 \), it follows that

\[
\Pr \left( \left| A_j (\mathcal{N}_j) \right|^2 < x \mid k \geq l \right) = 1 - e^{-\frac{\left| \Gamma (\mathcal{N}_i) \right| \left| A_j (\mathcal{N}_j) \right| ^2}{\sum_{t=0}^{l-1} \left| F \left( T_t^* (\mathcal{N}_i) \right) \right| ^2}} \sum_{k=0}^{l-1} \frac{1}{k!} \left( x - \frac{\left| F \left( T_t^* (\mathcal{N}_i) \right) \right| ^2}{\left| A_j (\mathcal{N}_j) \right| ^2} \right)^k, \] (92)

while for \( k < l \) the corresponding relation for \( \Pr \Lambda, \left( \left| A_j (\mathcal{N}_j) \right|^2 < x, k < l \right) \) is

\[
\Pr \Lambda \left( \left| A_j (\mathcal{N}_j) \right|^2 < x, k < l \right) = \Pr \Lambda \left( \Gamma_1 + \Gamma_2 < x, \Gamma_2 < \frac{1}{T} \left| F \left( T_t^* (\mathcal{N}_i) \right) \right| ^2 \right), \] (93)

where \( \Gamma_1, \Gamma_2 \) were defined in (60) and (61), respectively, and

\[
\Pr \Lambda \left( \Gamma_1 + \Gamma_2 < x, \Gamma_2 < \frac{1}{T} \left| F \left( T_t^* (\mathcal{N}_i) \right) \right| ^2 \right) = \min \left( \left| \Gamma (\mathcal{N}_i) \right| \right) \int_0^x P_{\Gamma_2, \Gamma_1} (y, z) dz dy. \] (94)

After some calculations, the \( \kappa_{\Lambda} \) overall average number of the iterations at \( \Lambda \) is yielded as

\[
\kappa_{\Lambda} = \sum_{i=1}^{n} \left( \begin{array}{c} i - 1 \\hfill i - l \end{array} \right) \left( 1 - f_c \left( \frac{1}{T} \left| F \left( T_t^* (\mathcal{N}_i) \right) \right| ^2 \right) \right) \left( f_c \left( \frac{1}{T} \left| F \left( T_t^* (\mathcal{N}_i) \right) \right| ^2 \right) \right)^{i-l} + \sum_{k=0}^{l-1} \left( n + \sum_{l=1}^{k} (n - k - l) \right) \left( \begin{array}{c} n \\hfill k \end{array} \right) f_c \left( \frac{1}{T} \left| F \left( T_t^* (\mathcal{N}_i) \right) \right| ^2 \right)^{n-k} \left( 1 - f_c \left( \frac{1}{T} \left| F \left( T_t^* (\mathcal{N}_i) \right) \right| ^2 \right) \right)^{k}. \] (95)

The number of iterations at \( \Lambda_0 \) is \( \kappa_{\Lambda_0} = \mathcal{O}(n) \) for all values of \( \left| T_t^* (\mathcal{N}_i) \right| ^2 / \left| A_j (\mathcal{N}_j) \right| ^2 \). Increasing \( \left| T_t^* (\mathcal{N}_i) \right| ^2 / \left| A_j (\mathcal{N}_j) \right| ^2 \), \( \kappa_{\Lambda} \) converges from \( \mathcal{O}(l) \) to \( \mathcal{O}(n) \), while \( \kappa_{\Lambda} \) increases from \( \mathcal{O}(l) \) to \( \kappa_{\Lambda_0} \). The reason is that at \( \Lambda_0 \), all \( n \) sub-channels are scanned (no-progressive operator). Using \( \Lambda \), the progressive operator selects the first \( l \) sub-channels that requires a lower number of iterations. At \( \Lambda \), for low \( \left| T_t^* (\mathcal{N}_i) \right| ^2 / \left| A_j (\mathcal{N}_j) \right| ^2 \), the first \( l \)
sub-channels were selected, which results in $\kappa_{\mathcal{N}} \approx \kappa_{\Lambda} \approx \Theta(l)$, while as $\left| T'_i (\mathcal{N}_i) \right| / \left| A_j (\mathcal{N}_j) \right|$ increases, the iteration is extended to all $n$ sub-channels that yields $\kappa_{\mathcal{N}} \approx \Theta(n)$.

The proof is concluded here.

The values of parameter $\kappa$ from (81), (90), and (95) are compared in Figure 2.

### 3.4 Distribution of Gaussian subcarriers

**Proposition 2.** (Distribution of the Gaussian subcarriers). The (normalized) $\tilde{\vartheta}_i = \frac{1}{l} \left| d'_i \right|^2$ squared subcarrier magnitude is exponentially distributed, with single-carrier squared magnitude $\alpha_j (\mathcal{N}_j) = \sum_{i=0}^{l-1} \tilde{\vartheta}_i = \frac{1}{l} \sum_{i=0}^{l-1} \left| d'_i \right|^2$, where $d'_i \in \mathcal{CN} (0, \sigma^2_{\omega_0})$ is the noisy Gaussian subcarrier.

**Proof.** Let the output of $\mathcal{N}_i$ be the noisy Gaussian subcarrier $d'_i \in \mathcal{CN} (0, \sigma^2_{\omega_0})$. Then, the normalized random variable

$$\tilde{\vartheta}_i = \frac{1}{l} \left| d'_i \right|^2$$

is exponentially distributed with density

$$f (\tilde{\vartheta}_i) = \frac{1}{\sigma^2_{\tilde{\vartheta}_i}} e^{-\frac{\tilde{\vartheta}_i}{\sigma^2_{\tilde{\vartheta}_i}}}, \quad \tilde{\vartheta}_i \geq 0,$$

which can be rewritten as

$$f (x) = \frac{1}{\bar{\sigma}} e^{-\frac{x}{\bar{\sigma}}}, \quad x \geq 0,$$

where $\bar{\sigma}$ is the common mean.

The PDF of $P_T (x) = P_{\tilde{\vartheta}_i} (x) / f_{\tilde{\vartheta}_i} (\tilde{\vartheta}_i), 0 < x < \tilde{\vartheta}_i$ is evaluated as

$$P_T (x) = \frac{P_{\tilde{\vartheta}_i} (x)}{f_{\tilde{\vartheta}_i} (\tilde{\vartheta}_i)} = \frac{1}{\delta} e^{-\frac{x}{\delta}},$$

while $P_C (x) = P_{\tilde{\vartheta}_i} (x) / (f_{\tilde{\vartheta}_i} (\tilde{\vartheta}_i) - f_{\tilde{\vartheta}_i} (\delta)), \delta \leq x \leq \tilde{\vartheta}_i$ is expressed as

$$P_C (x) = \frac{P_{\tilde{\vartheta}_i} (x)}{f_{\tilde{\vartheta}_i} (\tilde{\vartheta}_i) - f_{\tilde{\vartheta}_i} (\delta)} = \frac{e^{-\frac{x}{\delta}}}{\bar{\sigma} \left( e^{-\frac{x}{\delta}} - e^{-\frac{\delta}{\sigma}} \right)}.$$
with an M-function
\[ M_\zeta(w) = \int_\delta P_\zeta(x) e^{ixw} dx = e^{i_\delta w_\delta} - e^{i_\delta w_{\delta/\delta}} \left( e^{-i_\delta} - e^{-i_\delta} \right) \left( 1 - w_\delta \right). \] (101)

Then, let \( \alpha_j(\mathcal{N}_j) \) be the averaged single-carrier squared magnitude as the sum of \( \partial_i \)'s, as
\[ \alpha_j(\mathcal{N}_j) = \sum_{i=0}^{l-1} \partial_i \]
\[ = \frac{1}{l} \sum_{i=0}^{l-1} |d'_i|^2, \] (102)
which can be rewritten as the sum of independent random variables as
\[ \alpha_j(\mathcal{N}_j) = \sum_{i=1}^{n} \sum_{k=i}^{n} x_k = x_1 + 2x_2 + \ldots + lx_l + lx_{l+1} + \ldots lx_n. \] (103)

Specifically, using (103), the M-function of a term \( kx_k \) is yielded as
\[ M_{kx_k}(w) = \int_0^\infty P_{kx_k}(x) e^{ixw} dx = \left( 1 - \frac{w_\delta}{h} \right)^{-1} \] (104)
and the M-function of \( \alpha_j(\mathcal{N}_j) \) is as
\[ M_{\alpha_j(\mathcal{N}_j)}(w) = \left( 1 - w_\delta \right)^{-l} \prod_{k=l+1}^{n} \left( 1 - \frac{w_\delta}{k} \right)^{-1}. \] (105)

Then, \( P_{\alpha_j(\mathcal{N}_j)}(x) \) is expressed as
\[ P_{\alpha_j(\mathcal{N}_j)}(x) = \frac{n!}{(n-l)!l!} \frac{e^{-x/l}}{x/l} \left( \frac{x^{l-1}}{\partial_i (l-1)!} + \frac{1}{\delta} \sum_{k=1}^{n-l} (-1)^{l+k-1} \right) \cdot \left( \frac{x}{\delta} - \sum_{m=i}^{l-2} \frac{1}{m!} \left( \frac{x}{l \delta} \right)^m \right). \] (106)

Particularly, at \( l - 1 \) total sub-channels, let us denote \( d'_i = \frac{1}{l} |d'_i|^2 \) the \( i \)th normalized Gaussian subcarrier. Then,
\[ P_{d'_i}(y) = \frac{1}{\delta} e^{y/x}, \quad x \geq y \] (107)
and the conditional PDF is as
\[
P_{\gamma_1|\gamma_2=y}(x) = P_{\sum_{i=0}^{l-2} \vartheta_i} (x) = \frac{1}{(l-2)!\vartheta^{l-1}} (x - (l - 1)y)^{(l-2)} e^{-\frac{x - (l-1)y}{\vartheta}}, x \geq (l - 1)y, \tag{108}
\]
where \(\Gamma_1 = \sum_{i=0}^{l-2} \vartheta_i, \Gamma_2 = \vartheta_{l-1}\), i.e., \(\vartheta\)'s are ordered such that \(\vartheta_0 \geq \ldots \geq \vartheta_{l-2} \geq \vartheta_{l-1}\), while
\[
M_{\vartheta_i} (w) = \int_0^{+\infty} P_{\vartheta_i} (y) e^{wy} dy
\]
\[
= \frac{1}{1 - w\vartheta} e^{wy},
\tag{109}
\]
and the M-function of \(\sum_{i=0}^{l-2} \vartheta_i\) is
\[
M_{\sum_{i=0}^{l-2} \vartheta_i} (w) = \left( M_{\vartheta_i} \right)^{l-1}
\]
\[
= \frac{1}{(1 - w\vartheta)^{l-1}} e^{(1-\text{Hex})w}. \tag{110}
\]
The joint PDF is
\[
P_{\gamma_1, \gamma_2} (x, y) = \frac{n!}{(n - l)! (l - 1)!} (f_c(x))^{n-l} \times (1 - f_c(x))^{l-1} P_c(x) P_{\sum_{i=0}^{l-2} \vartheta_i} (y) . \tag{111}
\]
where \(P_c(x)\) and \(f_c(x)\) are the common PDF and CDF of the unordered variables, while
\[
P_{\gamma_2} (x) = \frac{n!}{\delta (l - 1)!} \sum_{h=0}^{n-l} \frac{(-1)^h}{(n - l - h)!h!} e^{-\frac{\vartheta x}{\vartheta}} . \tag{112}
\]
Using (112), the joint PDF in (111) can be rewritten precisely as
\[
P_{\gamma_1, \gamma_2} (x, y) = \sum_{h=0}^{n-l} \frac{(-1)^h n!}{(n - l - h)! (l - 1)! (l - 2)!h!\vartheta} (y - (l - 1)x)^{(l-2)} e^{-\frac{x + h\vartheta}{\vartheta}}, x \geq 0, y \geq (l - 1)x. \tag{113}
\]
Note that by some fundamental theory,
\[
\lim_{x \to +\infty} \frac{1 - f_c(x)}{P_c(x)} = \Omega > 0 \tag{114}
\]
and
\[
\lim_{l \to +\infty} f_{\vartheta_i} (x) = e^{-x - \text{log} l}. \tag{115}
\]
Then, the \(x\) and \(p\) quadrature-level (single-carrier) error probability at \(\Lambda_0\) is as
\[
P_{\text{err}}(A_j) = \frac{1}{\pi} \int_{0}^{\frac{\pi}{2}} M_{A_j (\Lambda_0)} |_{\Lambda_0}^{\text{SNR}} \left( \frac{\sin^2 \left( \frac{x}{2} \right)}{\sin^2 \phi} \right) d\phi, \tag{116}
\]
where \(M_{A_j (\Lambda_0)} |_{\Lambda_0}^{\text{SNR}}\) is the M-function of \(A_j (\Lambda_j) |_{\text{SNR}} = \text{SNR}\); \(\text{SNR}\) is a scaled SNR quantity, \(\text{SNR} = \sigma_{\Lambda_0}^2 / \sigma_{\Lambda_j}^2\), and \(\phi \in [0, 2\pi]\). In particular, the formula of (116) can be applied to derive the \(p_{\text{err}}(A_j)\) error probabilities (single-carrier}
FIGURE 3  The $p_{\text{err}}^{\Lambda_0}(A_j)$ at $\Lambda_0$ via $M_{\Lambda_0}^{\Lambda_0} |A_j(N_j)|^2 \cdot \text{SNR}$ in function of $|A_j(N_j)|^2 \cdot \text{SNR}, T_i(N_i) \in \mathcal{CN} \left(0, \sigma^2_{T_i(N_i)} \right)$

