Adaptive Quadrature Detection for Multicarrier Continuous-Variable Quantum Key Distribution

Laszlo Gyongyosi

1 Quantum Technologies Laboratory, Department of Telecommunications
   Budapest University of Technology and Economics
   2 Magyar tudosok krt, Budapest, H-1117, Hungary
2 MTA-BME Information Systems Research Group
   Hungarian Academy of Sciences
   7 Nador st., Budapest, H-1051, Hungary

gyongyosi@hit.bme.hu

Abstract
We propose the adaptive quadrature detection for multicarrier continuous-variable quantum key distribution (CVQKD). A multicarrier CVQKD scheme uses Gaussian subcarrier continuous variables for the information conveying and Gaussian sub-channels for the transmission. The proposed multicarrier detection scheme dynamically adapts to the sub-channel conditions using a corresponding statistics which is provided by our sophisticated sub-channel estimation procedure. The sub-channel estimation phase determines the transmittance coefficients of the sub-channels, which information are used further in the adaptive quadrature decoding process. We define the technique called subcarrier spreading to estimate the transmittance conditions of the sub-channels with a theoretical error-minimum in the presence of a Gaussian noise. We introduce the terms of single and collective adaptive quadrature detection. We also extend the results for a multiuser multicarrier CVQKD scenario. We prove the achievable error probabilities, the signal-to-noise ratios, and quantify the attributes of the framework. The adaptive detection scheme allows to utilize the extra resources of multicarrier CVQKD and to maximize the amount of transmittable valuable information in diverse measurement and transmission conditions. The framework is particularly convenient for experimental CVQKD scenarios.

Keywords: quantum key distribution, continuous variables, CVQKD, AMQD, AMQD-MQA, quantum Shannon theory.
1 Introduction

The continuous-variable quantum key distribution (CVQKD) protocols allow for legal parties to establish an unconditionally secure communication through standard telecommunication devices and networks [1-13, 16-20]. In comparison with discrete-variable (DV) QKD protocols, the encoding and decoding processes do not require single-photon devices and can be implemented through standard devices of optical telecommunications [14], [21-22], [26-33]. In a CVQKD protocol, the information is generally conveyed through the position and momentum quadratures of quantum states. These quadratures together identify a continuous variable [CV] state in the phase space (referred to as single-carrier CV). In a practical CVQKD modulation, the quadratures have a Gaussian random distribution, and the presence of the eavesdropper adds a white Gaussian noise to the quadrature transmission [16-20]. At the receiver, the noisy quadratures are detected by a homodyne (e.g., a position or a momentum quadrature is measured) or a heterodyne (e.g., both position and momentum quadratures are measured) measurement apparatus. Although the practical implementation of CVQKD requires no specialized devices, the performance of CVQKD protocols still brings up several challenges and demands significant improvements. Because the single-carrier CVQKD transmission allows no to exploit several invaluable essential resources in the transmission phase, the multicarrier CVQKD has been proposed [2-8]. In comparison with single-carrier CVQKD, the multicarrier transmission uses Gaussian subcarrier CVs for the information conveying, which are sent through Gaussian sub-channels. Particularly, the Gaussian sub-channels are derived from the physical Gaussian link via a CV unitary [2]. The multicarrier CVQKD modulation has been introduced via the adaptive multicarrier quadrature division (AMQD) framework [2], which also has been extended to a multiuser multicarrier CVQKD setting through the multiuser quadrature allocation scheme [3]. The multicarrier transmission possesses several benefits over single-carrier transmission, such as improved noise tolerance, higher secret key rates, enhanced security thresholds, and extended transmission distances [2-8]. The multicarrier modulation also allows to exploit those additional degrees of freedom of the transmission that are not available in a single-carrier scenario. Specifically, these extra resources allow us to define several new phenomena that cannot be utilized in a single-carrier setting, such as singular layer transmission [4], improved security thresholds [5], multidimensional manifold extraction [6], and subcarrier domain achievement [7]. These additional resources are provided by the extra degree of freedom of the multicarrier CVQKD scheme. In this work, we are focusing on the decoding mechanism and provide an efficient decoding framework for multicarrier CVQKD that allows for the legal parties to utilize and manifest the potential of the multicarrier modulation.

We define the adaptive quadrature detection for multicarrier CVQKD. The adaptive detection dynamically adapts to the channel conditions using a corresponding statistics of the sub-channels. This statistics is provided for the adaptive quadrature decoding process by our sophisticated sub-channel estimation procedure. Precisely, the proposed estimation determines the transmittance coefficients of the sub-channels, which are used further in the process of adaptive quadrature decoding. In particular, the conditions of the sub-channels are determined by pilot-subcarrier CV quantum states, which carry no valuable information and used only in a dedicated calibration
phase prior to the private information transmission of the protocol run. We introduce the technique called subcarrier spreading, which uses a subcarrier flow to estimate the transmittance conditions of the sub-channels with a theoretical minimum error probability. The adaptive quadrature detection procedure can be applied for single or collective, homodyne, or heterodyne measurement settings, receptively. We also extend the adaptive quadrature detection for a multiuser multicarrier CVQKD scenario. We derive the details of the adaptive decoding procedure, prove the achievable error probabilities and signal-to-noise ratios (SNRs), and quantify the attributes of the quadrature detection scheme. The adaptive detection scheme allows to perform the decoding of the quadratures with maximal efficiency at diverse channel conditions, and for arbitrarily distributed channel coefficients. In particular, it also allows to utilize the extra resources of multicarrier CVQKD and to maximize the amount of transmittable valuable information in diverse measurement and transmission conditions for any multicarrier CVQKD scenario.

This paper is organized as follows. Section 2 summarizes some preliminary findings. Section 3 proposes sub-channel estimation procedure for multicarrier CVQKD. Section 4 discusses the adaptive quadrature detection scheme. Section 5 extends the adaptive quadrature detection for a multiuser multicarrier scenario. Finally, Section 6 concludes the results. Supplemental information is included in the Appendix.

2 Preliminaries

In Section 2, we briefly summarize the notations and basic terms. For further information, see the detailed descriptions of [2–7].

2.1 Basic Terms and Definitions

2.1.1 Multicarrier CVQKD

In this section we very briefly summarize the basic notations of AMQD from [2]. The following description assumes a single user, and the use of $n$ Gaussian sub-channels $\mathcal{N}_i$ 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 $\mathcal{S}$, with i.i.d. Gaussian random position and momentum quadratures $x_j \in \mathbb{N}\left(0, \sigma_{x_0}^2\right)$, $p_j \in \mathbb{N}\left(0, \sigma_{p_0}^2\right)$, where $\sigma_{x_0}^2$ is the modulation variance of the quadratures. In the multicarrier scenario, the information is carried by Gaussian subcarrier CVs, $|\phi_i\rangle = |x_i + ip_i\rangle$, $x_i \in \mathbb{N}\left(0, \sigma_{x_0}^2\right)$, $p_i \in \mathbb{N}\left(0, \sigma_{p_0}^2\right)$, where $\sigma_{x_0}^2$ is the modulation variance of the subcarrier quadratures, which are transmitted through a noisy Gaussian sub-channel $\mathcal{N}_i$. Precisely, 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 a subcarrier CV, index $j$ to a single-carrier CV, respectively.)
The single-carrier state $|\varphi_j\rangle$ in the phase space $\mathcal{S}$ can be modeled as a zero-mean, circular symmetric complex Gaussian random variable $z_j \in \mathcal{CN}\left(0, \sigma^2_{\omega_j}\right)$, with a variance

$$\sigma^2_{\omega_j} = E\left[|z_j|^2\right] = 2\sigma^2_{\omega_j},$$

(1)

and with i.i.d. real and imaginary zero-mean Gaussian random components

$$\text{Re}\left(z_j\right) \in \mathbb{N}\left(0, \sigma^2_{\omega_j}\right), \quad \text{Im}\left(z_j\right) \in \mathbb{N}\left(0, \sigma^2_{\omega_j}\right).$$

(2)

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

$$z = x + ip = (z_0, \ldots, z_{n-1})^T \in \mathcal{CN}\left(0, K_z\right),$$

(3)

where each $z_j$ is a zero-mean, circular symmetric complex Gaussian random variable

$$z_j \in \mathcal{CN}\left(0, \sigma^2_{\omega_j}\right), \quad z_j = x_j + ip_j.$$  

(4)

In the first step of AMQD, Alice applies the inverse FFT (fast Fourier transform) operation to vector $z$ (see (3)), which results in an $n$-dimensional zero-mean, circular symmetric complex Gaussian random vector $d$, $d \in \mathcal{CN}\left(0, K_d\right)$, $d = (d_0, \ldots, d_{n-1})^T$, precisely as

$$d = F^{-1}\left(z\right) = \frac{e^{i\omega d} - e^{-i\omega d}}{2\sigma^2_{\omega}} = e^{-i\omega d} \sum_{j=0}^{n-1} e^{i\omega d},$$

(5)

where

$$d_i = x_i + ip_i, \quad d_i \in \mathcal{CN}\left(0, \sigma^2_{d_i}\right).$$

(6)

where $\sigma^2_{d_i} = E\left[|d_i|^2\right] = 2\sigma^2_{\omega}$, thus the position and momentum quadratures of $|\varphi_i\rangle$ are i.i.d. Gaussian random variables with a constant variance $\sigma^2_{\omega}$ for all $N_i, i = 0, \ldots, l - 1$ sub-channels:

$$\text{Re}\left(d_i\right) = x_i \in \mathbb{N}\left(0, \sigma^2_{\omega}\right), \quad \text{Im}\left(d_i\right) = p_i \in \mathbb{N}\left(0, \sigma^2_{\omega}\right),$$

(7)

where $K_d = \mathbb{E}\left[dd^\dagger\right]$, $\mathbb{E}\left[d\right] = \mathbb{E}\left[e^{i\gamma}d\right] = \mathbb{E}e^{i\gamma}\left[d\right]$, and $\mathbb{E}\left[dd^T\right] = \mathbb{E}\left[e^{i\gamma}d\left(e^{i\gamma}d\right)^T\right] = \mathbb{E}e^{i2\gamma}\left[dd^T\right]$ for any $\gamma \in \{0, 2\pi\}$. The $T(N)$ transmittance vector of $N$ in the multicarrier transmission is

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

(8)

where

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

(9)

is a complex variable, which quantifies the position and momentum quadrature transmission (i.e., gain) of the $i$-th Gaussian sub-channel $\mathcal{N}_i$, in the phase space $\mathcal{S}$, with real and imaginary parts.
0 ≤ \text{Re} T_i(\mathcal{N}_i) ≤ 1/\sqrt{2}, \text{ and } 0 ≤ \text{Im} T_i(\mathcal{N}_i) ≤ 1/\sqrt{2}.

(10)

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

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

(11)

where

\[ \text{Re} T_i(\mathcal{N}_i) = \text{Im} T_i(\mathcal{N}_i). \]

(12)

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

\[ |F(T_i(\mathcal{N}_i))|^2. \]

(13)

The \( n \)-dimensional zero-mean, circular symmetric complex Gaussian noise vector \( \Delta \in \mathbb{C}^n\left(0, \sigma^2_\Delta \right) \), of the quantum channel \( \mathcal{N} \), is evaluated as

\[ \Delta = (\Delta_0, \ldots, \Delta_{n-1})^T \in \mathbb{C}^n\left(0, \mathbf{K}_\Delta \right), \]

(14)

where

\[ \mathbf{K}_\Delta = \mathbb{E}\left[\Delta\Delta^\dagger\right], \]

(15)

with independent, zero-mean Gaussian random components

\[ \Delta_{x_i} \in \mathbb{N}\left(0, \sigma^2_{\mathcal{N}_i} \right), \text{ and } \Delta_{p_i} \in \mathbb{N}\left(0, \sigma^2_{\mathcal{N}_i} \right), \]

(16)

with variance \( \sigma^2_{\mathcal{N}_i} \), 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 \( x_i, p_i \) in the phase space \( \mathcal{S} \).