FIGURE 4  The $p_{\text{err}}^{\Lambda}(A_j)$ and $p_{\text{err}}^{\Lambda'}(A_j)$ at $\Lambda$ and $\Lambda'$ via $M_{\Lambda}^{\Lambda} |A_j(N_j)|^2 \cdot \text{SNR}$ and $M_{\Lambda}^{\Lambda'} |A_j(N_j)|^2 \cdot \text{SNR}$ in function of $|A_j(N_j)|^2 \cdot \text{SNR}$, $T_i(N_i) \in \mathcal{CN} \left(0, \sigma^2_{T_i(N_i)} \right)$

quadrature level) of the operators using the M-functions proposed in Sections 3.1 and 3.2, precisely as

$$p_{\text{err}}^{\Lambda}(A_j) = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} M_{|A_j(N_j)|^2 \cdot \text{SNR}}^{\Lambda} \left( \frac{\sin^2 \left( \frac{\phi}{2} \right)}{\sin^2 \phi} \right) d\phi$$

and

$$p_{\text{err}}^{\Lambda'}(A_j) = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} M_{|A_j(N_j)|^2 \cdot \text{SNR}}^{\Lambda'} \left( \frac{\sin^2 \left( \frac{\phi}{2} \right)}{\sin^2 \phi} \right) d\phi.$$  

(117)

Specifically, assuming $T_i(N_i) \in \mathcal{CN} \left(0, \sigma^2_{T_i(N_i)} \right)$ and by using the M-functions derived in the previous sections, the corresponding $p_{\text{err}}^{\Lambda_0}(A_j)$ single-carrier quadrature level error probability at $\Lambda_0$ in function of $|A_j(N_j)|^2 \cdot \text{SNR}$ are yielded as shown in Figure 3. The results can be extended for arbitrarily distributed $T_i(N_i)$ coefficients.

Using operators $\Lambda$ and $\Lambda'$ with $M_{|A_j(N_j)|^2 \cdot \text{SNR}}^{\Lambda}$ and $M_{|A_j(N_j)|^2 \cdot \text{SNR}}^{\Lambda'}$, the complexity can be reduced; however, the yielding single-carrier quadrature level error probabilities $p_{\text{err}}^{\Lambda}(A_j)$ and $p_{\text{err}}^{\Lambda'}(A_j)$ are slightly increased, as depicted in Figure 4.

The $p_{\text{err}}^{\Lambda'}(A_j)$ approximately coincidences with $p_{\text{err}}^{\Lambda_0}(A_j)$ because both operators find $l$ sub-channels; however, the threshold differs that leads to $p_{\text{err}}^{\Lambda'}(A_j) \geq p_{\text{err}}^{\Lambda_0}(A_j)$. In comparison to $\Lambda$, $p_{\text{err}}^{\Lambda}(A_j) \geq p_{\text{err}}^{\Lambda'}(A_j)$ because operator $\Lambda'$ always determines the required number $l$ of the sub-channels at a given threshold. It leads to the final conclusion $p_{\text{err}}^{\Lambda_0}(A_j) \leq p_{\text{err}}^{\Lambda'}(A_j) \leq p_{\text{err}}^{\Lambda}(A_j)$.
4 | RANDOM MATRIX FORMALISM OF MULTICARRIER CVQKD

First, we summarize the basic functions and random matrix tools in Propositions 3 and 4, to evaluate the results in Theorem 3 and Lemma 1. The proofs throughout Section 4 follow the notations of and. For the detailed description of the AMQD-MQA multiple-access multicarrier CKQKD scheme, see.

4.1 | Multiuser quadrature allocation for multicarrier CVQKD

**Proposition 3.** (Random matrix decomposition of $F(T(N))$ of $K$ users.) At $l$ Gaussian sub-channels and $K$ users, the $l \times K$ channel matrix $F(T(N))$ of $K$ users can be decomposed as $F(T(N)) = XZ\Phi$, where $Z$ is an $l \times K$ random matrix, $X$ is an $l \times l$ random matrix, while $\Phi$ is a $K \times K$ random matrix.

Proof. Let the $Z_{i,j}$ entries of $Z$ be independent, arbitrarily distributed complex random variables with identical mean $\mu_{i,j} = \mu$ and variance $\sigma_{i,j}^2 = 1/l$ such that the Lindeberg condition is satisfied, where $P$ is a probability measure function that returns an event’s probability.

Let $X$ be an $l \times l$ random matrix, while $\Phi$ is a $K \times K$ random matrix, independent from each other and from $Z$.

Without loss of generality, let the logical channel $M_k$ of user $U_k$ be defined as

$M_k = \{N_0, \ldots, N_{m-1}\}.$

The single-carrier transmittance coefficient of $M_k$ is referred to as $A_j(M_k)$.

Particularly, then, for $K, l \to \infty$ and $K/l \to \chi$, where $\chi$ is a nonnegative variable, for the $\eta$-transform of $F(T(N))F(T(N))^\dagger$,

$$\eta_{F(T(N))F(T(N))}^\dagger(D, \gamma) = \mathbb{E} \left[ V_{F(T(N))F(T(N))}^\dagger(D, \gamma) \right],$$

where $D \in D_{\{XX\}^\dagger}$ is an independent random variable with a distribution $D_{\{XX\}^\dagger}$ of the asymptotic spectra of $XX^\dagger$, and

$$V_{F(T(N))F(T(N))}^\dagger(D, \gamma) = \frac{1}{1 + \gamma \mathbb{D} \mathbb{E} \left[ \frac{T}{1 + \gamma \mathbb{D} \mathbb{E} \left[ \frac{TV_{F(T(N))F(T(N))}^\dagger(D,\tau) \right] } \right]},$$

where $T \in D_{\{\Phi\}^\dagger}$ is an independent random variable with a distribution of the asymptotic spectra of $\Phi\Phi^\dagger$.

The $\nu$-transform (Shannon transform) of a nonnegative random variable $X$ is defined as

$$\nu_X(\gamma) = \mathbb{E} \left[ \log_2 (1 + \gamma X) \right],$$

where $\gamma$ is a nonnegative real number.

Let the $\nu$-transform of $F(T(N))F(T(N))^\dagger$ is as

$$\nu_{F(T(N))F(T(N))}^\dagger(\gamma) = \nu_{XX}^\dagger(\chi d) + \chi \nu_{\Phi\Phi}^\dagger(\gamma) - \chi \frac{y_d}{\gamma} \log_2 e,$$
where $\gamma_d$ and $\gamma_t$ are random variables such that

\[
\frac{\gamma_d \gamma_t}{\gamma} = 1 - \eta_{\Phi \Phi'} (\gamma_t)
\]  

(126)

and

\[
\frac{\chi \gamma_d \gamma_t}{\gamma} = 1 - \eta_{\text{XX'}} (\chi \gamma_d).
\]  

(127)

Note that by denoting $\gamma_d (\gamma)$ the solution for (126) and (127), the result in (122) can be rewritten as

\[
\eta_{F(T(N'))F(T(N'))} = \eta_{\text{XX'} (\chi \gamma_d (\gamma))}.
\]  

(128)

Throughout the manuscript, let $X$ and $Y$ be defined as independent random variables $X \in U_{[0,1]}$ and $Y \in U_{[0,1]}$ drawn from a $U'$ uniform distribution on $[0,1]$. Specifically, the decomposition of $F (T (N')) = XZ \Phi$ with a $j$th column $F (T (N'))_j$ allows us to define a function $H^{(0)} (a, \gamma)$, $(j - 1) / K \leq a < j / K$, where $a$ is a random variable, precisely as

\[
H^{(0)} (a, \gamma) = \frac{1}{\left[ F(T(N'))_j \right]^2} \left[ I + \gamma \sum_{k \neq j} F(T(N'))_k F(T(N'))_k^T \right]^{-1} F(T(N'))_j.
\]  

(129)

where $I$ is the identity, such that for $K, l \to \infty$, and $a \in [0, 1]

\[
H^{(0)} (a, \gamma) \to \frac{\gamma_t (\gamma)}{\gamma \mathbb{E} [D]},
\]  

(130)

where for $\gamma_t (\gamma)$, the result of (126) and (127) holds and $H^{(0)}$ converges to

\[
\frac{H (a, \gamma)}{\mathbb{E} [B(X, a)]},
\]  

(131)

where $B (\cdot)$ is a limiting bounded measurable function, and $H (a, \gamma)$ is evaluated as

\[
H (a, \gamma) = \mathbb{E} \left[ \frac{1}{B(X, a)} \frac{1}{1 + \gamma \mathbb{E} \left[ B(X, Y) \frac{1}{1 + \gamma H(X, Y)} \right] X} \right].
\]  

(132)

Without loss of generality, the entries of $XZ \Phi$ are independent, arbitrarily distributed zero-mean ($\mu_{ij} = 0$) complex random variables with variance

\[
\sigma_{ij}^2 = \frac{\Pi_{ij}}{T},
\]  

(133)

where $\Pi$ is an $I \times K$ deterministic matrix with uniformly bounded $(i, j)$ entries, with variance profile $\text{var} (a, b)$. Let $\text{var}^l (\cdot)$ be the variance profile function as

\[
\text{var}^l : [0, 1) \times [0, 1) \to \mathbb{R},
\]  

(134)

such that for $\frac{l-1}{I} \leq a < \frac{l}{I}$ and $\frac{l-1}{K} \leq b < \frac{l}{K}$,

\[
\text{var}^l (a, b) = \Pi_{ij},
\]  

(135)

Particularly, if $\text{var}^l (a, b)$ converges uniformly to a limiting bounded measurable function $B (a, b) = \text{var} (a, b)$, then the limit

\[
\text{var}^l (a, b) \to B (a, b) = \text{var} (a, b)
\]  

is the asymptotic variance profile\footnote{Assumption} of $F (T (N'))$. In this case, (132) can be expressed as

\[
\frac{H (a, \gamma)}{\mathbb{E} [B(X, a)]} = \mathbb{E} \left[ \frac{1}{\text{var} (X, a)} \frac{1}{1 + \gamma \mathbb{E} \left[ \text{var} (X, Y) \frac{1}{1 + \gamma H(X, Y)} \right] X} \right].
\]  

(137)
Then, let us presume that for these entries the condition of

$$\frac{1}{K} \sum_{i,j} \int_{\{|F(T(N))_{i,j}| > \delta\}} \|F(T(N))_{i,j}\|^2 dP = 0$$  \hspace{1cm} (138)

is satisfied,\(^2\) where \(F(T(N))_{i,j}\) stands for the \((i,j)\)th entry of \(F(T(N))\).

Precisely, if for the entries of \(F(T(N))\), the conditions (133) and (138) are satisfied, then for \(K, l \to \infty\), and \(K / l \to \chi\), then for independent random variables \(X \in U_{[0,1]}\) and \(Y \in U_{[0,1]}\) drawn from a \(U\) uniform distribution on \([0,1]\),

$$\eta_{F(T(N))F(T(N))}(\gamma) = \mathbb{E} \left[ W_{F(T(N))F(T(N))}(X, \gamma) \right],$$ \hspace{1cm} (139)

where

$$W_{F(T(N))F(T(N))}(a, \gamma) = \frac{1}{1 + \gamma \mathbb{E} \left[ \text{var}(X, Y) Y_{F(T(N))F(T(N))}(Y, \gamma) \right]}.$$ \hspace{1cm} (140)

and

$$Y_{F(T(N))F(T(N))}(b, \gamma) = \frac{1}{1 + \gamma \mathbb{E} \left[ \text{var}(X, b) \Gamma_{F(T(N))F(T(N))}(X, \gamma) \right]}.$$ \hspace{1cm} (141)

Note that it is precisely a coincidence with the \(\eta\)-transform of the empirical (squared) eigenvalue distribution of \(F(T(N))\) \(F(T(N))\)^\dagger at \(K, l \to \infty\) and \(K / l \to \chi\).

In particular, if for the entries of \(F(T(N))\) the conditions (133) and (138) are satisfied, and \(W_{F(T(N))F(T(N))}(a, \gamma)\) and \(Y_{F(T(N))F(T(N))}(b, \gamma)\) are given as (140) and (141), respectively, then the \(\nu\)-transform of \(F(T(N))\) \(F(T(N))\)^\dagger can be rewritten as

$$\nu_{F(T(N))F(T(N))}(\gamma) = \chi \mathbb{E} \left[ \log_2 \left( 1 + \gamma \mathbb{E} \left[ \text{var}(X, Y) W_{F(T(N))F(T(N))}(X, \gamma) \right] \right) \right]$$

$$+ \mathbb{E} \left[ \log_2 \left( 1 + \gamma \mathbb{E} \left[ \text{var}(X, Y) Y_{F(T(N))F(T(N))}(Y, \gamma) \right] \right) \right]$$

$$- \gamma \mathbb{E} \left[ \text{var}(X, Y) \Gamma_{F(T(N))F(T(N))}(X, \gamma) \right] \log_2 e.$$ \hspace{1cm} (142)

Specifically, further note that for

$$\chi' = \chi \frac{P \left( \mathbb{E} \left[ \text{var}(X, Y) | Y \right] \not= 0 \right)}{P \left( \mathbb{E} \left[ \text{var}(X, Y) | X \right] \not= 0 \right)},$$ \hspace{1cm} (143)

the following limit holds:

$$\tau_\infty = \lim_{\gamma \to \infty} \left( \log_2 (\gamma \chi) - \frac{\nu_{F(T(N))F(T(N))}(\gamma)}{\min (\chi P \left( \mathbb{E} \left[ \text{var}(X, Y) | Y \right] \not= 0 \right), P \left( \mathbb{E} \left[ \text{var}(X, Y) | X \right] \not= 0 \right))} \right),$$ \hspace{1cm} (144)

where \(\tau_\infty\) depends on \(\chi'\). Precisely, \(\tau_\infty\) differs for \(\chi' < 1, \chi' = 1\) and \(\chi' > 1\), as

$$\tau_{\infty, \chi' < 1} = -\mathbb{E} \left[ \log_2 \frac{\Gamma_{\infty}(Y')}{\delta} - \frac{1}{\chi} \mathbb{E} \left[ \log_2 \left( 1 + \mathbb{E} \left[ \frac{\text{var}(X', Y')}{W_{\infty}(Y')} \right] \right) \right] \right],$$ \hspace{1cm} (145)

where \(W_{\infty}(\cdot)\) is yielded from

$$\mathbb{E} \left[ \frac{1}{1 + \mathbb{E} \left[ \frac{\text{var}(X', Y')}{W_{\infty}(Y')} \right] X'} \right] = 1 - \chi',$$ \hspace{1cm} (146)

while

$$\tau_{\infty, \chi' = 1} = -\mathbb{E} \left[ \log_2 \frac{\text{var}(X', Y')}{\delta} \right],$$ \hspace{1cm} (147)
and
\[
\tau_{\infty, \chi' > 1} = -\mathbb{E} \left[ \log_2 \left( \frac{1}{e} \mathbb{E} \left[ \frac{\text{var} (X', Y')} {1 + \varphi (Y')} X' \right] \right) \right] - \chi' \mathbb{E} \left[ \log_2 (1 + \varphi (Y')) \right],
\]

(148)
where \( \varphi (\cdot) \) is yielded from
\[
\varphi (b) = \frac{1}{\chi'} \mathbb{E} \left[ \frac{\text{var} (X', b)} {1 + \varphi (X')} X' \right].
\]

(149)

Precisely, the asymptotic theory of singular values of rectangular matrices assumes the existence of an \( l \times K \) matrix \( M \), for which the aspect ratio converges to a nonnegative variable \( \chi \),
\[
\frac{K}{l} \to \chi,
\]

(150)
as \( K, l \to \infty \).

**Proposition 4.** (Channel profile of the \( l \times K \) channel matrix \( F (T (\mathcal{N})) = XZ\Phi \) of \( K \) users.) The \( \rho_{F(T(\mathcal{N}))}(a, b) : [0, 1]^2 \to \mathbb{R} \) function is the channel profile of \( F (T (\mathcal{N})) \), if for \( X \in U_{[0,1]} \) and \( Y \in U_{[0,1]} \), \( D_{F(\mathcal{N})}(a, Y) = D_{\Phi}(\cdot) \) and \( D_{F(\mathcal{N})}(a, b) = D_{\Phi}(\cdot) \) where \( D_{\Phi}(\cdot) \) is the distribution of \( \rho_{F(T(\mathcal{N}))}(a, b) \), while \( F_a (\cdot) \) and \( F_b (\cdot) \) are nonrandom limits.

**Proof.** Without loss of generality, let the \( l \times K \) channel matrix of \( K \) users be given as \( F (T (\mathcal{N})) \). Focusing on the case that \( Z \) has arbitrarily distributed, \( Z_{i,j} \) zero-mean complex random variables with \( \sigma^2_{Z_{i,j}} = 1 / l \), for a given \( \Omega, \Lambda \geq 0 \) there exist a channel profile function for \( F (T (\mathcal{N})) \) as
\[
\rho_{F(T(\mathcal{N}))}(a, b) : [0, 1]^2 \to \mathbb{R},
\]

(151)
such that if \( X \in U_{[0,1]} \), then without loss of generality, the following relation holds for the \( D \) distribution of \( \rho_{F(T(\mathcal{N}))}(a, b) \):
\[
D_{\rho_{F(T(\mathcal{N}))}(a, Y)} = F_{\Phi} (\cdot),
\]

(152)
while if \( Y \in U_{[0,1]} \), then
\[
D_{\rho_{F(T(\mathcal{N}))}(a, Y)} = F_a (\cdot),
\]

(153)
where the nonrandom limits \( F_a (\cdot) \), \( F_b (\cdot) \) for a given \( a, b \in [0, 1] \) have all bounded moments.

Then, it can be shown that, if \( F (T (\mathcal{N})) = Z\Phi \), then \( \phi \) stands for the Hadamard product, then for \( K, l \to \infty \) and \( K / l \to \chi \), then for independent random variables \( X \in U_{[0,1]} \) and \( Y \in U_{[0,1]} \) the following coincidence holds:
\[
\rho_{F(T(\mathcal{N}))}(X, Y) = \text{var} (X, Y),
\]

(154)

**Theorem 3.** (Random matrix formalism of multiple-access multicarrier CVQKD). The random matrix decomposition of the \( l \times K \) channel matrix \( F (T (\mathcal{N})) \) of the \( K \) users is \( F (T (\mathcal{N})) = XZ\Phi \), where \( X \) is an \( l \times K \) random matrix \( X = (X_0, \ldots, X_{K-1}) \), with \( X_i = [A_{i,0}, \ldots, A_{i,k}]^T \) for user \( U_k \), where \( A_{i,k} = \frac{1}{m} \sum_{t=0}^{m-1} F (T_i (\mathcal{N}_t)) \) is the averaged transmittance coefficients of \( U_k \) derived by operator \( \Lambda_0, \Lambda, \) or \( \Lambda', \) \( Z = (\Theta_0, \ldots, \Theta_{K-1}) \) is an \( l \times K \) random matrix, \( \Theta_k = [\Theta_{k,0}, \ldots, \Theta_{k,l-1}]^T \) is user \( U_k \)’s entry, \( m \) is the number of sub-channels of \( U_k \), \( \circ \) is the Hadamard product, while \( \Phi \) is an \( l \times K \) random matrix, \( \Phi = \text{diag} (\Phi_0, \ldots, \Phi_{K-1}) \).

**Proof.** Let the number of the users be \( k \leq K \). The transmission of the users is realized through \( l \) sub-channels, such that for each \( U_k \) user, a given number \( (m) \) of sub-channels are allocated. The transmittance coefficient statistics of the users are determined via operators \( \Lambda_0, \Lambda, \) and \( \Lambda', \) see Theorem 1. The derivation also utilizes the random matrix formulas introduced in Propositions 2 and 3, respectively. The proof utilizes the terms and notations of.

Let the \( l \times K \) channel matrix \( F (T (\mathcal{N})) \) of \( K \) users be given as
\[
F (T (\mathcal{N})) = XZ\Phi,
\]

(155)
where $\circ$ is the Hadamard (element-wise) product, and
\[ Z = (\Theta_0, \ldots, \Theta_{K-1}) \quad (156) \]
is an $l \times K$ random matrix with zero-mean and $\sigma_Z^2 = 1/l$ variance entries, where
\[ \Theta_k = [\Theta_{k,0}, \ldots, \Theta_{k,l-1}]^T \quad (157) \]
is user $U_k$’s entry, $X$ is an $l \times K$ random matrix with independent entries for the users, such that
\[ X = (\mathcal{X}_0, \ldots, \mathcal{X}_{K-1}) \quad (158) \]
where for user $U_k$
\[ \mathcal{X}_k = [A^{(k)}_{j,0}, \ldots, A^{(k)}_{j,l-1}]^T \quad (159) \]
is the averaged transmittance coefficients of $U_k$ derived via a corresponding distribution statistics operator (see Theorems 1 and 2), $m$ is the number of sub-channels of $U_k$, while $\Phi$ is a $l \times K$ random matrix,
\[ \Phi = \text{diag}(\Phi_0, \ldots, \Phi_{K-1}) \quad (161) \]

Specifically, for user $U_k$, let us identify $\mathcal{M}_k$ the logical channel (a set of $m$ sub-channels) of $U_k$ of the $k$th column of $F(T(\mathcal{N})) = (\mathcal{M}_0, \ldots, \mathcal{M}_{K-1})^T$ such that
\[ \mathcal{M}_k = [\mathcal{M}^{(0)}_k, \ldots, \mathcal{M}^{(l)}_k]^T \quad (162) \]
where $\mathcal{M}^{(l)}_k$ identifies the $i$th logical sub-channel of $U_k$ such that
\[ \mathcal{M}^{(l)}_k = \Phi_k A^{(k)}_{j,l} \Theta_{k,i}. \quad (163) \]

Let $r$ be a nonnegative variable that identify the ratio of the sub-channels allocated to the logical channel $\mathcal{M}_k$ of $U_k$, as
\[ r = \frac{m}{l} \quad (164) \]
where $0 \leq r \leq 1$.

Using (155), the $Y$ output matrix of the $K$ users can be written as
\[ Y = F(T(\mathcal{N}))X + F(\Delta^{(K)}) \]
\[ = (X \circ Z \Phi)X + F(\Delta^{(K)}) \quad (165) \]
where $X$ refers to the input matrix of the $K$ users while $F(\Delta^{(K)})$ is the Fourier transformed matrix of the $\Delta^{(K)}$ noise matrix of the $K$ users.

Let us utilize the results of Propositions 3 and 4 for $K, l \to \infty$ and $K/l \to \chi$, where $\chi$ is a nonnegative variable. Let $\eta_{U_k}$ be transmission efficiency of $U_k$ in function of the $\text{SNR}_{U_k}^+$ (evaluated for the transmission of private classical information, see$^{38,82}$) is as
\[ \lim_{K \to \infty} \eta_{U_k}(\text{SNR}_{U_k}^+) = \mathbb{E}
\left[\frac{F(h, \text{SNR}_{U_k}^+)}{\rho_\theta(X, b)}\right]. \quad (166) \]
where \( \rho_\theta (X, b) \) is the two-dimensional profile function of the \( l \times K \) matrix \( \theta \) and where an \( (r, t) \) entry of \( \theta \) is

\[
\theta_{r, t} = A_{j, t} \Phi_t, \tag{167}
\]

which identifies the \( r \)th logical sub-channel of the \( t \)th user, \(^92\) and let

\[
b = \frac{k}{K}, \tag{168}
\]

where \( 0 \leq b \leq 1 \), and \( X \in U_{[0,1]} \) and \( Y \in U_{[0,1]} \).