Thus \( F(\Delta) \in \mathbb{C}^n\left(0, \sigma^2_\Delta \right) \), where

\[ \sigma^2_{\Delta_i} = 2\sigma^2_{\mathcal{N}_i}. \]

(17)

The CVQFT-transformed noise vector can be rewritten as

\[ F(\Delta) = (F(\Delta_0), \ldots, F(\Delta_{n-1}))^T, \]

(18)

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

\[ \mathbf{K}_{F(\Delta)} = \mathbb{E}\left[F(\Delta)F(\Delta)^\dagger\right]. \]

(19)

### 3 Sub-channel Estimation for Multicarrier CVQKD

In the first part, we study the process of building multicarrier channel statistics. In the second part, we introduce the subcarrier spreading transmission technique, which minimizes the error probability of the estimation process in the presence of a Gaussian noise.
3.1 Sub-channel and Single-Carrier Channel Model

**Theorem 1** (Sub-channel estimation of multicarrier CVQKD). For any \( p_i \in \mathcal{C}, \ |p_i| > 0 \) pilot-subcarrier CV, the \( S_i(\mathcal{N}_i) \in \mathcal{C} \) sufficient statistic for the estimation of \( F(T_i(\mathcal{N}_i)) \) of \( \mathcal{N}_i \) is
\[
S_i(\mathcal{N}_i) = \varsigma_i |p_i'| = F(T_i(\mathcal{N}_i)) + F'(\Delta), \quad \text{where} \quad \varsigma_i = p_i/\|p_i\|^2, \quad p_i' = F(T_i(\mathcal{N}_i))p_i + F(\Delta), \quad F(\Delta) \in \mathbb{CN}(0,2\sigma_\Delta^2), \quad F'(\Delta) \in \mathbb{CN}(0,2\sigma_\Delta^2/\|p_i\|^2).
\]
The \( S(\mathcal{N}_j) \in \mathcal{C} \) of \( \mathcal{N}_j \) is \( S(\mathcal{N}_j) = \varsigma_j |q_j'| = A_j + F'(\Delta), \) where \( q_j = (p_{j,0}, \ldots, p_{j,l-1})^T \in \mathcal{C}^l \), \( q_j' = (p'_{j,0}, \ldots, p'_{j,l-1})^T \in \mathcal{C}^l \) are pilot-subcarrier CV vectors, \( A_j = \frac{1}{\mathbb{I}} \left( \sum_{i=0}^{l-1} F(T_{j,i}(\mathcal{N}_{j,i})) \right) \in \mathcal{C}^l \), \( \varsigma_j = q_j/\|q_j\|^2 \), and \( F'(\Delta) \in \mathbb{CN}(0,2\sigma_\Delta^2/\|q_j\|^2) \).

**Proof.**
The proof assumes the use of \( n \) sub-channels from which \( l, l < n \) sub-channels are selected via the proposed estimation process. For the sub-channel selection criteria, see the properties of AMQD modulation [2]. Throughout the manuscript we focus only on the \( l \) sub-channels that are used for valuable private information transmission in the multicarrier CVQKD protocol run. The \( i \)-th sub-channel is referred via \( \mathcal{N}_i \). From the \( l \) sub-channels, a \( j \)-th single-carrier channel is derived, depicted via \( \mathcal{N}_j \) [2-7]. In general, the referred channel output variables and vectors are yielding from a \( M_{\text{hom}} \) homodyne or \( M_{\text{het}} \) heterodyne measurement apparatus, respectively. These quantities are then post-processed via the corresponding functions and operators.
Let \( p_i \in \mathcal{C} \) be a complex scalar variable known by Alice and Bob (also referred to as a pilot-subcarrier CV), which is used for the estimation of the \( i \)-th Gaussian sub-channel \( \mathcal{N}_i \). (Note: the pilot CVs carry no valuable information and used in the sub-channel estimation phase to determine the channel transmittance coefficients).

In particular, in an AMQD multicarrier CVQKD setting [2], \( p_i \) is defined via the inverse Fourier operation as
\[
p_i = F^{-1}(p_j) = x_{p_i} + ip_{p_i}, \quad (20)
\]
which identifies a pilot-subcarrier CV with position and momentum quadratures \( x_{p_i} \) and \( p_{p_i} \), respectively, \( \sigma_{\omega_{p_i}}^2 = \mathbb{E}\left[ |p_i|^2 \right] = 2\sigma_{\omega_i}^2 \), for the estimation of the \( F(T_i(\mathcal{N}_i)) \) transmittance coefficient of the sub-channel \( \mathcal{N}_i \), and where \( p_j \) is referred to as the single-carrier pilot CV with quadrature components \( x_{p_j} \) and \( p_{p_j} \), evaluated as
\[
p_j = F(p_i) = x_{p_j} + ip_{p_j}, \quad (21)
\]
where \( F(\cdot) \) stands for the Fourier operator, \( \sigma_{\omega_{p_j}}^2 = \mathbb{E}\left[ |p_j|^2 \right] = 2\sigma_{\omega_j}^2 \).
The $p'_i$ output of $\mathcal{N}_i$ is expressed as
\[
p'_i = F(T_i(\mathcal{N}_i))p_i + F(\Delta).
\] (22)

Then let
\[
\zeta_i = \frac{p_i}{|p_i|},
\] (23)
from which the $\mathcal{S}_i(\mathcal{N}_i)$ sufficient statistics \[23-25\] is defined as follows:
\[
\mathcal{S}_i(\mathcal{N}_i) = \zeta_i^* p'_i
= \frac{p_i}{|p_i|} F(T_i(\mathcal{N}_i)) + F'(\Delta),
\] (24)

where
\[
F'(\Delta) \in \mathcal{CN}(0,2\sigma^2\mathcal{N}/|p_i|^2).
\] (25)

To estimate $F(T_i(\mathcal{N}_i))$ from $\mathcal{S}_i(\mathcal{N}_i)$, one can utilize the $\mathcal{E}$ mean square error \[23-25\] as
\[
\mathcal{E} = \mathbb{E} \left[ |F(T_i(\mathcal{N}_i)) - \zeta(F(T_i(\mathcal{N}_i)))|^2 \right],
\] (26)

where $\zeta(F(T_i(\mathcal{N}_i)))$ is the linear estimate of $F(T_i(\mathcal{N}_i))$, evaluated as
\[
\zeta(F(T_i(\mathcal{N}_i))) = \mathbb{E} \left[ F(T_i(\mathcal{N}_i)) | \mathcal{S}_i(\mathcal{N}_i) \right].
\] (27)

Without loss of generality, the minimum mean squared error $E$ is expressed as
\[
E = \min(\mathcal{E}) = \frac{\mathbb{E}[F(T_i(\mathcal{N}_i))^2]}{\mathbb{E}[|p_i|]} \frac{2\sigma^2}{|p_i|^2 + 2\sigma^2}. \]
(28)

In particular, from the orthogonality property \[23\] follows that
\[
\mathbb{E} \left[ (\zeta(F(T_i(\mathcal{N}_i))) - F(T_i(\mathcal{N}_i))|\mathcal{S}_i(\mathcal{N}_i))^2 \right] = 0.
\] (29)

The $\zeta(F(T_i(\mathcal{N}_i)))$ in (27) can be rewritten as
\[
\zeta(F(T_i(\mathcal{N}_i))) = C^\dagger \mathcal{S}_i(\mathcal{N}_i),
\] (30)

where $C \in \mathbb{C}$ refers to a constant complex variable, defined as
\[
C = \frac{\mathbb{E}[F(T_i(\mathcal{N}_i))^2]}{\mathbb{E}[|F(T_i(\mathcal{N}_i)|^2] + 2\sigma^2}. \]
(31)

Thus, $\zeta(F(T_i(\mathcal{N}_i)))$ can be expressed as
\[
\zeta(F(T_i(\mathcal{N}_i))) = \frac{\mathbb{E}[F(T_i(\mathcal{N}_i))^2]}{\mathbb{E}[|F(T_i(\mathcal{N}_i)|^2] + 2\sigma^2} \bigg( F(T_i(\mathcal{N}_i)) + F'(\Delta) \bigg). \]
(32)

As follows, $\mathcal{S}_i(\mathcal{N}_i)$ is provably a sufficient statistics to achieve the linear estimation of $F(T_i(\mathcal{N}_i))$ with minimum mean squared error $E$.

The results can be extended to the transmission of the $j$-th single-carrier Gaussian CV as follows.
The single-carrier level channel \( \mathcal{N}_j \) utilizes \( l \) Gaussian sub-channels, \( \mathcal{N}_j = (\mathcal{N}_{j,0}, \ldots, \mathcal{N}_{j,l-1})^T \), and the output \( p_j' \) is evaluated as
\[
p_j' = A_j p_j + F(\Delta),
\] (33)
where \( A_j \) is the transmittance coefficient of \( \mathcal{N}_j \), averaged from the \( l \) sub-channels,
\[
A_j = \frac{1}{l} \left( \sum_{i=0}^{l-1} F(T_{j,i}(\mathcal{N}_{j,i})) \right) \in \mathcal{C},
\] (34)
while \( p_j \in \mathbb{CN}(0,2\sigma_w^2) \) is the \( j \)-th Gaussian single-carrier input CV, and \( p_j' \in \mathbb{CN}(0,2\left(\sigma^2 + \sigma_N^2\right)) \), where \( \sigma_N^2 \) is the separated quadrature noise variance of \( \mathcal{N}_j \).

A \( \mathbf{q}_j \) pilot-subcarrier CV vector is defined as
\[
\mathbf{q}_j = (p_{j,0}, \ldots, p_{j,l-1})^T \in \mathcal{C}^l,
\] (35)
where \( p_{j,i} \) is transmitted through the Gaussian sub-channel \( \mathcal{N}_{j,i} \).

The \( \mathbf{q}_j' \) output vector is as
\[
\mathbf{q}_j' = A_j \mathbf{q}_j + F(\mathbf{v}(\Delta)) = (p_{j,0}', \ldots, p_{j,l-1}')^T \in \mathcal{C}^l,
\] (36)
where \( F(\mathbf{v}(\Delta)) \) is the \( l \)-dimensional noise vector
\[
F(\mathbf{v}(\Delta)) = (F(\Delta_0), \ldots, F(\Delta_{l-1}))^T \in \mathbb{CN}(0,2\sigma_N^2 I),
\] (37)
where \( I \) is the \( l \times l \) identity. The \( \mathcal{S}(\mathcal{N}_j) \in \mathcal{C} \) sufficient statistics for \( \mathcal{N}_j \) is then evaluated as
\[
\mathcal{S}(\mathcal{N}_j) = \mathcal{S}_j \mathbf{q}_j' = \frac{\mathbf{q}_j'}{|\mathbf{q}_j'|} \mathbf{q}_j' = A_j + F'(\Delta)
\] (38)
where
\[
\mathcal{S}_j = \frac{|\mathbf{q}_j'|}{|\mathbf{q}_j|},
\] (39)
\[
F'(\Delta) \in \mathbb{CN}(0,2\sigma_N^2 |\mathbf{q}_j|^2).
\] (40)

Then similar to (31), \( \mathbf{C} \in \mathcal{C}^l \) can be defined specifically as
\[
\mathbf{C} = \frac{E[|A_j|^2]}{E[|A_j|^2 |\mathbf{q}_j|^2 + 2\sigma_N^2]} \mathbf{q}_j,
\] (41)
from which \( \zeta(A_j^2) \) of \( A_j \) is yielded as
\[
\zeta(A_j) = CS(N_j)
\]
\[
= \frac{E[H_j]}{E[H_j]} q_j \frac{q_j^\dagger}{|q_j|^2} q_j^\prime
\]
\[
= \frac{E[H_j]}{E[H_j]} q_j^\prime.
\]
Thus, the E minimum mean squared error is precisely
\[
E = \frac{E[H_j]}{E[H_j]} 2 \sigma_{N_j}^2.
\]
In particular, the determination of \( S(N_j) \) in (38) can be interpreted via a projection \( P \) in \( C^l \).
The noisy vector \( q_j^\prime \) is projected onto \( \zeta_j = q_j / |q_j|^2 \), which results the scalar quantity
\( S(N_j) = \zeta_j q_j^\prime = A_j + F'(\Delta) \).
The projection of \( q_j^\prime \) onto \( \zeta_j \) in the phase space \( S \) is illustrated in Fig. 1.

\textbf{Figure 1.} Determination of \( S(N_j) \) sufficient statistics via projection \( P \) in \( C^l \). The noisy vector \( q_j^\prime \) is projected onto \( \zeta_j \), which results the scalar quantity \( S(N_j) = \zeta_j q_j^\prime \) (\( x \), position quadrature; \( p \), momentum quadrature).

The noise ratio of the estimation process on the \( x \) position and \( p \) momentum quadrature components separately can be identified by \( \vartheta \) as
\[
\vartheta = \frac{\left((\chi(C))^T \chi(q_j)\right)^T E[\chi(A_j)^2]}{|\chi(C)|^2 \sigma_{N_j}^2},
\]
where function \( \chi(\cdot) \) separately identifies the \( x \) position or \( p \) momentum quadrature components as \( \text{Re}(\cdot) \) and \( \text{Im}(\cdot) \), respectively. Note that
\[
\left((\chi(C))^T \chi(q_j)\right)^2 \leq |\chi(C)|^2 |\chi(q_j)|^2,
\]
by some fundamental theory [23-25].
The $p_{\text{err}}(p^\prime_x)$ of a noisy pilot-subcarrier CV $p^\prime_x$ determines the noise of $\zeta(F(T_i(N_i)))$. Since the $p_{\text{err}}(p^\prime_x)$ quantifies the amount of noise $F(\Delta)$ on $p^\prime_x$ and $S_i(N_i)$ (see (22), (24)), we derive this quantity by $\zeta(F(T_i(N_i)))$ via an exact formula, as follows.

Let assume the case that $p_i = \text{Re}(p_i) + \text{Im}(p_i) = x_{p_i} + ip_{p_i} \in \mathbb{C}$, $|p_i| > 0$ is a constant $p_i = p_x$ complex variable (CV quantum state with position $x_{p_i}$ and momentum quadrature $p_{p_i}$) for all $N_i, i = 0, \ldots, l - 1$ (which is reasonable in a practical CVQKD calibration phase), the error probability of the detection of the noisy $p^\prime_x$ pilot-subcarrier CVs is evaluated as follows.

Let $p_x \in \mathbb{C}^l$ identify an $l$-dimensional complex pilot-subcarrier CV vector,

$$p_x = (p_{x,0}, \ldots, p_{x,l-1})^T,$$

where $p_{x,i}$ is the pilot-subcarrier CV of sub-channel $N_i, i = 0, \ldots, l - 1$, such that

$$p_{x,i} = p_x \in \mathbb{C}, i = 0, \ldots, l - 1,$$

and $p'_x$ the output vector as $p'_x = (p'_{x,0}, \ldots, p'_{x,l-1})^T$.

Let $p_i = p_{x,i}$ for all $i$, then

$$p'_x = \zeta(F(v(N_i)))p_x + F(v(\Delta)),\quad (48)$$

which can be rewritten as

$$p'_x = \zeta(F(v(N_i)))p_x + F(v(\Delta)),\quad (49)$$

where $\zeta(F(v(N_i)))$ is expressed as

$$\zeta(F(v(N_i))) = (\zeta(F(T(N_0))), \ldots, \zeta(F(T(N_{l-1}))))^T,$$

where $v(N)$ is the $l$-dimensional sub-channel vector.

Without loss of generality, the $S(p'_x)$ sufficient statistics for the detection of $p'_x$ is then yielded [23] precisely as

$$S(p'_x) = \eta^l p'_x$$

$$= \frac{\zeta(F(v(N_i)))}{\| F(v(N_i)) \|} p'_x$$

$$= [\zeta(F(v(N_i)))][p_x + \frac{\zeta(F(v(N_i)))}{\| F(v(N_i)) \|} F(v(\Delta))],$$

where

$$\eta = \frac{\zeta(F(v(N_i)))}{\| F(v(N_i)) \|},$$

and

$$\eta^l F(v(\Delta)) \in \mathbb{C}N(0, 2\sigma^2_N).$$

Specifically, assuming that each $\zeta(T(N_i))$ of $\zeta(v(N))$ has a distribution of

$$\zeta(T(N_i)) \in \mathbb{C}N(0, \sigma^2_{\zeta(T(N_i))}),$$

(54)
the quantity of $|\zeta(F(v(N)))|^2$ is $\chi^2$ Chi-square distributed [23-25] with $2l$ degrees of freedom, which yields a density $f_{\chi^2}(x)$ precisely as
\[ f_{\chi^2}(x) = \frac{1}{(l-1)!} x^{l-1} e^{-x}, \] (55)
where $x \geq 0$. In particular, the density of (55) at $x \to 0$ is simplified into
\[ f_{\chi^2}(x) = \frac{1}{(l-1)!} x^{l-1}. \] (56)
From (55), the $p_{err}(p'_z)$ error probability of the detection of $p'_z$ for the $l$ sub-channels is
\[
p_{err}(p'_z) = \int_0^{\infty} Q\left(\sqrt{2xSNR} \right) f_{\chi^2}(x) \, dx
\]
\[
= \left(1 - \frac{\sqrt{SNR}}{\sqrt{SNR}} \right) \sum_{i=0}^{l-1} \binom{l-1+i}{i} \left(\frac{1+\sqrt{SNR}}{2} \right)^i,
\] (57)
where $Q(\cdot)$ is the Gaussian tail function [23], and $\sqrt{SNR}$ is a scaled SNR quantity as
\[
\sqrt{SNR} = \frac{0.5p'_z}{2\sigma_N} = \frac{1}{2}SNR,
\] (58)
where $SNR$ is the complex SNR.
The $p_{err}(p'_z | \zeta(F(v(N))))$ conditional error probability is evaluated as [23]
\[
p_{err}(p'_z | \zeta(F(v(N)))) = Q\left(\sqrt{2\zeta(F(v(N)))} \right) \sqrt{SNR}.
\] (59)
In particular, the result in (57) at $SNR > 1$ is simplified into
\[
p_{err}(p'_z) = \left(1 - \frac{\sqrt{SNR}}{\sqrt{SNR}} \right) \binom{2l-1}{l}. \] (60)
Introducing an error event
\[
E: |\zeta(F(v(N)))|^2 < \frac{1}{SNR}, \] (61)
the corresponding $Pr(E)$ is
\[
Pr(E) \approx p_{err}(p'_z), \] (62)
which is at $x \to 0$ without loss of generality is yielded as
\[
Pr(E) = \int_0^{\frac{1}{\sqrt{SNR}}} f_{\chi^2}(x) \, dx
\]
\[
= \int_0^{\frac{1}{\sqrt{SNR}}} \frac{1}{(l-1)!} x^{l-1} \, dx.
\] (63)
For the subcarrier spreading-based sub-channel estimation scheme with a theoretical minimum of $p_{err}$ in the presence of a Gaussian noise, see Lemma 1. ■
3.2 Sub-channel Estimation with Subcarrier Spreading

Lemma 1 (Subcarrier spreading-based sub-channel estimation for multicarrier CVQKD). The subcarrier spreading results in a minimized sub-channel estimation error \( p_{err} = \mathcal{O}\left(\sqrt{\frac{1}{2\sigma_N^2}}\right) \), where \( \sigma_N = \left| \mathbf{p}_x \right|^2 / g \), and \( \mathbf{p}_x \in \mathbb{C}^g \) is \( g \)-dimensional pilot-subcarrier CV vector.

Proof. In Theorem 1, it has been already shown that the \( p_{err}(p'_x) \) error probability quantifies the amount of noise on the \( S \) sufficient statistics. Here we prove that the error of the sub-channel estimation can be minimized via a technique, called subcarrier spreading. This type of transmission technique allows to evaluate \( \zeta(F(T(N_i))) \) with minimal error.

Let \( \mathbf{q}_x \in \mathbb{C}^g \) be a \( g \)-dimensional pilot-subcarrier CV vector
\[
\mathbf{q}_x = \left( p_{x,0}, \ldots, p_{x,g-1} \right)^T,
\]
where
\[
g + (l-1) = n,
\]
and \( p_{x,i} \) is sent through sub-channel \( N_i \), \( i = 0, \ldots, l-1 \), \( l < n \).

Then define \( n \)-dimensional vector \( \mathbf{P}_i \in \mathbb{C}^n \), \( i = 0, \ldots, l-1 \) precisely as
\[
\mathbf{P}_i = \left( \mathbf{a}_i, \mathbf{q}_x, \mathbf{b}_0 \right),
\]
where \( \mathbf{a}_0 \) is an \( i \)-dimensional vector
\[
\mathbf{a}_0 = \left( \rho_0^0, \ldots, \rho_{i-1}^0 \right)^T,
\]
where \( \rho_w^0 = |0\rangle\langle 0|, w = 0, \ldots, i-1 \), and \( \mathbf{b}_0 \) is an \( u = (l-1) - i \)-dimensional vector
\[
\mathbf{b}_0 = \left( \rho_0^0, \ldots, \rho_{u-1}^0 \right)^T,
\]
where \( \rho_w^0 = |0\rangle\langle 0|, w = 0, \ldots, u - 1 \).

Then for any \( i \), without loss of generality,
\[
\left| \left( \mathbf{P}_i^\dagger \right)^\dagger \mathbf{P}_m^m \right| < \left| \mathbf{q}_x \right|^2 = \sum_{i=0}^{g-1} \left| p_{x,i} \right|^2,
\]
where \( m \neq i \). Assuming full orthogonality [23], for any \( m \neq i \),
\[
\left( \mathbf{P}_i^i \right) \left( \mathbf{P}_m^m \right) = 0.
\]

Then let output of the \( i \)-th iteration is
\[
\mathbf{P}_i' = F(T_i(N_i))\mathbf{P}_i + F(V_i(\Delta))
\]
where \( N_i \) is the \( i \)-th sub-channel of the total \( l \) “good” sub-channels, and \( F(V_i(\Delta)) \) is an \( n \)-dimensional vector.

The \( \mathbf{P}_i' \) outputs of the \( l \) iterations formulate the output vector \( \mathbf{P}_{out} \) as
\[
\mathbf{P}_{\text{out}} = \sum_{l} \mathbf{P}_{x}^{l} = \sum_{l} F(T_{l}(\mathcal{N}_{i})) \mathbf{P}_{x}^{l} + F(\mathbf{V}^{l}(\Delta)). \tag{72}
\]

After some calculations, \(p_{\text{err}}\) is yielded as
\[
p_{\text{err}} = \mathbb{E} \left[ Q \left( \sqrt{\frac{|\mathbf{p}_{x}^{l} \sum_{i=0}^{l-1} F(T_{l}(\mathcal{N}_{i}))|^{2}}{g2\sigma_{N}^{2}}} \right) \right]. \tag{73}
\]

Assuming that \(p_{x,i} = p_{x} \in \mathcal{C}, i = 0, \ldots, g-1\) holds in (64), the vector \(\mathbf{q}_{x}\) can be rewritten as a \(\mathbf{p}_{x}\) vector,
\[
\mathbf{p}_{x} = (p_{x,0}, \ldots, p_{x,g-1})^{T}, \quad (74)
\]
and further assuming that each \(F(T(\mathcal{N}_{i}))\) has a distribution of \(F(T(\mathcal{N}_{i})) \in \mathcal{C} \mathbb{N} \left( 0, \sigma_{T(\mathcal{N}_{i})}^{2} \right)\), (73) results in
\[
p_{\text{err}}(\mathbf{p}_{x}^{l}) = \left( 1 - \frac{\text{SNR}}{2} \right)^{l-1} \sum_{i=0}^{l-1} \left( l - 1 + i \right) \left( 1 + \frac{\text{SNR}}{2} \right) i, \quad (75)
\]
which coincidences with (57), and
\[
\text{SNR} = \frac{0.5 \mathbf{p}_{x}}{2\sigma_{N}^{2}} = \frac{1}{2} \text{SNR}. \tag{76}
\]
From the law of large numbers, for \(l \to \infty\) follows that
\[
\mathbb{E} \left[ \sum_{l} \left| F(T(\mathcal{N}_{i})) \right|^{2} \right] = 1 \tag{77}
\]
with unit probability, which allows to rewrite (73) specifically as
\[
p_{\text{err}} = \mathbb{E} \left[ Q \left( \sqrt{\frac{|\mathbf{p}_{x}^{l} \sum_{i=0}^{l-1} F(T_{l}(\mathcal{N}_{i}))|^{2}}{g2\sigma_{N}^{2}}} \right) \right]
= \mathbb{E} \left[ Q \left( \sqrt{\frac{\mathbf{p}_{x}^{l} \sum_{i=0}^{l-1} F(T_{l}(\mathcal{N}_{i}))}{2\sigma_{N}^{2}}} \right) \right]
= Q\left( \sqrt{\frac{\mathbf{T}_{l} \frac{1}{2\sigma_{N}^{2}}} \right)
= Q\left( \sqrt{2\text{SNR}} \right)
= Q\left( \sqrt{\text{SNR}} \right), \quad (78)
\]
where
\[
\mathbf{T} = \frac{\mathbf{p}_{x}^{l} \sum_{i=0}^{l-1} F(T_{l}(\mathcal{N}_{i}))}{g}, \tag{79}
\]
In particular, projecting \(\mathbf{P}_{x}^{l}\) onto \(\mathbf{\varsigma}_{x} = \mathbf{P}_{x}^{l} / \mathbf{|P}_{x}^{l}|\) results \(\mathcal{S}(\mathcal{N}_{i})\) as [23]