The SNR*, of \( U_k \) is as

\[
\text{SNR}^*_U = \sum_{i=0}^{m-1} \text{SNR}^*_i = \sum_{i=0}^{m-1} \sigma^2_{X_i} \tag{169}
\]

where \( m \) is the number of Gaussian subcarrier CVs allocated to \( U_k \), \( \sigma^2_{X_i} \) is the constant subcarrier modulation variance, while \( \sigma^2_{X_i} \) is expressed precisely as

\[
\sigma^2_{X_i} = \sigma^2_0 + N_i, \tag{171}
\]

where \( \sigma^2_0 \) is the vacuum noise and \( N_i \) is the excess noise of the Gaussian sub-channel \( \mathcal{N}_i \) defined as

\[
N_i = \frac{(W_i - 1) \left( \left| F (T_{\text{Eve}, i}) \right|^2 \right)}{1 - \left| F (T_{\text{Eve}, i}) \right|^2}, \tag{172}
\]

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

\[
|T_{\text{Eve}, i}|^2 = 1 - |T_i|^2 \tag{173}
\]

is the transmittance of Eve’s beam splitter (BS), while \( |T_i|^2 \) is the transmittance of \( \mathcal{N}_i \), while function \( F (b, \text{SNR}^*_U) \) is yielded as

\[
F (b, \text{SNR}^*_U) = \mathbb{E} \left[ \frac{\rho_\theta (X, b)}{1 + \text{SNR}^*_U \mathbb{E} \left[ \frac{\rho_\theta (X, Y)}{1 + \text{SNR}^*_U \mathbb{E} \left[ \psi (X, \text{SNR}^*_U) \right]} X \right]} \right]. \tag{174}
\]

Particularly, the result in (174) can be rewritten as

\[
F (b, \text{SNR}^*_U) = \mathbb{E} \left[ \rho_\theta (X, b) \psi (X, \text{SNR}^*_U) \right]. \tag{175}
\]

where function \( \psi (X, \text{SNR}^*_U) \) is as

\[
\psi (X, \text{SNR}^*_U) = \frac{1}{1 + \text{SNR}^*_U \mathbb{E} \left[ \frac{\rho_\theta (X, Y)}{1 + \text{SNR}^*_U \mathbb{E} \left[ \psi (X, \text{SNR}^*_U) \rho_\theta (X, Y) \right]} Y \right]} \tag{176}
\]
Then, let us assume that for $\rho_\theta (a, b)$, the following relation holds:

$$\rho_\theta (a, b) \approx |\Phi_k|^2 |A_{j,i}^{(k)}|^2,$$

where $(i-1)/l \leq a < i/l$, and $(k-1)/K \leq b < k/K$. Specifically, in this case, $\eta_{U_k} (\text{SNR}^*_U)$ is yielded as

$$\eta_{U_k} (\text{SNR}^*_U) = \frac{\varphi_k (\text{SNR}^*_U)}{|A_{j,i}^{(k)}|^2} = \frac{1}{m} \sum_{i=0}^{m-1} F (T_i (N_i)),$$

where $m$ identifies the number of sub-channels of $U_k$ used in the transmission, that is, for the remaining $l - k$ sub-channels, $|F (T_i (N_i))|^2 = 0$ and $\varphi_k (\text{SNR}^*_U)$ is expressed as

$$\varphi_k (\text{SNR}^*_U) = \frac{1}{l} \sum_{r=0}^{l-1} \frac{|A_{r,k}^{(k)}|^2}{1 + \text{SNR}^*_U \sum_{h=0}^{K-1} \frac{|\Phi_h|}{\sum_{k=0}^{m-1} \text{SNR}^*_U |\Phi_k|} F (T_i (N_i))},$$

where $(r, k)$ identifies the $r$th subcarrier of user $U_k$.

Using (178), an $f_{\text{eff}} (\cdot)$ efficiency function is introduced as

$$f_{\text{eff}} (\chi, \text{SNR}^*_U) = \chi^E \left[ \log_2 \left( 1 + \text{SNR}^*_U \frac{F (Y, \text{SNR}^*_U)}{F (Y)} \right) \right],$$

where $F (\cdot)$ is derived via (174).

Using Proposition 2, let

$$P (\mathbb{E} [\rho_\theta (X, Y) | Y] > 0) \leq P (\mathbb{E} [\rho_\theta (X, Y) | X] > 0) < 1.$$ 

If (181) holds, then without loss of generality,

$$f_{\text{eff}} (\chi, \text{SNR}^*_U) = \chi^E \left[ \log_2 \left( 1 + \text{SNR}^*_U \frac{F (Y, \text{SNR}^*_U)}{F (Y)} \right) \right],$$

and if $\text{SNR}^*_U \to \infty$ also holds, then

$$F (b, \text{SNR}^*_U) \to \mathbb{E} \left[ \frac{\rho_\theta (X, b)}{1 + \chi^E \left[ \frac{\rho_\theta (X, b)}{F (Y)} X \right]} \right].$$

Specifically, using (180), the $P_{\text{sym}} (\mathcal{M}_k)$ symmetric private classical capacity (the maximum common rate at which the $K$ users both can reliably transmit private classical information over the $l$ sub-channels of $\mathcal{N}$) of the $\mathcal{M}_k$ logical channel of $U_k$ is expressed as follows:
\[ P_{\text{sym}}(M_k) = \frac{1}{K} \left( f_{\text{eff}} \left( \chi \sum_{i=0}^{l-1} \text{SNR}_i^* \right) \right) \]

\[ + \mathbb{E} \left[ \log_2 \left( 1 + \sum_{i=0}^{l-1} \text{SNR}_i^* \mathbb{E} \left[ \rho_0(X, Y) Y \left( Y, \sum_{i=0}^{l-1} \text{SNR}_i^* \right) \mid X \right] \right) \right] \]

\[ - \chi \sum_{i=0}^{l-1} \text{SNR}_i^* \mathbb{E} \left[ \mathcal{F} \left( Y, \sum_{i=0}^{l-1} \text{SNR}_i^* \right) Y \left( Y, \sum_{i=0}^{l-1} \text{SNR}_i^* \right) \right] \log_2 e \]

\[ = \frac{1}{K} \left( f_{\text{eff}} \left( \chi \sum_{i=0}^{l-1} \text{SNR}_i^* \right) \right) + \mathbb{E} \left[ \log_2 \left( \frac{1}{\psi(X, \sum_{i=0}^{l-1} \text{SNR}_i^*)} \right) \right] \]

\[ + \left( \mathbb{E} \left[ \psi \left( X, \sum_{i=0}^{l-1} \text{SNR}_i^* \right) \right] - 1 \right) \log_2 e , \tag{184} \]

where $\sum_{i=0}^{l-1} \text{SNR}_i^*$ is the total SNRs of the $l$ Gaussian sub-channels evaluated for the transmission of private classical information expressed as $\sum_{i=0}^{l-1} \text{SNR}_i^* = \sum_{i=0}^{l-1} \sigma_i^2 / \sigma_{X_i^*}^2$, where $\sigma_{X_i^*}^2$ is shown in (170), $X \in \mathcal{U}_{[0,1]}$ and $Y \in \mathcal{U}_{[0,1]}$, and

\[ \mathcal{F} \left( b, \sum_{i=0}^{l-1} \text{SNR}_i^* \right) = \mathbb{E} \left[ \frac{\rho_0(X, b)}{1 + \chi \sum_{i=0}^{l-1} \text{SNR}_i^* \mathbb{E} \left[ \rho_0(X, Y) Y \left( Y, \sum_{i=0}^{l-1} \text{SNR}_i^* \right) \mid X \right] \right] \right], \tag{185} \]

and function $\psi(\cdot)$ is as

\[ \psi \left( b, \sum_{i=0}^{l-1} \text{SNR}_i^* \right) = \frac{1}{1 + \sum_{i=0}^{l-1} \text{SNR}_i^* \mathcal{F} \left( b, \sum_{i=0}^{l-1} \text{SNR}_i^* \right)} . \tag{186} \]

In particular, defining function $\mathcal{E} \left( b, \sum_{i=0}^{l-1} \text{SNR}_i^* \right)$ precisely as

\[ \mathcal{E} \left( b, \sum_{i=0}^{l-1} \text{SNR}_i^* \right) = \mathbb{E} \left[ \frac{\rho_0(X, b)}{1 + \sum_{i=0}^{l-1} \text{SNR}_i^* \mathbb{E} \left[ \rho_0(X, Z) \frac{1}{1 + \sum_{i=0}^{l-1} \text{SNR}_i^* \mathcal{E} \left( Z, \sum_{i=0}^{l-1} \text{SNR}_i^* \right)} \mid X \right] \right] \right], \tag{187} \]

where $Z \in \mathcal{U}_{[b,1]}$ is an independent random variable, drawn from a $\mathcal{U}^*$ uniform distribution on $[b,1]$, the formula of (184) can be rewritten in a simplified form specifically as

\[ P_{\text{sym}}(M_k) = \frac{1}{K} \chi \mathbb{E} \left[ \log_2 \left( 1 + \sum_{i=0}^{l-1} \text{SNR}_i^* \mathcal{E} \left( Y, \sum_{i=0}^{l-1} \text{SNR}_i^* \right) \right) \right] . \tag{188} \]
The $P_{sym}(\mathcal{M}_k)$ of $U_k$ in function of SNR$^*_k$, for $0 \leq r \leq 1$, where SNR$^*_k$ is the SNR for the transmission of private classical information over the $\mathcal{M}_k$ logical channel of $U_k$, via $m$ Gaussian sub-channels; $r = m/l$ identifies the ratio of the sub-channels allocated to $U_k$.

From (188), the $S_{sym}(U_k)$ symmetric secret key rate (a common rate at which the $K$ users both can reliably transmit private classical information over the $l$ sub-channels of $U_k$) is as

$$S_{sym}(U_k) \leq \frac{1}{K} \mathbb{E} \left[ \log_2 \left( 1 + \sum_{i=0}^{l-1} \text{SNR}^*_i \left( Y, \sum_{i=0}^{l-1} \text{SNR}^*_i \right) \right) \right].$$

(189)

The proof is concluded here. \hfill \Box

The $P_{sym}(\mathcal{M}_k)$ of $U_k$ from (188) in function of $r$ is depicted in Figure 5.

4.2 Multiuser transmission over identical Gaussian sub-channels

**Lemma 1.** (Random matrix formalism of multiple-access multicarrier CVQKD for identically allocated sub-channels). Let us set $\mathcal{S} = \{\mathcal{N}_i\}, i = 0, \ldots, h-1, h \leq l$, refer to the sub-channels of the $1 \leq k \leq K \leq l$ users, obtained via $\Lambda_0, \Lambda, \Lambda'$. The random matrix decomposition of the $h \times K$ channel matrix $F(T(\mathcal{N}))$ is $F(T(\mathcal{N})) = XU\Phi$, where $U = (u_0, \ldots, u_{K-1})$ is an $h \times K$ isotropic unitary matrix, independent of $X$ and $\Phi$, $UU^\dagger = I$, with arbitrarily distributed random variables such that the Lindeberg condition (see (119)) is satisfied, with mean $\mu_{i,j} = \mu$ and variance $\sigma_{i,j}^2 = 1/l$.

The transmittance coefficients are determined via operators $\Lambda_0, \Lambda, \Lambda'$ (see Theorem 1). The proof utilizes the terms and notations of.

The random matrix decomposition of the $h \times K$ channel matrix $F(T(\mathcal{N}))$ is

$$F(T(\mathcal{N})) = XU\Phi,$$

(191)

where

$$U = (u_0, \ldots, u_{K-1})$$

(192)

is an $h \times K$ isotropic unitary matrix, independent of $X$ and $\Phi$, $UU^\dagger = I$, with arbitrarily distributed random variables such that the Lindeberg condition (see (119)) is satisfied, with mean $\mu_{i,j} = \mu$ and variance $\sigma_{i,j}^2 = 1/l$.

$$u_k = [q_{k,0}, \ldots, q_{k,h-1}]^T,$$

(193)
X is an $h \times h$ random matrix
\[
X = \text{diag}(\mathcal{X}_0, \ldots, \mathcal{X}_{h-1}) ,
\]  
(194)
where
\[
\mathcal{X}_k = \begin{bmatrix} A_{j,0}^{(k)} & \cdots & A_{j,h-1}^{(k)} \end{bmatrix}^T ,
\]
(195)
and
\[
A_{j}^{(k)} = \frac{1}{h} \sum_{i=0}^{h-1} F(T_i(N_i))
\]
(196)
is the averaged transmittance coefficients of $U_k$ taken over $S$, such that
\[
\mathcal{X}_i = \mathcal{X}_k ,
\]
(197)
for $i = 0, \ldots, K - 1$, while $\Phi$ is a $K \times K$ random matrix,
\[
\Phi = (\Phi_0, \ldots, \Phi_{K-1}) .
\]
(198)

Precisely, if the users transmit through the same subcarriers, then for all $U_i$, $i = 0, \ldots, k - 1$ users, an identical $\mathcal{M}_{U_i} = \mathcal{M}_k$ logical channel is allocated, see (197); thus, (194) can be rewritten as
\[
X = \text{diag}(\mathcal{X}_k) ,
\]
(199)
with the averaged coefficient of (196) for the $h$ sub-channels of user $U_k$.