13
\[ S\left( \mathcal{N}_i \right) = \varsigma_i^\dagger \mathbf{P}_s \]
\[
= \left[ \mathbf{P}_s \right]^\dagger \left( F(T_i(\mathcal{N}_i)) \mathbf{P}_i + F\left( \mathbf{V}^i(\Delta) \right) \right)
\]
\[ = F(T_i(\mathcal{N}_i)) \mathbf{P}_i + F(\Delta). \]

The subcarrier spreading technique is illustrated in Fig. 2 for \( n = 5, l = 3, g = 3 \). The subcarrier spreading technique scans through the \( n \) sub-channels to estimate the transmittance coefficients of the \( l \) “good” sub-channels \( \mathcal{N}_0, \mathcal{N}_1, \) and \( \mathcal{N}_4 \) (depicted by blue). The process iterates in \( l \) steps. The scanned sub-channels of the \( i \)-th iteration step are depicted by the thick frame.

![Figure 2](image)

**Figure 2.** The subcarrier spreading technique at \( n = 5, l = 3, g = 3 \). The \( n \) sub-channels are scanned over in \( l \) steps (a–c), \( i = 0, \ldots, l-1 \), utilizing \( g \) pilot-subcarrier CVs (sliding thick frame) in each iteration steps (The “good” sub-channels are depicted in blue.).

From (80), the \( \zeta(F(T_i(\mathcal{N}_i))) \) linear estimation of \( F(T_i(\mathcal{N}_i)) \) is expressed as
\[ \zeta(F(T_i(\mathcal{N}_i))) = \frac{\left[ \mathbf{P}_s \right]^\dagger}{\left[ \mathbf{P}_s \right]^\dagger + 2\sigma_i^2} S(\mathcal{N}_i), \]

which yields a \( \mathcal{E} \) mean square error without loss of generality as
\[ \mathcal{E} = \mathbb{E} \left[ \frac{1}{1 + \left[ \mathbf{P}_s \right]^\dagger + 2\sigma_i^2} \right], \]

and
\[ \text{SNR} = \frac{0.5 \left[ \mathbf{P}_s \right]^\dagger}{g \sigma_i^2} = \frac{0.5 \left[ \mathbf{P}_s \right]^\dagger}{2\sigma_i^2}. \]

Assuming that the sub-channel estimation phase is repeated for \( k \)-times, the resulting \( \zeta^{(k)}(F(T_i(\mathcal{N}_i))) \) is
\[ \zeta^{(k)}(F(T_i(\mathcal{N}_i))) = \frac{|P^*_x|}{kP^*_x + 2\sigma^2_x} \sum_k S(\mathcal{N}_i), \]  

(84)

from which

\[ \mathcal{E}^{(k)} = \mathbb{E} \left[ \frac{1}{1 + k|P^*_x|^2 / 2\sigma^2_x} \right], \]  

(85)

and

\[ \tilde{\text{SNR}}^{(k)} = \frac{0.5k|P^*_x|^2}{g2\sigma^2_x} = \frac{0.5k|P^*_x|^2}{2\sigma^2_x}. \]  

(86)

In particular, the resulting error probability is

\[ p_{err}^{(k)} = Q\left(\sqrt{2\text{SNR}^{(k)}}\right) \]
\[ = Q\left(\sqrt{k\frac{|P^*_x|^2}{2\sigma^2_x}}\right) \]
\[ = Q\left(\sqrt{k\text{SNR}}\right). \]

Hence, the subcarrier spreading technique allows us to construct \( \zeta(F(T(\mathcal{N}_i))) \) of \( F(T(\mathcal{N}_i)) \) with a theoretical error-minimum [23-25] in the presence of a Gaussian noise.

The \( p_{err} \) and \( p_{err}^{(k)} \) error probabilities of (57) and (87) for \( k = 2 \) at \( F(T(\mathcal{N}_i)) \in \mathcal{CN}(0,\sigma^2_{T(\mathcal{N}_i)}) \),

are compared in Fig. 3. By an averaging over \( \mathcal{CN}(0,\sigma^2_{T(\mathcal{N}_i)}) \), the results can be extended for arbitrary distributed \( F(T(\mathcal{N}_i)) \) sub-channel coefficients.

**Figure 3.** Comparison of the error probabilities of the sub-channel estimation \( (p_{err}) \) and the subcarrier spreading-based sub-channel estimation \( (p_{err}^{(k)}) \), at \( k = 1, 2, 4, 6, 8 \) and \( l \to \infty \), \( F(T(\mathcal{N}_i)) \in \mathcal{CN}(0,\sigma^2_{T(\mathcal{N}_i)}) \).
4 Adaptive Detection for Multicarrier CVQKD

First the results are proposed for single adaptive quadrature detection. The collective adaptive quadrature detection for multicarrier CVQKD is discussed in the second part.

4.1 Single Adaptive Quadrature Detection

**Proposition 1** (Single adaptive multicarrier detection). For any $z \in \mathbb{C}(0,2\sigma^2_{\omega_b})$, the $S$ for a single detection is $S = \nu^\dagger z'$, where $\nu = A/[A]$, $A = \frac{1}{\xi} \sum_{i=0}^{l-1} F(T_i(\mathcal{N}_i))$, $Az \in \mathbb{C}(0,2\sigma^2_{\omega_b})$, $z' = Az + F(\Delta) \in \mathbb{C}(0,2(\sigma^2_{\omega_b} + \sigma^2_N))$, and $\nu^\dagger F(\Delta) \in \mathbb{C}(0,2\sigma^2_N)$.

**Proof.**

The first part of the proof discusses the $M_{\text{hom}}$ homodyne detection. In the second part, the results for the $M_{\text{het}}$ heterodyne measurement setting are derived.

Let $\chi(z')$, $z' \in \mathbb{C}(0,2(\sigma^2_{\omega_b} + \sigma^2_N))$ identify the result of an $M_{\text{hom}}$ single homodyne measurement applied on the output Gaussian CV $\phi_j^\dagger$ as

$$x', p' \in \mathbb{N}(0,\sigma^2_{\omega_b} + \sigma^2_N),$$

where $x', p'$ stands for the position and momentum quadrature of $z' = x' + ip'$.

The term $\chi(z')$ can be rewritten as

$$\chi(z') = \left(\frac{1}{\xi} \sum_{i=0}^{l-1} F(\chi(T_i(\mathcal{N}_i)))\right) \chi(z) \in \mathbb{N}(0,\sigma^2_{\omega_b} + \sigma^2_N),$$

and $\nu$ can be defined as

$$\chi(\nu) = \frac{\chi(A)}{[A]} = \frac{\left[\sum_{i=0}^{l-1} F(\chi(T_i(\mathcal{N}_i)))\right]}{\left[\sum_{i=0}^{l-1} F(\chi(T_i(\mathcal{N}_i)))\right]},$$

In particular, from $\chi(z')$ and $\chi(\nu)$, the $S = (\chi(\nu))^T \chi(z')$ sufficient statistics [23] in $\mathbb{R}$ is as follows:

$$S = (\chi(\nu))^T \chi(z')$$

$$= \frac{(\chi(A))^T}{[A]^T} \chi(z')$$

$$= \left(\frac{1}{\xi} \sum_{i=0}^{l-1} F(\chi(T_i(\mathcal{N}_i)))\right) \chi(z') + \frac{\left[\sum_{i=0}^{l-1} F(\chi(T_i(\mathcal{N}_i)))\right]}{\left[\sum_{i=0}^{l-1} F(\chi(T_i(\mathcal{N}_i)))\right]} \chi(F(\Delta)),$$

where $\chi(F(\Delta)) \in \mathbb{N}(0,\sigma^2_N)$.

For $M_{\text{het}}$, let the output be identified via operator $\Lambda(\cdot)$ as

$$\Lambda(z') \in \mathbb{C}(0,2c(\sigma^2_{\omega_b} + \sigma^2_N)),$$

where $c$ is a constant.
where \( c \) is a real variable, and without loss of generality let \( F\left( \Lambda \left( T_i \left( \mathcal{N}_i \right) \right) \right) \in \mathbb{C}N\left( 0, c^2 \sigma_N^2 \right) \), and

\[
\tilde{\mathcal{O}} = \frac{\Lambda(A)}{|A|} = \frac{\frac{1}{t} \sum_{i=1}^{t-1} F\left( \Lambda \left( T_i \left( \mathcal{N}_i \right) \right) \right)}{\frac{1}{t} \sum_{i=0}^{t-1} |F\left( \Lambda \left( T_i \left( \mathcal{N}_i \right) \right) \right)|}
\]

(93)

thus,

\[
\mathcal{S} = \tilde{\mathcal{O}}^\dagger \Lambda \left( z' \right) = \frac{\Lambda(A)}{|A|} \Lambda \left( z' \right)
\]

\[
= \left( \frac{1}{t} \sum_{i=0}^{t-1} \left| F\left( \Lambda \left( T_i \left( \mathcal{N}_i \right) \right) \right) \right| \right) \Lambda \left( z' \right) + \frac{\frac{1}{t} \sum_{i=0}^{t-1} |F\left( \Lambda \left( T_i \left( \mathcal{N}_i \right) \right) \right)|}{\frac{1}{t} \sum_{i=0}^{t-1} |F\left( \Lambda \left( T_i \left( \mathcal{N}_i \right) \right) \right)|} \Lambda \left( F \left( \Delta \right) \right),
\]

(94)

where \( \Lambda \left( F \left( \Delta \right) \right) \in \mathbb{C}N\left( 0, c^2 \sigma_N^2 \right) \).

The result in (94), at \( c = 1 \), can be rewritten as

\[
\mathcal{S} = \nu^\dagger z' = \frac{\tilde{\mathcal{O}}^\dagger z'}{|\tilde{\mathcal{O}}^\dagger|}
\]

\[
= \left( \frac{1}{t} \sum_{i=0}^{t-1} \left| F\left( \Lambda \left( T_i \left( \mathcal{N}_i \right) \right) \right) \right| \right) z + \frac{\frac{1}{t} \sum_{i=0}^{t-1} |F\left( \Lambda \left( T_i \left( \mathcal{N}_i \right) \right) \right)|}{\frac{1}{t} \sum_{i=0}^{t-1} |F\left( \Lambda \left( T_i \left( \mathcal{N}_i \right) \right) \right)|} F \left( \Delta \right)
\]

(95)

which provides \( \mathcal{S} = \tilde{\mathcal{O}}^\dagger z' \) in the \( C \) complex space.

Note that if \( z' = x' + ip' \), the condition

\[
x' \in \mathbb{N} \left( 0, \sigma_x^2 + \sigma_N^2 \right) = p' \in \mathbb{N} \left( 0, \sigma^2 + \sigma_N^2 \right)
\]

(96)

is satisfied, then \( \mathcal{S} \) can also be extracted in \( \mathbb{R} \), using \( \chi \left( F \left( \Delta \right) \right) \in \mathbb{N} \left( 0, \sigma_N^2 \right) \in \mathbb{R} \), as shown in (91).

The results are proposed for collective adaptive quadrature detection in Theorem 2.

### 4.2 Collective Adaptive Quadrature Detection

**Theorem 2 (Sufficient statistics for collective adaptive detection).** For a \( d \)-dimensional input \( z = \text{diag} \left( z_0, \ldots, z_{d-1} \right) \in \mathbb{C}N \left( 0, K_z \right) \), the sufficient statistics is \( \mathcal{S}^d = \left( \nu^d \right)^\dagger z' \), where \( \nu^d = A^\dagger M^N \),

\[
A = \left[ \frac{1}{t} \sum_{i=0}^{t-1} F \left( T_{0,i} \left( \mathcal{N}_0,i \right) \right), \ldots, \frac{1}{t} \sum_{i=0}^{t-1} F \left( T_{d-1,i} \left( \mathcal{N}_{d-1,i} \right) \right) \right]^T,
\]

\( M^N \) is the codeword difference matrix of the \( N \) matrices \( z_0, \ldots, z_{N-1} \),

\[
z'^T = A^\dagger z + \left( F^d \left( \Delta \right) \right)^T \in \mathbb{C}N \left( 0, K_z' \right),
\]

where \( F^d \left( \Delta \right) = \left( F \left( \Delta_0 \right), \ldots, F \left( \Delta_{d-1} \right) \right)^T \in \mathbb{C}N \left( 0, K_{F^d(\Delta)} \right) \),

\[
|A| z \in \mathbb{C}N \left( 0, K_z \right).
\]
Proof.
Let the $d$-dimensional output $z'$ be given as
$$z'^T = A^\dagger z + \left(F^d(\Delta)\right)^T = (z'_0, \ldots, z'_{d-1}),$$
where $z = \text{diag}(z_0, \ldots, z_{d-1}) \in \mathbb{CN}(0, K_z)$ is a $d$-dimensional diagonal input matrix with $z_j \in \mathbb{CN}\left(0, 2\sigma^2_{w_0}\right)$, and $A$ is a $d$-dimensional vector with the $\frac{1}{l} \sum_{i=0}^{l-1} F\left(T_{j,i}\left(N_{j,i}\right)\right)$ averaged Fourier-transformed sub-channel coefficients for $z_j$, $j = 0, \ldots, d-1$, at $l$ sub-channels $N_{j,i}, i = 0, \ldots, l-1$, as
$$A = \left(A_0^\dagger, \ldots, A_{d-1}^\dagger\right)^T = \left(\frac{1}{l} \sum_{i=0}^{l-1} F\left(T_{0,i}\left(N_{0,i}\right)\right), \ldots, \frac{1}{l} \sum_{i=0}^{l-1} F\left(T_{d-1,i}\left(N_{d-1,i}\right)\right)\right)^T,$$
and
$$F^d(\Delta) = \left(F(\Delta_0), \ldots, F(\Delta_{d-1})\right)^T \in \mathbb{CN}(0, K_{F^d(\Delta)}),$$
$$z'_j = \left(\frac{1}{l} \sum_{i=0}^{l-1} F\left(T_{j,i}\left(N_{j,i}\right)\right)\right) z_j + F(\Delta) \in \mathbb{CN}\left(0, 2\left(\sigma^2_{w_0} + \sigma^2_N\right)\right).$$

From $A$, $|A|$ is expressed as
$$|A| = \sum_{j=0}^{d-1} |A_j| = \sum_{j=0}^{d-1} \frac{1}{l} \sum_{i=0}^{l-1} |F\left(T_{j,i}\left(N_{j,i}\right)\right)|;$$
thus,
$$|A| z = \sum_{j=0}^{d-1} \frac{1}{l} \sum_{i=0}^{l-1} |F\left(T_{j,i}\left(N_{j,i}\right)\right)||z| \in \mathbb{CN}(0, K_z),$$
whereas $z'^T$ is evaluated as
$$z'^T = \left(\frac{1}{l} \sum_{i=0}^{l-1} F\left(T_{0,i}\left(N_{0,i}\right)\right), \ldots, \frac{1}{l} \sum_{i=0}^{l-1} F\left(T_{d-1,i}\left(N_{d-1,i}\right)\right)\right) \text{diag}(z_0, \ldots, z_{d-1}) + \left(F(\Delta_0), \ldots, F(\Delta_{d-1})\right)^T \in \mathbb{CN}(0, K_{z'}).$$

Note that in a CVQKD setting, private classical information (i.e., $d$-dimensional random private classical $p$ codewords) is shared between the legal parties. Thus, in particular, using $z_A$ and $z_B$, the $d$-dimensional random private codewords $p_A$ and $p_B$ [5-7] are defined with the relation
$$C_{p_A} \subseteq C_{z_A},$$
and
$$C_{p_B} \subseteq C_{z_B},$$
where $\{C_{z_A}, C_{z_B}\}$ and $\{C_{p_A}, C_{p_B}\}$ are the corresponding phase-space constellations of $z_A, z_B$, and $p_A, p_B$, respectively. Because the results for $z$ trivially follow for any $p$, the proof demonstrates the decoding of $z$.

Using (97), $z$ at $N = 2$ is
$$A^\dagger z \in \{A^\dagger z_A, A^\dagger z_B\},$$
where \( z_A = \text{diag}(z_{A,0}, \ldots, z_{A,d-1}) \in \mathcal{CN}(0, K_{z_A}) \) and \( z_B = \text{diag}(z_{B,0}, \ldots, z_{B,d-1}) \in \mathcal{CN}(0, K_{z_B}) \).

Without loss of generality, let the number of \( d \)-dimensional input codewords, \( N = 2 \), be denoted by \( z_A \) and \( z_B \). The results can be extended for arbitrary \( N \).

Projecting \( z' \) onto the \( d \)-dimensional unit vector \( \nu^d \), such that
\[
\nu^d = A^\dagger M^2,
\]
where \( M^2 \) is the codeword difference matrix at \( N = 2 \), expressed as
\[
M^2 = z_A - z_B.
\]
From (107) and (108), the \( S^d \) sufficient statistic is precisely as follows
\[
S^d = (\nu^d)^\dagger z' = s \left| A^\dagger M^2 \right| + F(\Delta),
\]
where
\[
s \in \{-0.5, 0.5\} \in \mathbb{R}
\]
and \( F(\Delta) \in \mathcal{CN}(0,2\sigma^2_N) \) are scalars.

To verify (109), first we rewrite (106) as
\[
A^\dagger z = s \left( A^\dagger z_A - A^\dagger z_B \right) + \frac{1}{2} \left( A^\dagger z_A + A^\dagger z_B \right),
\]
which lies in a \( \gamma \) subspace of one \( \mathbb{R} \) real dimension. From (111), let \( Z' \) be defined as
\[
Z'^T = z'^T - \frac{1}{2} \left( A^\dagger z_A + A^\dagger z_B \right)
\]
\[
= A^\dagger z + \left( F^d(\Delta) \right)^T - \frac{1}{2} \left( A^\dagger z_A + A^\dagger z_B \right)
\]
\[
= s \left( A^\dagger z_A - A^\dagger z_B \right) + \left( F^d(\Delta) \right)^T,
\]
where \( F^d(\Delta) \in \mathcal{CN}(0,2\sigma^2_N I) \).

Specifically, using the results obtained in (111) and (112), \( \nu^d \) can be expressed as
\[
\nu^d = \frac{A^\dagger (z_A - z_B)}{\left| A^\dagger (z_A - z_B) \right|} = \frac{A^\dagger M^2}{\left| A^\dagger M^2 \right|}
\]
Thus, projecting \( z' \) along \( \nu^d \) via \( P(z') \) yields a complex scalar \( \Gamma \in \mathcal{C} \) as follows:
\[
P(z') = (\nu^d)^\dagger Z'
\]
\[
= (\nu^d)^\dagger \left( z' - \frac{1}{2} \left( A^\dagger z_A + A^\dagger z_B \right) \right)^T
\]
\[
= s \left( A^\dagger z_A - A^\dagger z_B \right) + F(\Delta)
\]
\[
= s \left| A^\dagger M^2 \right| + F(\Delta)
\]
\[
= \Gamma,
\]
where \( F(\Delta) \in \mathcal{CN}(0,2\sigma^2_N) \) is a complex scalar.

Thus, \( \text{Re}(\Gamma) \in \mathbb{R} \) and \( \text{Im}(\Gamma) \in \mathbb{R} \) are real variables with noise
\[ \chi(F(\Delta)) \in \mathbb{N}\left(0, \sigma_X^2\right), \]

which identifies the \( \text{Re}(F(\Delta)) \in \mathbb{N}\left(0, \sigma_X^2\right) \) real or \( \text{Im}(F(\Delta)) \in \mathbb{N}\left(0, \sigma_X^2\right) \) imaginary component of \( F(\Delta) \in C\mathbb{N}\left(0,2\sigma_X^2\right) \), respectively.

In particular, the fact that the result \( \Gamma \) of the \( \mathcal{P} \) projection contains all information for the decoding is verified as follows. Let \( G_{uv} \) be an orthogonal matrix \([23]\), where \( uv \) indexes the row and column of \( G \). Let \( G_{1u} \equiv A \), and let the other unit norm rows to be orthogonal to \( A \) and to each other. Then, (114) yields a vector \( L \) precisely as

\[
L = G\left(z'^T - \frac{1}{2}(A^\dagger z_A + A^\dagger z_B)\right) = \begin{pmatrix} s \left| \left(A^\dagger z_A - A^\dagger z_B\right)\right| \\ 0 \\ \vdots \\ 0 \end{pmatrix} + GF^d(\Delta),
\]

where \( GF^d(\Delta) \in C\mathbb{N}\left(0,2\sigma_X^2I\right) \), and \( I \) is the \( d \times d \) identity. From \( L \), only \( s \left| \left(A^\dagger z_A - A^\dagger z_B\right)\right| \) (i.e., the first component of \( L \)) is not independent from \( s \) and \( F^d(\Delta) \). Thus, all information is conveyed in the first component of \( L \), which exactly coincides with (114).

Exploiting some fundamentals of the maximum likelihood theory \([23-25]\), the decision rule in \( \mathcal{C}^d \) with respect to the \( \mathbb{R}^d \ d\)-dimensional subspace with \( \chi(F^d(\Delta)) \in C\mathbb{N}\left(0,\sigma_X^2I\right) \) is as

\[
A^\dagger z = A^\dagger z_A : \frac{1}{(\pi\sigma_X^2)^{d/2}} e^{\left(-\frac{\left| z'^T - A^\dagger z_A \right|^2}{2\sigma_X^2}\right)} \geq \frac{1}{(\pi\sigma_X^2)^{d/2}} e^{\left(-\frac{\left| z'^T - A^\dagger z_A \right|^2}{2\sigma_X^2}\right)},
\]

and

\[
A^\dagger z = A^\dagger z_B : \frac{1}{(\pi\sigma_X^2)^{d/2}} e^{\left(-\frac{\left| z'^T - A^\dagger z_B \right|^2}{2\sigma_X^2}\right)} \geq \frac{1}{(\pi\sigma_X^2)^{d/2}} e^{\left(-\frac{\left| z'^T - A^\dagger z_B \right|^2}{2\sigma_X^2}\right)},
\]

which conditions can be rewritten as

\[
A^\dagger z = A^\dagger z_A : \left| z'^T - A^\dagger z_A \right| < \left| z'^T - A^\dagger z_B \right|,
\]

and

\[
A^\dagger z = A^\dagger z_B : \left| z'^T - A^\dagger z_B \right| < \left| z'^T - A^\dagger z_A \right|.
\]

Precisely, using (114), the results of (117)–(118) with \( \chi(F(\Delta)) \in \mathbb{N}\left(0, \sigma_X^2\right) \) can be rewritten with respect to the subspace \( \mathbb{R} \) of \( \mathcal{C} \) as

\[
Az = A z_A : \frac{1}{\sqrt{\pi\sigma_X^2}} e^{\left(-\frac{\left( z' - \mu_{A_A} \right)^2}{2\sigma_X^2}\right)} \geq \frac{1}{\sqrt{\pi\sigma_X^2}} e^{\left(-\frac{\left( z' - \mu_{A_B} \right)^2}{2\sigma_X^2}\right)},
\]

and
whereas (119)–(120) are reevaluated as

\[ Az = A_{z_A} : |z' - \mu_{A_{z_A}}| < |z' - \mu_{A_{z_B}}| , \]  

(123)

and

\[ Az = A_{z_B} : |z' - \mu_{A_{z_B}}| < |z' - \mu_{A_{z_A}}| . \]  

(124)

The decision region is decomposed into hyperplanes \( H_{A_{z_A}} \) and \( H_{A_{z_B}} \) along \( \nu^d \) via the decision rule

\[ \frac{|A_{z_A}^\dagger z_A - A_{z_B}^\dagger z_B|}{2} = \frac{\mu_{A_{z_A}} + \mu_{A_{z_B}}}{2}, \]

where \( \mu_{A_{z_A}}, \mu_{A_{z_B}} \in \mathbb{C} \) are the expected means of \( \Gamma \), whereas \( A_{z_A}, A_{z_B} \in \mathbb{C} \) and \( z'_A, z'_B \in \mathbb{C} \) are complex scalar quantities.