Particularly, since all users use the same Gaussian sub-channels, the empirical distribution of $XX^\dagger$ converges to a nonrandom limit $F_{|C|^2}$, thus
\[
D_{XX^\dagger} \xrightarrow{\text{dist}} F_{|C|^2} ,
\]
(200)
where $|C|$ is a random variable having a distribution of the asymptotic singular value distribution of the singular values of $X$, ie, the distribution of $|C|^2$ is determined by the asymptotic spectra of $XX^\dagger$, thus without loss of generality
\[
|C| = |A_j(M_k)| = |A_j^{(k)}| ,
\]
(201)
where $A_j(M_k)$ is the $A_j$ coefficient of the $M_k$ channel of $U_k$, see (196). Let $|\Omega|$ be a random variable having a distribution of the asymptotic singular value distribution of the singular values of $\Phi$, the distribution of $|\Omega|^2$ is determined by the asymptotic spectra of $\Phi \Phi^\dagger$.

Specifically, the $f_{\text{eff}}(\cdot)$ efficiency function in (180) can be rewritten as
\[
f_{\text{eff}}(\chi, \text{SNR}_{U_k}^*) = \chi \mathbb{E} \left[ \log_2 \left( 1 + \mathbb{E} \left[ |A_j(M_k)|^2 \right] \text{SNR}_{U_k}^* \eta_{U_k} \left( \text{SNR}_{U_k}^* \right) \right) \right] ,
\]
(202)
where $\eta_{U_k}$ is the multiuser efficiency, evaluated as
\[
\eta_{U_k} = \frac{1}{\mathbb{E} \left[ |C|^2 \right]} \mathbb{E} \left[ \frac{|C|^2}{1 + \text{SNR}_{U_k}^* \chi |C|^2 \mathbb{E} \left[ \frac{|\Omega|^2}{1 + \mathbb{E} \left[ |C|^2 \right] \text{SNR}_{U_k}^* |\Omega|^2 \eta_{U_k}} \right]} \right] ,
\]
(203)
\[
= \frac{1}{\mathbb{E} \left[ |A_j(M_k)|^2 \right]} \mathbb{E} \left[ \frac{|A_j(M_k)|^2}{1 + \text{SNR}_{U_k}^* \chi |A_j(M_k)|^2 \mathbb{E} \left[ \frac{|\Omega|^2}{1 + \mathbb{E} \left[ |A_j(M_k)|^2 \right] \text{SNR}_{U_k}^* |\Omega|^2 \eta_{U_k}} \right]} \right] .
\]
such that
\[ \eta \left( \text{SNR}^*_{U_k} \rangle \right) \to \eta \left( \text{SNR}^*_{U_k} \right) \mathbb{E} \left[ |A_j (M_k)|^2 \right] \right). \tag{204} \]

where
\[
\eta \left( \text{SNR}^*_{U_k} \right) = \frac{\eta_{U_k}}{1 + \left( \text{SNR}^*_{U_k} \right) \mathbb{E} \left[ |A_j (M_k)|^2 \right]} \tag{205}
\]

\[
\mathbb{E} \left[ \frac{|A_j (M_k)|^2 / \mathbb{E} \left[ |A_j (M_k)|^2 \right]}{\chi \left( \text{SNR}^*_{U_k} \right) \mathbb{E} \left[ |A_j (M_k)|^2 \right]} \left( |A_j (M_k)|^2 / \mathbb{E} \left[ |A_j (M_k)|^2 \right] \right) + 1 \right] + \left( 1 - \chi \right) \left( \text{SNR}^*_{U_k} \right) \mathbb{E} \left[ |A_j (M_k)|^2 \right] \right) \eta_{U_k} \right].
\]

Without loss of generality, the term \( \eta_{U_k} \left( \text{SNR}^*_{U_k} \right) \) in (202) for \( 0 \leq \chi \leq 1 \) is expressed as
\[ \eta_{U_k} \left( \text{SNR}^*_{U_k} \right) = (1 - \chi). \tag{206} \]

Precisely, the \( P_{sym} (M_k) \) symmetric private classical capacity of the \( M_k \) logical channel of \( U_k \) is particularly yielded as
\[ P_{sym} (M_k) = \frac{1}{K} \chi \mathbb{E} \left[ \log_2 \left( 1 + \xi \left( Y, \sum_{i=0}^{l-1} \text{SNR}^*_i \right) \right) \right] \tag{207} \]

\[
\frac{\sum_{i=0}^{l-1} \text{SNR}^*_i}{\mathbb{E}} = \frac{1}{K} \int_0^1 \frac{1}{\chi} \left( 1 - \eta_{F(T (N))} F(T (N))^\dagger \right) dx,
\]

where \( \sum_{i=0}^{l-1} \text{SNR}^*_i = \sum_{i=0}^{l-1} \sigma^2_i / \sigma^2_i, Y \in U_{[0,1]} \), and \( \eta_{F(T (N))} F(T (N))^\dagger \) is the \( \eta \)-transform of \( F(T (N)) F(T (N))^\dagger \), specifically as
\[ \eta_{F(T (N))} F(T (N))^\dagger \left( \sum_{i=0}^{l-1} \text{SNR}^*_i \right) = \eta \left( \sum_{i=0}^{l-1} \text{SNR}^*_i \right) \mathbb{E} \left[ \frac{\chi - 1 + \eta_{F(T (N))} F(T (N))^\dagger \left( \sum_{i=0}^{l-1} \text{SNR}^*_i \right)}{\eta_{F(T (N))} F(T (N))^\dagger \left( \sum_{i=0}^{l-1} \text{SNR}^*_i \right)} \right]. \tag{208} \]

while function \( \xi \left( Y, \sum_{i=0}^{l-1} \text{SNR}^*_i \right) \) is as
\[
\frac{\sum_{i=0}^{l-1} \text{SNR}^*_i}{\mathbb{E}} = \left[ \mathbb{E} \left[ \int_{\mathbb{R}} \eta_{F(T (N))} F(T (N))^\dagger \left( \sum_{i=0}^{l-1} \text{SNR}^*_i \right) \right] \right]. \tag{209} \]

Using (208), the following relation holds for the \( K \) users:
\[
\frac{1}{K} \text{Tr} \left( I + \sum_{i=0}^{l-1} \text{SNR}^*_i F(T (N))^\dagger F(T (N)) \right)^{-1}
\]

\[
= 1 - \frac{1}{\chi} \left( 1 - \eta_{F(T (N))} F(T (N))^\dagger \left( \sum_{i=0}^{l-1} \text{SNR}^*_i \right) \right). \tag{210} \]
Precisely, the $S_{\text{sym}}(U_k)$ symmetric secret key rate of $U_k$ over identical sub-channels is expressed as

$$S_{\text{sym}}(U_k) \leq \frac{1}{K} \int 0^1 x \left( 1 - h_F(T(x))F(T(x))' \right) dx.$$  

(211)

In particular, using the density function $f_x(x)$ (Marchenko-Pastur density function),

$$f_x(x) = \left( 1 - \frac{1}{x} \right)^+ \xi(x) + \frac{\sqrt{(x-u)^+(v-x)^+}}{2\pi x},$$

(212)

where $\xi(\cdot)$ is a related random function, and $u = (1 - \chi)^2$ and $v = (1 + \chi)^2$, (210) can be rewritten precisely as

$$\frac{1}{K} \text{Tr} \left( I + \sum_{i=0}^{l-1} \text{SNR}_i^* F(T(\mathcal{N}_i))T(\mathcal{N}_i)' \right)^{-1}$$

$$= \int_a^b \frac{1}{1 + \sum_{i=0}^{l-1} \text{SNR}_i^*} f_x(x) dx.$$  

(213)

The proof is concluded here. □

The density function $f_x(x)$ for $\chi = 0.2, 0.5, 1$ is depicted in Figure 6.

5 | CONCLUSIONS

The multicarrier CVQKD systems are aimed to avoid the main drawbacks of CVQKD, such as low secret key rates, low tolerable losses, and short communication distances, allowing the legal parties to establish an unconditional secure communication over the standard networks. We provided a distribution statistics and random matrix framework for multicarrier CVQKD. Exploiting order statistics, we defined different statistics methods to derive the averaged transmittance coefficients from the Gaussian sub-channel transmittances. The provided operators order, select, and sum the sub-channel coefficients for the information transmission at a given threshold. We analyzed the complexity and the error probabilities of the sub-channel selection operators and defined an optimized progressive sub-channel scanning scheme. We characterized a random matrix formalism for multicarrier CVQKD that utilizes the mathematical background of random matrix theory. The framework is formulated for multiple-access multicarrier CVQKD, through the multiuser quadrature allocation multiuser transmission scheme. Using the random matrix formalism, we studied
the private classical information capabilities of the users at different subcarrier allocation mechanisms. The proposed combined framework of order statistics and random matrix theory is particularly convenient for the firm portrayal of the information flowing in experimental multicarrier CVQKD scenarios.

ETHICS STATEMENT

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

DATA ACCESSIBILITY STATEMENT

This work does not have any experimental data.

COMPETING NONFINANCIAL INTERESTS STATEMENT

We have no competing non-financial interests.

COMPETING FINANCIAL INTERESTS STATEMENT

We have no competing financial interests.

CONFLICT OF INTERESTS

We have no competing interests.

FUNDING INFORMATION

No relevant funding.

AUTHOR CONTRIBUTIONS

L.GY. designed and wrote the manuscript. L.GY. analyzed the results.

ACKNOWLEDGMENTS

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

ORCID

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

REFERENCES

1. Pirandola, S. et al. Advances in quantum cryptography, arXiv:1906.01645 (2019).
2. Pirandola, S.. Bounds for multi-end communication over quantum networks. Quantum Sci Technol. 2019;4:045006.
3. Grosshans F, Cerf NJ. Continuous-variable quantum cryptography is secure against non-Gaussian attacks. Phys Rev Lett. 2004;92:047905.
4. Grosshans F, Van Assche G, Wenger J, Broui R, Cerf NJ, Grangier P. Quantum key distribution using Gaussian-modulated coherent states. Nature. 2003;421:238.
5. Grosshans F, Cerf NJ, Wenger J, Broui R, Grangier P. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. Quant Inf Comp. 2003;3:535.
6. Navascues M, Grosshans F, Acin A. Optimality of Gaussian attacks in continuous variable quantum cryptography. Phys Rev Lett. 2006;97:190502.

7. Garcia-Patron R, Cerf NJ. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. Phys Rev Lett. 2006;97:190503.

8. Pirandola S. Capacities of repeater-assisted quantum communications. arXiv:1601.00966 (2016).

9. Pirandola S. End-to-end capacities of a quantum communication network. Commun Phys. 2019;2:51.

10. Pirandola S, Braunstein SL. Unite to build a quantum internet. Nature. 2016;532:169-171.

11. Gyongyosi L, Imre S, Nguyen HV. A survey on quantum channel capacities. IEEE Communications Surveys and Tutorials. 2018;99:1149-1205. 1. https://doi.org/10.1109/COMST.2017.2786748

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

13. Pirandola, S., Mancini, S., Lloyd, S. and Braunstein, S. L. Continuous variable quantum cryptography using two-way quantum communication, arXiv:quant-ph/0611167v3 (2008).

14. Adcock MRA, Hoyer P, Sanders BC. Limitations on continuous variable quantum algorithms with Fourier transforms. New J Phys. 2009;11:103035.

15. Gyongyosi L, Imre S. Multiple access multichannel continuous-variable quantum key distribution. Chaos, Solitons Fractals. 2018;104:491-505. Elsevier. https://doi.org/10.1016/j.chaos.2018.07.006, ISSN: 0960-0779

16. Pirandola S, Garcia-Patron R, Braunstein SL, Lloyd S. Phys Rev Lett. 2009;102:050503.

17. Pirandola S, Serafini A, Lloyd S. Phys Rev. A. 2009;79:052327.

18. Pirandola S, Braunstein SL, Lloyd S. Phys Rev Lett. 2008;101:200504.

19. Weedbrook C, Pirandola S, Lloyd S, Ralph T. Phys Rev Lett. 2010;105:110501.

20. Weedbrook C, Pirandola S, Garcia-Patron R, et al. Rev Mod Phys. 2012;84:621.

21. Sun M, Peng X, Shen Y, Guo H. Int J Quant Inf. 2012;10:1250059.

22. Sun M, Peng X, Guo H. J Phys B: At Mol Opt Phys. 2013;46:085501.

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

24. Imre S, Balazs F. Quantum Computing and Communications – An Engineering Approach. John Wiley and Sons Ltd; 2005:283. ISBN:9-470-86902-X.

25. Petz D. Quantum Information Theory and Quantum Statistics. Springer-Verlag, Heidelberg, Hiv; 2008:6.

26. Van Meter R. Quantum Networking. John Wiley and Sons Ltd, ISBN 1118648927, 9781118648926; 2014.

27. Leverrier A, Garcia-Patrón R, Renner R, Cerf NJ. Security of continuous-variable quantum key distribution against general attacks. Phys Rev Lett. 2013;110:030502.

28. Renner R, de Cirac JI. Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. Phys Rev Lett. 2009;102:110504.

29. Furrer F, Franz T, Berta M, et al. Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks. Phys Rev Lett. 2012;109:105040.

30. Leverrier A. Composable Security Proof for continuous-variable quantum key distribution with coherent states. Phys Rev Lett. 2015;114:070501.

31. Van Assche G, Cardinal J, Cerf NJ. Reconciliation of a quantum-distributed Gaussian key. IEEE Transactions on Information Theory. 2004;50:394.

32. Leverrier A, Grangier P. Continuous security proof of local distance continuous-variable quantum key distribution with discrete modulation. Phys Rev Lett. 2009;102:180504.

33. Mitra AMSP. Capacity of multivariate channels with multiplicative noise: random matrix techniques and large-N expansions. Journal of Statistical Physics. 2006;125(5–6):1223-1242.

34. Lodewyck J, Bloch M, Garcia-Patron R, et al. Phys Rev A. 2007;76:042305.

35. Qi, B. and Lim, C. C. W. Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator, arXiv:1708.08742v1 (2017).

36. Gyongyosi L, Imre S. Low-dimensional reconciliation for continuous-variable quantum key distribution. Appl Sci. 2018;8(1):87. https://doi.org/10.3390/app8010087, ISSN 2076-3417

37. Gyongyosi, L. and Imre, S. Singular layer transmission for continuous-variable quantum key distribution, IEEE Photonics Conference (IPC) 2014, IEEE, DOI: https://doi.org/10.1109/IPCOn.2014.6995246 (2014).

38. Gyongyosi, L. and Imre, S. Proc SPIE 9377, Advances in Photonics of Quantum Computing, Memory, and Communication VIII, 937711 (March 4, 2015; doi:10.1117/12.2076532)

39. Gyongyosi, L. Diversity extraction for multichannel continuous-variable quantum key distribution, Proceedings of the 2016 24th European Signal Processing Conference (EUSIPCO 2016), (2016).

40. Gyongyosi, L. and Imre, S. http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=2195505

41. Lloyd S. Capacity of the noisy quantum channel. Physical Rev. A. 1997;55:1613-1622.
43. Lloyd, S. The universe as quantum computer, a computable universe: understanding and exploring nature as computation, H. Zenil ed., World Scientific, Singapore, arXiv:1312.4455v1 (2013).
44. Lloyd S, Shapiro JH, Wong FNC, Kumar P, Shahriar SM, Yuen HP. Infrastructure for the quantum Internet. ACM SIGCOMM Computer Communication Review. 2004;34:9-20.
45. Lloyd S, Mohseni M, and Rebentrost, P. Quantum algorithms for supervised and unsupervised machine learning. arXiv:1307.0411 (2013).
46. Lloyd S, Mohseni M, Rebentrost P. Quantum principal component analysis. Nature Physics. 2014;10:631.
47. Pirandola S, Laurenza R, Ottaviani C, Banchi L. Fundamental limits of repeaterless quantum communications. Nature Communications. 2017;8:15043. https://doi.org/10.1038/ncomms15043
48. Pirandola S, Braunstein SL, Laurenza R, et al. Theory of channel simulation and bounds for private communication. Quantum Sci Technol. 2018;3:035009.
49. Laurenza R, Pirandola S. General bounds for sender-receiver capacities in multipoint quantum communications. Phys Rev A. 2017;96:032318.
50. Bacsardi L. On the way to quantum-based satellite communication. IEEE Comm Mag. 2013;51(08):50-55.
51. Muralidharan S, Kim J, Lukenhaus N, Lukin MD, Jiang L. Ultrafast and fault-tolerant quantum communication across long distances. Phys Rev Lett. 2014;112:250501.
52. Kiktenko EO, Pozhar NO, Anufriev MN, et al. Quantum-secured blockchain. Quantum Sci Technol. 2018;3:035004.
53. Shor PW. Scheme for reducing decoherence in quantum computer memory. Phys Rev A. 1995;52:R2493-R2496.
54. Biamonte J et al. Quantum Machine Learning Nature. 2017;549:195-202.
55. 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;1(1):1-37, 1800011.
56. Gyongyosi, L. and Imre, S. Long-distance continuous-variable quantum key distribution with advanced reconciliation of a Gaussian modulation, Proceedings of SPIE Photonics West OPTO 2013 (2013).
57. Gyongyosi, L. and 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 (2016).
58. Wehner S, Elkouss D, Hanson R. Quantum internet: a vision for the road ahead. Science. 2018;362:6412.
59. Preskill J. Quantum Computing in the NISQ era and beyond. Quantum. 2018;2:79.
60. Arute F et al. Quantum supremacy using a programmable superconducting processor. Nature. 2019;574. https://doi.org/10.1038/s41586-019-1666-5
61. Harrow AW, Montanaro A. Quantum computational supremacy. Nature. 2017;549:203-209.
62. Aaronson, S. and Chen, L. Complexity-theoretic foundations of quantum supremacy experiments. Proceedings of the 32nd Computational Complexity Conference, CCC’17, pages 22:1-22:67, (2017).
63. Farhi, E., Goldstone, J., Gutmann, S. and Neven, H. Quantum algorithms for fixed qubit architectures. arXiv:1703.06199v1 (2017).
64. Farhi, E. and Neven, H. Classification with quantum neural networks on near term processors, arXiv:1802.06002v1 (2018).
65. Tse D, Viswanath P. Fundamentals of Wireless Communication. Cambridge University Press; 2005.
66. Middlet, D. An Introduction to Statistical Communication Theory: An IEEE Press Classic Reissue, Hardcover, IEEE, ISBN-10: 0780311787, ISBN-13: 978-0780311787 (1960).
67. Kay S. Fundamentals of Statistical Signal Processing. 1-III Prentice Hall; 2013.
68. Gyongyosi L, Bacsardi L, Imre S. A survey on quantum key distribution. Infocom J. 2019;XI(2):14-21.
69. Gyongyosi, L. and Imre, S. Adaptive Gaussian quadrature detection for continuous-variable quantum key distribution, Proceedings Volume 9762, Advances in Photonics of Quantum Computing, Memory, and Communication IX; 97620E; doi: https://doi.org/10.1117/12.2211743 (2016).
70. Gyongyosi, L. and Imre, S. Proceedings Volume 8997, Advances in Photonics of Quantum Computing, Memory, and Communication VII; 89970C; do: https://doi.org/10.1117/12.2038532 (2014).
71. Imre S, Gyongyosi L. Advanced Quantum Communications - An Engineering Approach. New Jersey, USA: Wiley-IEEE Press; 2012.
72. Gyongyosi, L. and Imre, S. Multidimensional manifold extraction for multicarrier continuous-variable quantum key distribution, SPIE Quantum Information and Computation XIII, 20-24 Apr 2015, Baltimore, Maryland, USA, (2015).
73. Mraz A, Kis Z, Imre S, Gyongyosi L, Bacsardi L. Quantum circuit-based modeling of continuous-variable quantum key distribution system. International Journal of Circuit Theory and Applications (IJCTA), Special Issue on Quantum Circuits (Wiley). 2017;1017-1028.
74. Gyongyosi L, Imre S. Geometrical analysis of physically allowed quantum cloning transformations for quantum cryptography. Information Sciences, 2014;1-23. https://doi.org/10.1016/j.ins.2014.07.010
75. 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. 18:00 39. 2019. https://doi.org/10.1007/s11128-018-2147-8
76. 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.
77. Gyongyosi L. Multicarrier continuous-variable quantum key distribution. Theoret Comput Sci. 2020-1-29. https://doi.org/10.1016/j.tcs. 2019.11.026
78. Gyongyosi L, Imre S. Secret key rate proof of multicarrier continuous-variable quantum key distribution. Int J Commun Syst. (Wiley). 2018:e3865. https://doi.org/10.1002/dac.3865
79. Gyongyosi L, Imre S. Diversity space of multicarrier continuous-variable quantum key distribution. *Int J Commun Syst.* (Wiley). 2019:1-30, e4003. https://doi.org/10.1002/dac.4003
80. Gyongyosi L, Imre S. Gaussian quadrature inference for multicarrier continuous-variable quantum key distribution. *Quantum Studies: Mathematics and Foundations, Springer Nature.* 2019:397-430. https://doi.org/10.1007/s40509-019-00183-9
81. Gyongyosi L, Imre S. Statistical quadrature evolution by inference for multicarrier continuous-variable quantum key distribution. *Quantum Studies: Mathematics and Foundations, Springer Nature.* 2019:1-26. https://doi.org/10.1007/s40509-019-00202-9
82. Gyongyosi L. Singular value decomposition assisted multicarrier continuous-variable quantum key distribution. *Theoret Comput Sci.* 2019:35-63. https://doi.org/10.1016/j.tcs.2019.07.029
83. Gyongyosi L, Imre S. Secret key rates of free-space optical continuous-variable quantum key distribution. *Int J Commun Syst.* (Wiley). 2019:e4152. https://doi.org/10.1002/dac.4152
84. Gyongyosi, L. and Imre, S. Adaptive multicarrier quadrature division modulation for long-distance continuous-variable quantum key distribution, *Proc. SPIE 9123, Quantum Information and Computation XII, 912307* (May 22, 2014); doi:10.1117/12.2050095, From Conference Volume 9123, Quantum Information and Computation XII, Baltimore, Maryland, USA (2014).
85. Gyongyosi L, Imre S. Subcarrier domain of multicarrier continuous-variable quantum key distribution. *J Stat Phys.* Springer Nature. 2019;177(5):960-983. https://doi.org/10.1007/s10955-019-02404-2
86. Gyongyosi L, Imre S. Secret key rate adaption for multicarrier continuous-variable quantum key distribution. *SN Comput Sci Nature.* 2019:1-30. https://doi.org/10.1007/s42979-019-0027-7
87. Yang H-C, Alouini M-S. *Order Statistics in Wireless Communications.* Cambridge, UK: Cambridge University Press; 2011.
88. Chow, P. S. *Bandwidth optimized digital transmission techniques for spectrally shaped channels with impulse noise,* Ph. D. thesis, Stanford University, (1993).
89. Yu W, Cioffi JM. On Constant Power Water-filling. *IEEE International Conference on Communications.* 2001:7106253, https://doi.org/10.1109/ICC.2001.937077
90. Shieh W, Djordjevic I. *OFDM for Optical Communications.* Elsevier; 2010.
91. Zhang, W. *The Role of Correlation in Communication Over Fading Channels,* PhD Thesis, Notre Dame, Indiana (2006).
92. Tulino AM, Verdu S. *Random Matrix Theory and Wireless Communications.* Hanover, USA, ISBN: 1-933019-00-X; ISSN: Paper version 1567-2190; Electronic version 1567-2328: Now Publishers; 2004.
93. Edelman A, Rao NR. Random matrix theory. *Acta Numerica.* 2005:1-65. https://doi.org/10.1017/S0962492904000236

---

**How to cite this article:** Gyongyosi L. Order Statistics and Random Matrix Theory of Multicarrier Continuous-Variable Quantum Key Distribution. *Int J Commun Syst.* 2020;33:e4314. https://doi.org/10.1002/dac.4314