The decision region is decomposed into hyperplanes \( H_{A_{z_A}} \) and \( H_{A_{z_B}} \) along \( \nu^d \) via the decision rule

\[ \frac{|A_{z_A}^\dagger z_A - A_{z_B}^\dagger z_B|}{2} = \frac{\mu_{A_{z_A}} + \mu_{A_{z_B}}}{2}, \]

where \( \mu_{A_{z_A}}, \mu_{A_{z_B}} \in \mathbb{C} \) are the expected means of \( \Gamma \), whereas \( A_{z_A}, A_{z_B} \in \mathbb{C} \) and \( z'_A, z'_B \in \mathbb{C} \) are complex scalar quantities.

The decision region is decomposed into hyperplanes \( H_{A_{z_A}} \) and \( H_{A_{z_B}} \) along \( \nu^d \) via the decision rule

\[ \frac{|A_{z_A}^\dagger z_A - A_{z_B}^\dagger z_B|}{2} = \frac{\mu_{A_{z_A}} + \mu_{A_{z_B}}}{2}, \]

where \( \mu_{A_{z_A}}, \mu_{A_{z_B}} \in \mathbb{C} \) are the expected means of \( \Gamma \), whereas \( A_{z_A}, A_{z_B} \in \mathbb{C} \) and \( z'_A, z'_B \in \mathbb{C} \) are complex scalar quantities.

The decision region is decomposed into hyperplanes \( H_{A_{z_A}} \) and \( H_{A_{z_B}} \) along \( \nu^d \) via the decision rule

\[ \frac{|A_{z_A}^\dagger z_A - A_{z_B}^\dagger z_B|}{2} = \frac{\mu_{A_{z_A}} + \mu_{A_{z_B}}}{2}, \]

where \( \mu_{A_{z_A}}, \mu_{A_{z_B}} \in \mathbb{C} \) are the expected means of \( \Gamma \), whereas \( A_{z_A}, A_{z_B} \in \mathbb{C} \) and \( z'_A, z'_B \in \mathbb{C} \) are complex scalar quantities.

The decision region is decomposed into hyperplanes \( H_{A_{z_A}} \) and \( H_{A_{z_B}} \) along \( \nu^d \) via the decision rule

\[ \frac{|A_{z_A}^\dagger z_A - A_{z_B}^\dagger z_B|}{2} = \frac{\mu_{A_{z_A}} + \mu_{A_{z_B}}}{2}, \]

where \( \mu_{A_{z_A}}, \mu_{A_{z_B}} \in \mathbb{C} \) are the expected means of \( \Gamma \), whereas \( A_{z_A}, A_{z_B} \in \mathbb{C} \) and \( z'_A, z'_B \in \mathbb{C} \) are complex scalar quantities.

The decision region is decomposed into hyperplanes \( H_{A_{z_A}} \) and \( H_{A_{z_B}} \) along \( \nu^d \) via the decision rule

\[ \frac{|A_{z_A}^\dagger z_A - A_{z_B}^\dagger z_B|}{2} = \frac{\mu_{A_{z_A}} + \mu_{A_{z_B}}}{2}, \]

where \( \mu_{A_{z_A}}, \mu_{A_{z_B}} \in \mathbb{C} \) are the expected means of \( \Gamma \), whereas \( A_{z_A}, A_{z_B} \in \mathbb{C} \) and \( z'_A, z'_B \in \mathbb{C} \) are complex scalar quantities.

The decision region is decomposed into hyperplanes \( H_{A_{z_A}} \) and \( H_{A_{z_B}} \) along \( \nu^d \) via the decision rule

\[ \frac{|A_{z_A}^\dagger z_A - A_{z_B}^\dagger z_B|}{2} = \frac{\mu_{A_{z_A}} + \mu_{A_{z_B}}}{2}, \]

where \( \mu_{A_{z_A}}, \mu_{A_{z_B}} \in \mathbb{C} \) are the expected means of \( \Gamma \), whereas \( A_{z_A}, A_{z_B} \in \mathbb{C} \) and \( z'_A, z'_B \in \mathbb{C} \) are complex scalar quantities.
where
\[
\left( A^\dagger z_A - A^\dagger z_B \right) F^d (\Delta) \in CN \left( 0, \left[ \left( A^\dagger z_A - A^\dagger z_B \right) \right]^2 2\sigma_N^2 \right).
\] (126)

In the \( \mathbb{R}^d \) \( d \)-dimensional subspace of \( C^d \), it is evaluated with \( \chi (F^d (\Delta)) \in \mathbb{N} (0, \sigma_N^2 I) \) as
\[
p_{err} = \Pr \left( \left| \chi (F^d (\Delta)) \right|^2 > \left| \chi (F^d (\Delta))^T + \chi (A^\dagger z_A - A^\dagger z_B) \right|^2 \right)
\[
= \Pr \left( \chi (A^\dagger z_A - A^\dagger z_B) \chi (F^d (\Delta)) < \frac{\left| \chi (A^\dagger z_A - A^\dagger z_B) \right|^2}{2} \right)
\] (127)
\[
= Q \left( \frac{\left| A^\dagger z_A - A^\dagger z_B \right|}{2\sigma_N} \right),
\]
where
\[
\chi (A^\dagger z_A - A^\dagger z_B) \chi (F^d (\Delta)) \in \mathbb{N} \left( 0, \left| \chi (A^\dagger z_A - A^\dagger z_B) \right|^2 \sigma_N^2 \right).
\] (128)

Exploiting \( \Gamma \), the \( p_{err} \) decoding error probability in \( C \) is
\[
p_{err} = \Pr \left( z' < \frac{1}{2} \left( \mu_{A z_A} + \mu_{A z_B} \right) \right) \ | \ A z_A \right)
\[
= \Pr \left( F(\Delta) > \frac{1}{2} \left( \left| \mu_{A z_A} - \mu_{A z_B} \right| \right) \right)
\] (129)
\[
= Q \left( \frac{\left| \mu_{A z_A} - \mu_{A z_B} \right|}{2\sigma_N} \right),
\]
and in the subspace of \( \mathbb{R} \), it can be evaluated precisely as
\[
p_{err} = \Pr \left( \chi (z') < \frac{1}{2} \chi (\mu_{A z_A} + \mu_{A z_B}) \ | \ \chi (z) = \chi (A z_A) \right)
\[
= \Pr \left( \chi (F(\Delta)) > \frac{1}{2} \left| \chi (\mu_{A z_A} - \mu_{A z_B}) \right| \right)
\] (130)
\[
= Q \left( \frac{\left| \mu_{A z_A} - \mu_{A z_B} \right|}{2\sigma_N} \right).
\]

Focusing on subspace \( \mathbb{R}^d \) with \( N \) codewords, at a given \( A \), let \( E \) be an error event. Then the conditional error probability is
\[
\Pr (E|A) = Q \left( \frac{|A^\dagger M^N|}{2\sigma_N} \right).
\] (131)

After some calculations, the corresponding error probability is yielded as
\[
\Pr (E) = \mathbb{E} \left[ Q \left( \sqrt{\frac{SNR A^\dagger M^N (M^N)^\dagger A}{2}} \right) \right].
\] (132)

The matrix \( M^N \) is Hermitian, that is, \( (M^N)^\dagger = M^N \), which can be diagonalized by a \( U \) unitary operation, such that \( M^N (M^N)^\dagger = U \tau U^\dagger \), where
\[
\tau = \text{diag} \left( \lambda_1^2, \ldots, \lambda_{d-1}^2 \right),
\] (133)
where \( \lambda_i^2 \) are the singular values of \( M^N \) [23-25].

In particular, the result in (133) can be further exploited to derive \( \Pr (E) \) as
\[ \Pr(E) = \mathbb{E}\left[ Q\left( \sqrt{\frac{\text{SNR} U_j^H A_j}{2}} \right) \right] \]
\[ = \mathbb{E}\left[ Q\left( \sqrt{\frac{\text{SNR} \sum_{j=0}^{d-1} U_j^H A_j \lambda_j^2}{2}} \right) \right], \quad (134) \]

where an averaging over a \( U_j^H A_j \in \mathbb{C}N\left( 0, \sigma^2 A_j \right) \) distribution leads to an upper bound on \( \Pr(E) \) as
\[ \Pr(E) \leq \mathbb{E}\left[ \prod_{j=0}^{d-1} \frac{1}{1 + \text{SNR} \lambda_j^2} \right]. \quad (135) \]

Specifically, assuming the case of \( N \geq d \), and \( \forall \lambda_j^2 > 0 \), after some calculations the success probability is yielded as precisely
\[ \Pr \geq 1 - \mathbb{E}\left[ \frac{d^d}{\text{SNR}^d \prod_{j=0}^{d-1} \lambda_j^2} \right] \]
\[ = 1 - \mathbb{E}\left[ \frac{d^d}{\text{SNR}^d \det(M_N^N)} \right], \quad (136) \]

Putting the pieces together, the \( S^d \) sufficient statistics for the decoding of \( d \)-dimensional outputs in a multicarrier CVQKD scenario at \( N = 2 \) is
\[ S^d = \left( \nu^d \right)^\dagger z' \]
\[ = s \left| A^H M^2 \right| + F(\Delta), \quad (137) \]

which result can be extended for arbitrary \( N \) as
\[ S^d = \left( \nu^d \right)^\dagger z' \]
\[ = \left( \frac{A^H M^2}{A^H A^H} \right)^\dagger z', \quad (138) \]

where \( M_N \) is the codeword difference matrix of the \( N \) codewords \( z \in \{ z_0, \ldots, z_{N-1} \} \).

5 Multiuser Adaptive Quadrature Detection

**Theorem 3** (Adaptive quadrature detection for multiuser multicarrier CVQKD). Assuming a \( (K_{in}, K_{out}) \) multiuser multicarrier CVQKD setting, the \( p_{err} \) error probability of the adaptive detection of user \( U_k \) is \( p_{err} \leq \mathbb{E}\left[ \frac{1}{\prod_{j=0}^{r_k-1} \frac{1}{1 + \text{SNR}_{U_k} \lambda_j^2}} \right] \), where \( \lambda_j^2 \) is the \( j \)-th singular value of the \( M_{U_k}^N \) codeword difference matrix of the \( N \), \( r_k \)-dimensional \( \tilde{z}_k \in \mathbb{C}N\left( 0, K_k \right) \) codewords of \( U_k \), \( r_k \leq d \), \( \sum_{K_{out}} r_k = d \), and \( \text{SNR}_{U_k} \) is the SNR of \( U_k \).
Proof.
Let the $d$-dimensional output $\mathbf{z}'$ be given as
\[
\mathbf{z}'^T = \left( \mathbf{z}'_{U_0} \right)^T + \ldots + \left( \mathbf{z}'_{U_{K_{out}}} \right)^T
\]
\[
= A_{U_0}^\dagger \mathbf{z}_0 + \left( F_{U_0}^r (\Delta) \right)^T + \ldots + A_{U_{K_{out}-1}}^\dagger \mathbf{z}_{K_{out}-1} + \left( F_{U_{K_{out}-1}}^r (\Delta) \right)^T,
\]
where $U_k$ is the $k$-th user, $k = 0, \ldots, K_{out} - 1$,
\[
\mathbf{z}_k = \text{diag} \left( \mathbf{z}_{U_k,0}, \ldots, \mathbf{z}_{U_k,r_k-1} \right) \in \mathbb{C}^N \left( 0, \mathbf{K}_{z_k} \right)
\]
is the $r_k$-dimensional input of $U_k$ (referred to as codeword $\mathbf{z}_k$ of $U_k$), $r_k \leq d$, $\sum_{K_{out}} r_k = d$,
and $\mathbf{z}_{U_k,j} \in \mathbb{C}^N \left( 0, 2\sigma^2_{w_0} \right)$, and $A_{U_k}$ is an $r_k$-dimensional vector with a $j$-th entry of $A_{U_k,j} = \frac{1}{l} \sum_{i=0}^{l-1} F_{U_k} \left( T_{j,i} (\mathcal{N}_{j,i}) \right)$, that is, the averaged Fourier-transformed sub-channel coefficients of $U_k$, $j = 0, \ldots, r_k - 1$,
\[
A_{U_k} = \left( A_{U_k,0}^\dagger, \ldots, A_{U_k,r_k-1}^\dagger \right)^T
\]
\[
= \left( \frac{1}{l} \sum_{i=0}^{l-1} F_{U_k} \left( T_{0,i} (\mathcal{N}_{0,i}) \right), \ldots, \frac{1}{l} \sum_{i=0}^{l-1} F_{U_k} \left( T_{r_k-1,i} (\mathcal{N}_{r_k-1,i}) \right) \right)^T,
\]
and
\[
F_{U_k}^r (\Delta) = \left( F (\Delta_{U_k,0}), \ldots, F (\Delta_{U_k,r_k-1}) \right)^T \in \mathbb{C}^N \left( 0, \mathbf{K}_{F_{U_k}^r (\Delta)} \right).
\]
From $A_{U_k}$, $\left| A_{U_k} \right|$ is expressed as
\[
\left| A_{U_k} \right| = \sum_{w=0}^{r_k-1} A_{U_k,w} = \sum_{w=0}^{r_k-1} \left| \frac{1}{l} \sum_{i=0}^{l-1} F_{U_k} \left( T_{w,i} (\mathcal{N}_{w,i}) \right) \right|,
\]
where
\[
\left| A_{U_k} \right| \mathbf{z}_k = \sum_{j=0}^{r_k-1} \frac{1}{l} \sum_{i=0}^{l-1} F (T_{j,i} (\mathcal{N}_{j,i})) \mathbf{z}_k.
\]
In the further parts of the proof, without loss of generality, we assume collective measurement for each $U_k$, and let the number input codewords be selected to $N = 2$, thus $\mathbf{z}_k \in \{ \mathbf{z}_{A,k}, \mathbf{z}_{B,k} \}$.

Then for any $U_k$, applying the results of Theorem 2 leads to
\[
U_{U_k}^r = \begin{bmatrix}
A_{U_k}^\dagger \mathbf{z}_{A,k} - A_{U_k}^\dagger \mathbf{z}_{B,k} \\
\left| A_{U_k} \right| \mathbf{z}_k
\end{bmatrix}
\]
\[
= \begin{bmatrix}
A_{U_k}^\dagger \left( \mathbf{z}_{A,k} - \mathbf{z}_{B,k} \right) \\
\left| A_{U_k} \right| \mathbf{z}_k
\end{bmatrix}
\]
\[
= \begin{bmatrix}
\left| A_{U_k} \right| \mathbf{M}_{U_k}^2 \\
\left| A_{U_k} \right| \mathbf{M}_{U_k}^2
\end{bmatrix},
\]
where $\mathbf{M}_{U_k}^2$ is the codeword difference matrix of $U_k$ at $N = 2$. 
\[ M^2_{U_k} = \tilde{z}_{A,k} - \tilde{z}_{B,k}. \]  

In particular, projecting \( z'_{U_k} \) along \( \nu^\dagger_{U_k} \) via \( \mathcal{P}(z'_{U_k}) \) yields a complex scalar \( \Gamma_{U_k} \in \mathbb{C} \) as follows:

\[ \mathcal{P}(z'_{U_k}) = \left( \nu^\dagger_{U_k} \right)^\dagger \left( z_{U_k} - \frac{1}{2} \left( \mathbf{A}^\dagger_{U_k} (\tilde{z}_{A,k} + \tilde{z}_{B,k}) \right) \right) = s_{U_k} \left| \mathbf{A}^\dagger_{U_k} \tilde{z}_{A,k} - \mathbf{A}^\dagger_{U_k} \tilde{z}_{B,k} \right| + F_{U_k} (\Delta) = s_{U_k} \left| \mathbf{A}^\dagger_{U_k} \mathbf{M}^2_{U_k} \right| + F_{U_k} (\Delta) = \Gamma_{U_k}, \]

where \( s_{U_k} \in \{-0.5, 0.5\} \in \mathbb{R} \) and \( F_{U_k} (\Delta) \in \mathbb{C}N \left(0, 2\sigma_N^2\right) \) are scalars, which yields the \( S_{U_k}^\dagger \) sufficient statistic of \( U_k \) as

\[ S_{U_k}^\dagger = \left( \nu^\dagger_{U_k} \right)^\dagger z'_{U_k} = s_{U_k} \left| \mathbf{A}^\dagger_{U_k} \mathbf{M}^2_{U_k} \right| + F_{U_k} (\Delta). \]

Note that a strictly suboptimal \( \kappa(z') \) decoding operation can also be defined by applying \( \kappa \) on the \( d \)-dimensional \( z' \) in the phase space, such that

\[ \kappa(z') = \mathbf{A}^{-1}z' = \mathbf{A}^{-1} (\mathbf{A}z + F^d (\Delta)) = z + \mathbf{A}^{-1}F^d (\Delta), \]

where \( \mathbf{A}^{-1} \) is the inverse of \( \mathbf{A} \),

\[ \mathbf{A} = \left( \frac{1}{7} \sum_{i=0}^{l-1} F \left( T_{0,i} (\mathcal{N}_0) \right)^\dagger, \ldots, \frac{1}{7} \sum_{i=0}^{l-1} F \left( T_{d-1,i} (\mathcal{N}_{d-1}) \right)^\dagger \right)^T. \]

Precisely, in this case, the resulting \( r_k \)-dimensional scaled noise \( \eta_{U_k}^\dagger \),

\[ \eta_{U_k}^\dagger = \mathbf{A}^{-1}F^d (\Delta) \in \mathbb{C}N \left(0, \mathbf{K}_{r_k} \right), \]

of each \( U_k \) user’s is correlated; thus, (139) can be rewritten as

\[ z^T = \left( z'_{U_0} \right)^T + \ldots + \left( z'_{U_{K_{out}}} \right)^T = \mathbf{A}^\dagger_{U_0} \tilde{z}_0 + \left( \eta_{U_0}^\dagger \right)^T + \ldots + \mathbf{A}^\dagger_{U_{K_{out}}} \tilde{z}_{K_{out}-1} + \left( \eta_{U_{K_{out}-1}}^\dagger \right)^T, \]

where \( \eta_{U_k} \) is a \( \mathbb{C}N \left(0, \sigma^2_{\eta_{U_k}}\right) \) distributed independent random variable.

In particular, applying a projection \( \mathcal{P}(\kappa(z'_{U_k})) \) on \( \kappa(z'_{U_k}) \) leads to

\[ \mathcal{P}(\kappa(z'_{U_k})) = z'_{U_k} = (\mathbf{A}^\dagger_{U_k}) \tilde{z}_{U_k} + \Omega (\Delta), \]
where \( \Omega(\Delta) \in \mathcal{CN}(0, \sigma_N^2) \) is a random variable (scaled noise), which is completely independent from the noise \( F_{U_k}(\Delta) \) of \( U_k \), and \( \partial_{U_k} \) is a \( r_k \)-dimensional vector expressed precisely as

\[
\partial_{U_k} = \frac{1}{A_k} - \left( A_k^{*} \right),
\]

(154)

where operator \(-\) inverts the sign of some corresponding terms of \( A_k^{*} \) (* is the complex conjugate). Specifically, because the resulting \( \Omega(\Delta) \) noise of each \( U_k \) is independent from the noise obtained by \( U_k \), the application of a \( \kappa(z_{U_k}') \) operation on \( z_{U_k}' \) is strictly suboptimal, and

\[
\mathcal{P}\left( \kappa(z_{U_k}') \right)
\]

results in a scaled scalar output \( z_{U_k}' \).

The \( (K_m, K_{out}) \) multiuser setting defines a \( K_{out} \)-dimensional space, which is depicted in Fig. 5. Each user \( U_k \) identifies a vector \( A_{U_k} \) and a sufficient statistics \( S_{U_k}^{r_k} \). The decoding of \( z_{U_k}' \) of \( U_k \) is achieved via operation \( \mathcal{P}(z_{U_k}') \).

![Figure 5. The \( S_{U_k}^{r_k} \) sufficient statics in the \( K_{out} \)-dimensional space for a multiuser multicarrier CVKQD decoding, for \( K_{out} = 3 \).](image)

To derive the error probability, we can directly apply the results of Theorem 2. Let \( N = 2 \); thus, in a \( (K_m, K_{out}) \) multiuser setting, for a particular user \( U_k \), (135) leads to an error probability precisely,

\[
\Pr(\tilde{z}_{A,k} \rightarrow \tilde{z}_{B,k}) \leq \mathbb{E} \left[ \prod_{j=0}^{n-1} \frac{1}{1 + \text{SNR}_{U_k} \lambda_j^2} \right],
\]

(155)

where \( \lambda_j^2 \) is the \( j \)-th singular value of \( M_{U_k}^2 = \tilde{z}_{A,k} - \tilde{z}_{B,k} \), and \( \text{SNR}_{U_k} \) is the SNR of \( U_k \). The results can be extended for arbitrary \( N \) and combination of \( (K_m, K_{out}) \).
6 Conclusions

The multicarrier CVQKD transmission utilizes subcarrier CVs for information transmission. We introduced the adaptive quadrature detection for multicarrier CVQKD. The proposed decoding scheme exploits the statistics of the sub-channels, which are provided by our sub-channel estimation phase. The sub-channel estimation procedure scans through the conditions of the sub-channels via pilot-subcarrier CVs. The error probability of the sub-channel estimation reaches the theoretical minimum via our subcarrier spreading technique. Adaptive quadrature decoding can be performed with homodyne or heterodyne measurement, single or collective measurement setting. We also extended the adaptive quadrature detection for a multiuser multicarrier CVQKD setting. The adaptive quadrature detection scheme provides a flexible framework to extract the potential of multicarrier CVQKD, specifically functional and convenient for experimental scenarios.

Acknowledgements

The author would like to thank Professor Sandor Imre for useful discussions. This work was partially supported by the GOP-1.1.1-11-2012-0092 (Secure quantum key distribution between two units on optical fiber network) project sponsored by the EU and European Structural Fund, and by the COST Action MP1006.