**APPENDIX A**

**Notations**

The notations of the manuscript are summarized in Table A1.
| Notation | Description |
|----------|-------------|
| i        | Index for an \(i\)th subcarrier Gaussian CV, \(|\phi_i\rangle = x_i + ip_i\). |
| j        | Index for a \(j\)th Gaussian single-carrier CV, \(|\varphi_j\rangle = x_j + ip_j\). |
| l        | Number of Gaussian sub-channels \(N_l\) for the transmission of the Gaussian subcarriers. The overall number of the sub-channels is \(n\). The remaining \(n - l\) sub-channels do not transmit valuable information. |
| \(x_i, p_i\) | Position and momentum quadratures of the \(i\)th Gaussian subcarrier, \(|\phi_i\rangle = x_i + ip_i\). |
| \(x'_i, p'_i\) | Noisy position and momentum quadratures of Bob’s \(i\)th noisy subcarrier Gaussian CV, \(|\phi'_i\rangle = x'_i + ip'_i\). |
| \(x_j, p_j\) | Position and momentum quadratures of the \(j\)th Gaussian single-carrier \(|\varphi_j\rangle = x_j + ip_j\). |
| \(x'_j, p'_j\) | Noisy position and momentum quadratures of Bob’s \(j\)th recovered single-carrier Gaussian CV \(|\varphi'_j\rangle = x'_j + ip'_j\). |
| \(x_{Al}, p_{Al}\) | Alice’s quadratures in the transmission of the \(i\)th subcarrier. |
| \(|\phi_i\rangle, | phi'\rangle\) | Transmitted and received Gaussian subcarriers. |
| \(Q(\cdot)\) | Gaussian tail function. |
| \(z\) | A \(d\)-dimensional input CV vector to transmit valuable information, \(z \in C^d N(0, K_z)\). |
| \(z'\rightarrow\) | A \(d\)-dimensional noisy output vector, \(z'\rightarrow = A'z + (F(\Delta))^T = (z'_1, \ldots, z'_{d-1})\), where \(z'_i = \left(\frac{1}{i\lambda} \sum_{i=0}^{\infty} F(T_{i,j}(N_i))\right) z_j + F(\Delta) \in C^d N\left(0, 2\left(\sigma_{\omega}^2 + \sigma_{\chi}^2\right)\right)\). |
| \(\Sigma^{\rightarrow}\) | The SNR quantity of \(U_k\), evaluated for the transmission of private classical information. |
| \(\Sigma^{\rightarrow} = \sum_{i=0}^{\infty} SNR_i^{\rightarrow}\) | Total SNR of the \(l\) Gaussian sub-channels, evaluated for the transmission of private classical information. \(\Sigma^{\rightarrow} = \sum_{i=0}^{\infty} \sigma_{\chi_i}^2 / \sigma_{\chi_i}^2\), where \(\sigma_{\chi_i}^2\) is the constant subcarrier modulation variance, and \(\sigma_{\chi_i}^2 = \sigma_{\chi_i}^2 \left(\frac{\sigma_{\omega_i}^2 |P(T_{i,j}(N_i))|^2 + \sigma_{\omega_i}^2}{1 + \sigma_{\omega_i}^2 |P(T_{i,j}(N_i))|^2} - 1\right)^{-1}\), where \(\sigma_{\chi_i}^2 = \sigma_{\chi_i}^2 + N_i\), \(\sigma_{\omega_i}^2\) is the vacuum noise, \(N_i\) is the excess noise of the Gaussian sub-channel \(N_i\), \(N_i = (W_i - 1)[|P(T_{i,j}(N_i))|^2\right)\), where \(W_i\) is the variance of Eve’s EPR state used for the attacking of \(N_i\), while \(|T_{Eve}|^2 = 1 - |T_e|^2\) is the transmittance of Eve’s beam splitter (BS), and \(|T_e|^2\) is the transmittance of \(N_i\). |
| \(\frac{1}{7} \left| F \left( \hat{T}_i \left( N_i \right) \right) \right|^2\) | Normalized, unordered sub-channel transmittance coefficient, real variable. |
| \(\frac{1}{7} \left| F \left( T_i \left( N_i \right) \right) \right|^2\) | Normalized, ordered sub-channel transmittance coefficient, real variable. |
| \(A_j \left( N_i \right)\) | Single-carrier channel coefficient, complex variable, expressed as \(A_j \left( N_i \right) = \frac{1}{7} \sum_{i=0}^{\infty} F \left( T_i \left( N_i \right) \right)\). |
| \(\left| A_j \left( N_i \right) \right|^2\) | Single-carrier channel coefficient, real variable, expressed as \(\left| A_j \left( N_i \right) \right|^2 = \frac{1}{7} \sum_{i=0}^{\infty} \left| F \left( T_i \left( N_i \right) \right) \right|^2\), real variable. |
| \(M(\cdot)\) | The moment-generating function (MGF) function. |
| \(P(\cdot)\) | The probability density function (PDF) function. |
| \(P_c(\cdot)\) | The common PDF of unordered random variables. |
| \(f(\cdot)\) | The cumulative distribution function (CDF) function. |
| \(f_c(\cdot)\) | The common CDF of unordered random variables. |
| \(R_{err}(x)\) | Error rate function. |
| \(R_{err}\) | Average error rate. |
| \(\Lambda_{U_k}\) | Channel selection operator for user \(U_k\), \(\Lambda_{U_k} = O \Sigma\), where \(O\) is the sub-channel ordering operator, while \(\Sigma\) is the sum generating operator. |
| \(\left| F \left( T_i \left( N_i \right) \right) \right|^2\) | Threshold parameter for the sub-channel selection process. If \(\left| F \left( T_i \left( N_i \right) \right) \right|^2 \leq \frac{1}{7} \left| F \left( T_i \left( N_i \right) \right) \right|^2\) for Gaussian sub-channel \(N_i\), the sub-channel is qualified as “good.” otherwise it is put into the “bad” set.

(Continues)
| Notation | Description |
|----------|-------------|
| $\Lambda_0$ | Sub-channel selection with complete scan at a priori fixed threshold $|F(T_i^r(N_i^i))|^2$, which is determined via the optimal Gaussian attack. All sub-channels (n) are scanned through, the best l selected. In a modified version of $\Lambda_0$, the threshold is evaluated via the transmission coefficient of the best available sub-channel as $\frac{1}{l} |F(T_i^r(N_i^i))|^2 = \mu \max_i \frac{1}{l} |F(T_i^r(N_i^i))|^2$. |
| $\Lambda$ | Progressive sub-channel selection with an a priori fixed threshold $|F(T_i^r(N_i^i))|^2$, at an optimized complexity. The iteration does not require full scan, as the l sub-channels are determined in the iteration steps. |
| $\Lambda'$ | Progressive sub-channel selection with a priori fixed threshold $|F(T_i^r(N_i^i))|^2$, at an optimized complexity. If no l sub-channels available at the threshold, the operator selects the remaining sub-channels from the bad channel set (bad: the a priori fixed threshold does not hold for the sub-channel). |
| $\lambda$ | Lagrange multiplier, used to determine the $|F(T_i^r(N_i^i))|^2$ threshold parameter, as $\lambda = \frac{1}{l} \sum_{i=0}^{l-1} |F(T_i^r(N_i^i))|^2 = \frac{1}{l} \sum_{i=0}^{l-1} T_i e^{-\frac{\omega}{\sigma}}$, where $T_i$ is the expected transmittance of the l sub-channels under an optimal Gaussian attack. |
| $\lambda'_{\Lambda'}$ | Lagrange multiplier at $\Lambda', \lambda'_{\Lambda'} = F\left(\hat{\lambda}_{\Lambda'}\right)^2 = |F(T_i^r(N_i^i))|^2 + \omega$, where $\omega$ is a nonnegative real variable, $\omega = |F(T_i^r(N_i^i))|^2 - \min \left(\left(|F(T(N_i^i))|^2, \ldots, |F(T(N_i^i))|^2\right)\right)$ and $|F(T(N_i^i))|^2$, $\ldots$, $|F(T(N_i^i))|^2$ are the corresponding coefficients of the bad set $B(N_i^i, \ldots, N_i^{l-1})$. |
| $\Gamma_1, \Gamma_2$ | Correlated random variables, $\Gamma_1 = \frac{1}{l} \sum_{i=0}^{l-1} |F(T_i^r(N_i^i))|^2$, and $\Gamma_2 = \frac{1}{l} |F(T_{l-1}(N_i^i))|^2$, where the transmittance coefficients are sorted in a descending order. $\frac{1}{l} |F(T_l(N_i^i))|^2 \geq \frac{1}{l} |F(T_l(N_i^i))|^2 \ldots \geq \frac{1}{l} |F(T_{l-1}(N_i^i))|^2$, and $|A_i(N_i^i)|^2 = \Gamma_1 + \Gamma_2$. |
| $\kappa_{\Lambda_0}, \kappa_{\Lambda}, \kappa_{\Lambda'}$ | The average number of the iterations (eg, the number of comparisons of sub-channel transmission coefficients at $|F(T_i^r(N_i^i))|^2$ threshold per sub-channels). |
| $p_{err}^W(A_j)$ | Single-carrier level, quadrature error probability at operator $\Lambda_0$. |
| $p_{err}^W(A_j)$ | Single-carrier level, quadrature error probability at operator $\Lambda$. |
| $p_{err}^W(A_j)$ | Single-carrier level, quadrature error probability at operator $\Lambda'$. |
| $M^\Lambda_{\Lambda_0, \Lambda_0}(\lambda_{\Lambda_0})_{\text{SNR}} (\cdot)$ | The MGF function of $A_i(N_i^i)$ $\Lambda_0^2 \cdot \text{SNR}$ at operator $\Lambda_0$. |
| $M^\Lambda_{\Lambda_0, \Lambda_0}(\lambda_{\Lambda_0})_{\text{SNR}} (\cdot)$ | The MGF function of $A_i(N_i^i)$ $\Lambda^2 \cdot \text{SNR}$ at operator $\Lambda$. |
| $M^\Lambda_{\Lambda_0, \Lambda_0}(\lambda_{\Lambda_0})_{\text{SNR}} (\cdot)$ | The MGF function of $A_i(N_i^i)$ $\Lambda^2 \cdot \text{SNR}$ at operator $\Lambda'$. |
| $\eta$ | $\eta$-transform. For a nonnegative random variable $X$ is defined as $\eta_X(\gamma) = E \left[ \frac{1}{1+\gamma X} \right]$, where $\gamma$ is a nonnegative real number, and $0 < \eta_X(\gamma) \leq 1$. |
| $\nu$ | $\nu$-transform (Shannon transform). For a nonnegative random variable $X$ is defined as, $\nu_X(\gamma) = E \left[ \log_2 (1 + \gamma X) \right]$, where $\gamma$ is a nonnegative real number. |
| $\nu_{F(T(N_i^i))} (\gamma)$ | The $\nu$-transform of $F(T(N_i^i)) = F(T(N_i^i)) \gamma$. |
| $D(x)$ | Distribution function of variable $x$. |
| $P$ | Probability measure function that returns an event's probability. |
| $f_{x}(x)$ | The Marcenko-Pastur density function, $f_{\xi} (x) = \left( 1 - \frac{1}{x} \right)^{+} \xi (x) + \frac{\nu_X(\gamma_X)}{2x} \log \left( \frac{1}{\gamma_X} \right)$, where $\xi(\cdot)$ is a relating random function, $\alpha = \left( 1 - \sqrt{x} \right)^2$ and $\beta = \left( 1 + \sqrt{x} \right)^2$. |
| $\mathcal{L}$ | Laplace transform. |

$X \in U_{[0,1]}$, $Y \in U_{[0,1]}$, $Z \in U_{[b,1]}$, $|C|$ | Independent, random variables, drawn from a $U$ uniform distribution on $[0,1]$. Independent random variable, drawn from a $U$ uniform distribution on $[b,1]$. Random variable having a distribution of the asymptotic singular value distribution of the singular values of $X$. The distribution of $|C|^2$ is determined by the asymptotic spectra of $XX^T$. |

(Continues)
Table A1 continued

| Notation | Description |
|----------|-------------|
| $|\Omega|$ | Random variable having a distribution of the asymptotic singular value distribution of the singular values of $\Phi$. The distribution of $|\Omega|^2$ is determined by the asymptotic spectra of $\Phi \Phi^\dagger$. |
| $\text{var}(a,b)$ | Variance profile function. |
| $\rho_{F(T(N'))}(a,b)$ | Channel profile function of $F(T(N'))$, $\rho_{F(T(N'))}(a,b)$ : $[0,1]^2 \rightarrow \mathbb{R}$. |
| $F_{U_k}(\cdot), F_{B_k}(\cdot)$ | Nonrandom limits. |
| $X$ | Nonnegative variable, such that $K/l \rightarrow X$ holds, where $K$ is the number of users, $l$ is the number of available sub-channels. |
| $\Delta_{k}^{(K)}$ | Noise matrix of $K$ users. |
| $\mathcal{M}_k$ | Logical channel of user $U_k$, a set formulated from $m$ subcarriers such that $\mathcal{M}_k = \{\mathcal{M}_k^{(0)}, \ldots, \mathcal{M}_k^{(b)}\}$, where $\mathcal{M}_k^{(b)}$ identifies the $b$th logical sub-channel of $U_k$. |
| $P_{\text{sym}}(\mathcal{M}_k)$ | Symmetric private classical capacity of the $\mathcal{M}_k$ logical channel of $U_k$, the maximum common rate at which the $K$ users both can reliably transmit private classical information over the $l$ sub-channels of $\mathcal{N}$. |
| $S_{\text{sym}}(\mathcal{M}_k)$ | Symmetric secret key rate of the $\mathcal{M}_k$ logical channel of $U_k$, a common rate at which the $K$ users both can reliably transmit private classical information over the $l$ sub-channels of $\mathcal{N}$. |
| $b$ | Ratio of the $k$ actual number of users and the total users $K$, $b = \frac{K}{E}$. |
| $X_{\text{CZ}}\Phi$ | The random matrix decomposition at arbitrarily allocated sub-channels. Random matrix decomposition of $F(T(N'))$, where $Z = (\Theta_0, \ldots, \Theta_{K-1})$ is an $l \times K$ random matrix, $\Theta_k = [\Theta_{k,0}, \ldots, \Theta_{k,l-1}]^T$ is user $U_k$'s entry, $X$ is an $l \times K$ random matrix $X = (X_0, \ldots, X_{K-1})$, with $X_k = [A_{ik}^{(0)}, \ldots, A_{ik}^{(l-1)}]^T$ for user $U_k$, where $A_{ik}^{(l)} = \frac{1}{\sqrt{l}} \sum_{j=0}^{l-1} F(T_i(N'))$ is the averaged transmission coefficient of $U_k$ derived by operator $\Lambda_s \Lambda$ or $\Lambda u$, $\mu$ is the number of sub-channels of $U_k$, $\circ$ is the Hadamard product operator, while $\Phi$ is an $l \times K$ random matrix, $\Phi = \text{diag}(\Phi_0, \ldots, \Phi_{K-1})$. |
| $X_{\text{U}}\Phi$ | The random matrix decomposition at identically allocated sub-channels. The $h \times K$ channel matrix $F(T(N'))$ is $F(T(N')) = X_{\text{U}}\Phi$, where $U = (u_0, \ldots, u_{K-1})$ is an $h \times K$ isotropic unitary matrix with arbitrarily distributed random variables with mean $\mu_{ij} = \mu$ and variance $\sigma^2_{ij} = 1/l$, $u_k = [q_{k,0}, \ldots, q_{k,h-1}]^T$, $X$ is an $h \times h$ random matrix $X = \text{diag}(X_0, \ldots, X_{h-1})$, with $X_k = [A_{ik}^{(0)}, \ldots, A_{ik}^{(h-1)}]^T$, where $A_{ik}^{(h)} = \frac{1}{h} \sum_{i=0}^{h-1} F(T_i(N'))$ is the averaged transmission coefficients of $U_k$ in $S$, such that $X_i = X_k$ for $l = 0, \ldots, K - 1$, while $\Phi$ is an $K \times K$ random matrix, $\Phi = (\Phi_0, \ldots, \Phi_{K-1})$. |
| $U_{\text{Kout}}$ | The unitary CVQFT operation, $U_{\text{Kout}} = \frac{1}{\sqrt{K_{\text{out}}}} e^{i \frac{\omega_{2k}}{2} }$, $i, k = 0, \ldots, K_{\text{out}} - 1, K_{\text{out}} \times K_{\text{out}}$ unitary matrix. |
| $U_{\text{Kin}}$ | The unitary inverse CVQFT operation, $U_{\text{Kin}} = \frac{1}{\sqrt{K_{\text{in}}}} e^{i \frac{\omega_{2k}}{2} }$, $i, k = 0, \ldots, K_{\text{in}} - 1, K_{\text{in}} \times K_{\text{in}}$ unitary matrix. |
| $z$ | The variable of a single-carrier Gaussian CV state, $z \in \mathcal{N}(0, \sigma^2_z)$, $|q_i|$ $\in$ $S$. Zero-mean, circular symmetric complex Gaussian random variable, $\sigma^2_z = \text{E} \left[|z|^2\right] = 2\sigma^2_{z_0}$, with i.i.d. zero mean, Gaussian random quadrature components $x, p \in \mathcal{N}(0, \sigma^2_z)$, where $\sigma^2_{z_0}$ is the variance. |
| $\Delta$ | The noise variable of the Gaussian channel $\mathcal{N}$, $\Delta \in \mathcal{N}(0, \sigma^2_\Delta)$, with i.i.d. zero-mean, Gaussian random noise components on the position and momentum quadratures $\Delta_x, \Delta_p \in \mathcal{N}(0, \sigma^2_\Delta)$, with i.i.d. zero-mean, Gaussian random quadrature components $x, p \in \mathcal{N}(0, \sigma^2_\Delta)$, where $\sigma^2_\Delta$ is the variance. |
| $d$ | The variable of a Gaussian subcarrier CV state, $d \in \mathcal{N}(0, \sigma^2_d)$, $|\phi_i|$ $\in$ $S$. Zero-mean, circular symmetric Gaussian random variable, $\sigma^2_d = \text{E} \left[|d|^2\right] = 2\sigma^2_{d_0}$, with i.i.d. zero mean, Gaussian random quadrature components $x, p \in \mathcal{N}(0, \sigma^2_d)$, where $\sigma^2_{d_0}$ is the (constant) modulation variance of the Gaussian subcarrier CV state. |
| $F^{-1}(\cdot)$ | The inverse CVQFT transformation, $F^{-1}(\cdot) = \text{CVQFT}^T(\cdot)$, 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. |
| $\sigma^2_{z_0}$ | Single-carrier modulation variance. |
Continued

TABLE A1

| Notation | Description |
|----------|-------------|
| \( \sigma_{d_i}^2 \) | Multicarrier modulation variance, \( \sigma_{d_i}^2 = \frac{1}{2} \sum_{m=0}^{n} \sigma_{d_i}^2 \). Average modulation variance of the \( i \)th Gaussian sub-channels \( \mathcal{N}_i \). |
| \( |\phi_i\rangle \) | The \( i \)th Gaussian subcarrier CV of user \( U_i \), \( |\phi_i\rangle = \text{IFFT} (z_{d_i}) \), where IFFT stands for the Inverse Fast Fourier Transform, \( |\phi_i\rangle \in \mathcal{S}, d_i \in \mathcal{C} \mathcal{N} (0, \sigma_{d_i}^2) \), \( \sigma_{d_i}^2 = \mathbb{E} [\|d_i\|^2] \), \( d_i = x_{d_i} + ip_{d_i}, x_{d_i} \in \mathcal{N} (0, \sigma_{x_{d_i}}^2) \), \( p_{d_i} \in \mathcal{N} (0, \sigma_{p_{d_i}}^2) \) are i.i.d. zero-mean Gaussian random quadrature components, and \( \sigma_{x_{d_i}}^2 \) is the variance of the Fourier transformed Gaussian state. |
| \( |\varphi_{k,i}\rangle \) | The decoded single-carrier CV of user \( U_k \) from the subcarrier CV, \( |\varphi_{k,i}\rangle = \text{CVQFT} (|\phi_i\rangle) \), expressed as \( F (|d_i\rangle) = F (\text{IFFT} (z_{k,i})) \) = \( |z_{k,i}\rangle \). |
| \( \mathcal{N} \) | Gaussian quantum channel. |
| \( \mathcal{N}_k \) | An \( i \)-th Gaussian sub-channel, \( i = 0, \ldots, n - 1 \). |
| \( T (\mathcal{N}) \) | Channel transmittance, normalized complex random variable, \( T (\mathcal{N}) = Re T (\mathcal{N}) + \text{Im} T (\mathcal{N}) \in \mathbb{C} \). 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 \( \mathcal{N}_i \), \( T_i (\mathcal{N}_i) = \text{Re} (T_i (\mathcal{N}_i)) + \text{Im} (T_i (\mathcal{N}_i)) \in \mathbb{C} \), quantifies the position and momentum quadrature transmission, with (normalized) real and imaginary parts \( 0 \leq T_i (\mathcal{N}_i) \leq 1 / \sqrt{2} \), \( 0 \leq \text{Im} T_i (\mathcal{N}_i) \leq 1 / \sqrt{2} \), where \( \text{Re} T_i (\mathcal{N}_i) = \text{Im} T_i (\mathcal{N}_i) \). |
| \( T_{Eve} \) | Eve's transmittance, \( T_{Eve} = 1 - T (\mathcal{N}) \). |
| \( T_{Eve,i} \) | Eve’s transmittance for the \( i \)-th subcarrier CV. |
| \( \mathbf{z} \) | A \( d \)-dimensional, zero-mean, circular symmetric complex random Gaussian vector that models \( d \) Gaussian CV input states, \( \mathbf{z} = x + i \mathbf{p} = (z_0, \ldots, z_{d-1})^T \), \( \mathcal{C} \mathcal{N} (0, \mathbf{K}_z) \), \( \mathbf{K}_z = \mathbb{E} [\mathbf{zz}^T] \), where \( z_t = x_t + ip_t, x_t = (x_0, \ldots, x_{d-1})^T \), \( \mathbf{p} = (p_0, \ldots, p_{d-1})^T \), \( x_t \in \mathcal{N} (0, \sigma_{x_{d_i}}^2) \), \( p_t \in \mathcal{N} (0, \sigma_{p_{d_i}}^2) \) i.i.d. zero-mean Gaussian random variables. |
| \( \mathbf{d} \) | An \( d \)-dimensional, zero-mean, circular symmetric complex random Gaussian vector, \( \mathbf{d} = F^{-1} (\mathbf{z}), \mathcal{C} \mathcal{N} (0, \mathbf{K}_d) \), \( \mathbf{K}_d = \mathbb{E} [\mathbf{dd}^T] \), \( \mathbf{d} = (d_0, \ldots, d_{d-1})^T \), \( d_t = x_t + ip_t, x_t, p_t \in \mathcal{N} (0, \sigma_{x_{d_i}}^2) \) are i.i.d. zero-mean Gaussian random variables, \( \sigma_{x_{d_i}}^2 = 1 / \sigma_{d_i}^2 \). The \( i \)-th component is \( d_i \in \mathcal{C} \mathcal{N} (0, \sigma_{d_i}^2) \). |
| \( \mathbf{y}_k \) | A \( d \)-dimensional zero-mean, circular symmetric complex Gaussian random vector, \( \mathbf{y}_k \in \mathcal{C} \mathcal{N} (0, \mathbb{E} [\mathbf{yy}^T] \). |
| \( y_{k,m} \) | The \( m \)-th element of the \( k \)-th user's vector \( \mathbf{y}_k \), expressed as \( y_{k,m} = \sum_{j} F (T_i (\mathcal{N}_i)) F (d_i) + F (\Delta_i) \). |
| \( F (\mathcal{N}) \) | Fourier transform of \( \mathcal{N} = [T_0 (\mathcal{N}_0) \ldots T_{d-1} (\mathcal{N}_{d-1})]^T \in \mathbb{C}^d \), the complex transmittance vector. |
| \( F (\Delta) \) | Complex vector, expressed as \( F (\Delta) = e^{-j \pi \Delta \mathbf{K}_d \mathbf{F} (\Delta)} \), with covariance matrix \( \mathbf{K}_d (\Delta) = \mathbb{E} [F (\Delta) F (\Delta)^T] \). |
| \( y [j] \) | A \( j \)-th AMQD block, \( y [j] = F (\mathcal{N}) F (d) [j] + F (\Delta) [j] \). |
| \( \tau \) | An exponentially distributed variable, \( \tau = ||F (\mathbf{d}) [j]||^2 \), with density \( f (\tau) = \frac{1}{2 \sigma_{d_i}^2} e^{-\frac{\tau}{\sigma_{d_i}^2}}, \mathbb{E} [\tau] \leq 2 \sigma_{d_i}^2 \). |
| \( T_{Eve,i} \) | Eve’s transmittance on the Gaussian sub-channel \( \mathcal{N}_i \), \( T_{Eve,i} = \text{Re} T_{Eve,i} + \text{Im} T_{Eve,i} \in \mathbb{C}, 0 \leq \text{Re} T_{Eve,i} \leq 1 / \sqrt{2}, 0 \leq \text{Im} T_{Eve,i} \leq 1 / \sqrt{2}, 0 \leq |T_{Eve,i}|^2 < 1 \). |
| \( d_i \) | An \( i \)-th subcarrier in an AMQD block. |
| \( \nu_{\text{min}} \) | The \( \min \{|v_0, \ldots, v_{d-1}\} \) minimum of the \( v_i \) sub-channel coefficients, where \( v_i = \sigma_{x_i}^2 / F (T_i (\mathcal{N}_i)) \|^2 \) and \( v_i < \nu_{\text{Eve}} \). |
| \( \sigma_{d_i}^2 \) | Constant modulation variance, \( \sigma_{d_i}^2 = \nu_{\text{Eve}} - \nu_{\text{min}} G (\delta) F (\Delta), \text{where} \nu_{\text{Eve}} = \frac{1}{2}, \lambda = \frac{1}{n} \sum_{i=0}^{n-1} \left| \sum_{k=0}^{n-1} E_k e^{-j 2 \pi i k \frac{i}{n}} \right|^2 \text{and} \mathcal{T}_{\mathcal{N}} \text{is the expected transmittance of the Gaussian sub-channels under an optimal Gaussian collective attack.} |