References

[1] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Continuous-variable Quantum Cryptography using Two-Way Quantum Communication, arXiv:quant-ph/0611167v3 (2008).
[2] L. Gyongyosi, Adaptive Multicarrier Quadrature Division Modulation for Continuous-variable Quantum Key Distribution, arXiv:1310.1608 (2013).
[3] L. Gyongyosi, Multiuser Quadrature Allocation for Continuous-Variable Quantum Key Distribution, arXiv:1312.3614 (2013).
[4] L. Gyongyosi, Singular Layer Transmission for Continuous-Variable Quantum Key Distribution, arXiv:1402.5110 (2014).
[5] L. Gyongyosi, Security Thresholds of Multicarrier Continuous-Variable Quantum Key Distribution, arXiv:1404.7109 (2014).
[6] L. Gyongyosi, Multidimensional Manifold Extraction for Multicarrier Continuous-Variable Quantum Key Distribution, arXiv:1405.6948 (2014).
[7] L. Gyongyosi, Subcarrier Domain of Multicarrier Continuous-Variable Quantum Key Distribution, arXiv:1406.6949 (2014).
[8] L. Gyongyosi, S. Imre, Geometrical Analysis of Physically Allowed Quantum Cloning Transformations for Quantum Cryptography, Information Sciences, Elsevier, pp. 1-23, DOI: 10.1016/j.ins.2014.07.010 (2014).
[9] S. Pirandola, R. Garcia-Patron, S. L. Braunstein and S. Lloyd. *Phys. Rev. Lett.* 102 050503. (2009).
[10] S. Pirandola, A. Serafini and S. Lloyd. *Phys. Rev. A* 79 052327. (2009).
[11] S. Pirandola, S. L. Braunstein and S. Lloyd. *Phys. Rev. Lett.* 101 200504 (2008).
[12] C. Weedbrook, S. Pirandola, S. Lloyd and T. Ralph. *Phys. Rev. Lett.* 105 110501 (2010).
[13] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. Ralph, J. Shapiro, and S. Lloyd. *Rev. Mod. Phys.* 84, 621 (2012).
[14] Wi. Shieh and I. Djordjevic. *OFDM for Optical Communications.* Elsevier (2010).
[15] L. Gyongyosi, Scalar Reconciliation for Gaussian Modulation of Two-Way Continuous-variable Quantum Key Distribution, *arXiv:1308.1391* (2013).
[16] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, *arXiv:1210.6216v1* (2012).
[17] M. Navascues, F. Grosshans, and A. Acín. Optimality of Gaussian Attacks in Continuous-variable Quantum Cryptography, *Phys. Rev. Lett.* 97, 190502 (2006).
[18] R. García-Patron and N. J. Cerf. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Phys. Rev. Lett.* 97, 190503 (2006).
[19] F. Grosshans, Collective attacks and unconditional security in continuous variable quantum key distribution. *Phys. Rev. Lett.* 94, 020504 (2005).
[20] M R A Adcock, P Høyer, and B C Sanders, Limitations on continuous-variable quantum algorithms with Fourier transforms, *New Journal of Physics* 11 103035 (2009)
[21] L. Hanzo, H. Haas, S. Imre, D. O’Brien, M. Rupp, L. Gyongyosi. Wireless Myths, Realities, and Futures: From 3G/4G to Optical and Quantum Wireless, *Proceedings of the IEEE*, Volume: 100, Issue: Special Centennial Issue, pp. 1853-1888. (2012).
[22] S. Imre and L. Gyongyosi. *Advanced Quantum Communications - An Engineering Approach*. Wiley-IEEE Press (New Jersey, USA), (2012).
[23] D. Tse and P. Viswanath. *Fundamentals of Wireless Communication*, Cambridge University Press, (2005).
[24] D. Middlet, *An Introduction to Statistical Communication Theory: An IEEE Press Classic Reissue*, Hardcover, IEEE, ISBN-10: 0780311787, ISBN-13: 978-0780311787 (1960)
[25] S. Kay, *Fundamentals of Statistical Signal Processing, Volumes I-III*, Prentice Hall, (2013)
[26] S. Imre, F. Balazs: *Quantum Computing and Communications – An Engineering Approach*, John Wiley and Sons Ltd, ISBN 0-470-86902-X, 283 pages (2005).
[27] D. Petz, *Quantum Information Theory and Quantum Statistics*, Springer-Verlag, Heidelberg, Hiv: 6. (2008).
[28] R. V. Meter, *Quantum Networking*, John Wiley and Sons Ltd, ISBN 1118648927, 9781118648926 (2014).
[29] L. Gyongyosi, S. Imre: Properties of the Quantum Channel, *arXiv:1208.1270* (2012).

[30] K Wang, XT Yu, SL Lu, YX Gong, Quantum wireless multihop communication based on arbitrary Bell pairs and teleportation, *Phys. Rev A*, (2014).

[31] Babar, Zunaira, Ng, Soon Xin and Hanzo, Lajos, EXIT-Chart Aided Near-Capacity Quantum Turbo Code Design. *IEEE Transactions on Vehicular Technology* (submitted) (2014).

[32] Botsinis, Panagiotis, Alanis, Dimitrios, Ng, Soon Xin and Hanzo, Lajos Low-Complexity Soft-Output Quantum-Assisted Multi-User Detection for Direct-Sequence Spreading and Slow Subcarrier-Hopping Aided SDMA-OFDM Systems. *IEEE Access*, PP, (99), doi:10.1109/ACCESS.2014.2322013 (2014).

[33] Botsinis, Panagiotis, Ng, Soon Xin and Hanzo, Lajos Fixed-complexity quantum-assisted multi-user detection for CDMA and SDMA. *IEEE Transactions on Communications*, vol. 62, (no. 3), pp. 990-1000, doi:10.1109/TCOMM.2014.012514.130615 (2014).
Supplemental Information

S.1 Notations

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

Table S.1. Summary of notations.

| Notation | Description |
|----------|-------------|
| $i$ | Index for the $i$-th subcarrier Gaussian CV, $|\phi_i\rangle = x_i + ip_i$. |
| $j$ | Index for the $j$-th Gaussian single-carrier CV, $|\varphi_j\rangle = x_j + ip_j$. |
| $l$ | Number of Gaussian sub-channels $N_i$ for the transmission of the Gaussian subcarriers. The overall number of the sub-channels is $n$. The remaining $n-l$ sub-channels do not transmit valuable information. |
| $x_i, p_i$ | Position and momentum quadratures of the $i$-th Gaussian subcarrier, $|\phi_i\rangle = x_i + ip_i$. |
| $x_i', p_i'$ | Noisy position and momentum quadratures of Bob’s $i$-th noisy subcarrier Gaussian CV, $|\phi_i'\rangle = x_i' + ip_i'$. |
| $x_j, p_j$ | Position and momentum quadratures of the $j$-th Gaussian single-carrier $|\varphi_j\rangle = x_j + ip_j$. |
| $x_j', p_j'$ | Noisy position and momentum quadratures of Bob’s $j$-th recovered single-carrier Gaussian CV $|\varphi_j'\rangle = x_j' + ip_j'$. |
| $x_{A,i}, p_{A,i}$ | Alice’s quadratures in the transmission of the $i$-th subcarrier. |
| $|\phi_i\rangle, |\phi_i'\rangle$ | Transmitted and received Gaussian subcarriers. The subcarriers have angles $\theta_i^* \in [0, 2\pi]$, $\theta_i \in [0, 2\pi]$ CVs in the phase space $S$. |
| $Q(\cdot)$ | Gaussian tail function. |
| $p_i$ | Pilot-subcarrier CV for the $S_i(N_i) \in C$ channel statistics. |
of sub-channel $\mathcal{N}_i$. Complex variable, $p_i = \text{Re}(p_i) + \text{Im}(p_i) = x_{p_i} + ip_{p_i} \in \mathcal{C}$, where $x_{p_i}, p_{p_i}$ identify the position and momentum quadratures. Used for the estimation of $F(T_i(\mathcal{N}_i))$ of $\mathcal{N}_i$. Also expressed as $p_i = F^{-1}(p_j)$, where $F^{-1}$ is the inverse Fourier operation.

| $p_j$ | Pilot single-carrier CV for the $\mathcal{N}_j$ single-carrier channel estimation. Complex variable, $p_j = F(p_i) = x_{p_j} + ip_{p_j}$, where $x_{p_j}, p_{p_j}$ identify the position and momentum quadratures. |
|---|---|
| $\mathcal{S}_i(\mathcal{N}_i)$ | Sufficient statistic for the estimation of $F(T_i(\mathcal{N}_i))$ of sub-channel $\mathcal{N}_i$, complex variable. Evaluated as $\mathcal{S}_i(\mathcal{N}_i) = \varsigma_i p_i' = \left(\frac{p_i}{|p_i|^2}\right) p_i' = F(T_i(\mathcal{N}_i)) + F'(\Delta)$, |
| $\mathcal{S}(\mathcal{N}_j)$ | Sufficient statistic for the estimation of $\frac{1}{i} \sum_i F(T_i(\mathcal{N}_i))$ of the single-carrier channel $\mathcal{N}_j$, expressed as $\mathcal{S}(\mathcal{N}_j) = \varsigma_j q_j' = A_j + F'(\Delta)$, where $\varsigma_j = q_j / |q_j|^2$, $q_j = (p_0, \ldots, p_{l-1})^T \in \mathcal{C}^i$, $q_j' = (p_0', \ldots, p_{l-1}')^T \in \mathcal{C}^i$, $A_j = \frac{1}{i} \left(\sum_{i=0}^{l-1} F(T_{j,i}(\mathcal{N}_{j,i}))\right) \in \mathcal{C}$, $F'(\Delta) \in \mathcal{CN}(0, 2\sigma_N^2 / |q_j|^2)$, |
| $\mathcal{P}(\cdot)$ | Projector. |
| $\Gamma$ | The result of projection $\mathcal{P}(\cdot)$, identifies the $\mathcal{S}$ sufficient statistics in the $\mathcal{C}$ complex scalar space. |
| $p_i'$ | Noisy pilot-subcarrier CV, complex variable, $p_i' = F(T_i(\mathcal{N}_i)) p_i + F(\Delta)$. |
| $\varsigma_i$ | Complex variable, $\varsigma_i = p_i / |p_i|^2$ to derive the $\mathcal{S}(\mathcal{N}_i)$ sufficient sub-channel channel statics of $\mathcal{N}_i$. |
| $s$ | Scalar real variable, $s \in \{-0.5, 0.5\} \subseteq \mathbb{R}$. |
| --- | --- |
| $\gamma$ | Subspace of one $\mathbb{R}$ real dimension. |
| $\mathcal{E}$ | Mean square error. |
| $\zeta(\cdot)$ | Linear estimation operator. |
| $E$ | Minimum mean squared error. |
| $C \in \mathcal{C}$ | Constant complex variable to derive $\zeta(\cdot)$. |
| $\mathcal{C}^l$ | Constant complex vector in $\mathcal{C}^l$ to derive $\zeta(\cdot)$ of the single-carrier channel $\mathcal{N}_j$. |
| $q_j$ | An $l$-dimensional complex pilot-subcarrier CV vector, conveys the $l$ pilot subcarrier CVs, $q_j = \left(p_{j,0}, \ldots, p_{j,l-1}\right)^T \in \mathcal{C}^l$. The noisy vector is $q_j' = \left(p_{j,0}', \ldots, p_{j,l-1}'\right)^T \in \mathcal{C}^l$. |
| $q_x \in \mathcal{C}^g$ | A $g$-dimensional complex pilot-subcarrier CV vector $q_x = \left(p_{x,0}, \ldots, p_{x,g-1}\right)^T$, defined for the subcarrier spreading, $g + (l - 1) = n$, where $n$ is the overall number of the sub-channels, $l$ is the number of sub-channels that are utilized for transmission in the private transmission phase. |
| $p_x \in \mathcal{C}^l$ | An $l$-dimensional complex pilot-subcarrier CV vector, $p_x = \left(p_{x,0}, \ldots, p_{x,l-1}\right)^T$, where $p_{x,i}$ is the constant pilot-subcarrier CV of sub-channel $\mathcal{N}_i, i = 0, \ldots, l - 1$, such that, $p_{x,i} = p_x \in \mathcal{C}, i = 0, \ldots, l - 1$. |
| $p_x'$ | The noisy version of $p_x$, $p_x' = \left(p_{x,0}', \ldots, p_{x,l-1}'\right)^T$, $l$-dimensional constant complex pilot-subcarrier CV vector. |
| $p_s^i = (a_0, q_x, b_0)$ | An $n$-dimensional complex vector $p_s^i \in \mathcal{C}^n$, defined for the subcarrier spreading technique, $i = 0, \ldots, l - 1$, $q_x = \left(p_{x,0}, \ldots, p_{x,g-1}\right)^T$, $a_0$ is an $i$-dimensional vector, $a_0 = \left(\rho_0^0, \ldots, \rho_{i-1}^0\right)^T$, where $\rho_w^0 = |0\rangle\langle 0|, w = 0, \ldots, i - 1$, $b_0$ is an $u = (l - 1) - i$-dimensional vector, $b_0 = \left(\rho_0^u, \ldots, \rho_{u-1}^u\right)^T$, where $\rho_w^u = |0\rangle\langle 0|, w = 0, \ldots, u - 1$. |
| $V^i(\Delta)$ | An $n$-dimensional noise vector, defined for the subcarrier... |
spreading technique.

\[ s_x = \frac{p^*_x}{|p^*_x|} \]

Sufficient statistics for the estimation of sub-channel \( \mathcal{N}_i \) in subcarrier spreading. Complex vector, \( s_x = \frac{p^*_x}{|p^*_x|} \).

\[ \Upsilon \]

Real variable, \( \Upsilon = \frac{|p^*_x|}{g} = |p_x|^2 \), where \( p_x = (p_{x,0}, \ldots, p_{x,g-1})^T \).

\[ M^N \]

Codeword difference matrix of the \( N \) codewords \( \{z_0, \ldots, z_{N-1}\} \). Hermitian matrix, \( (M^N)^\dagger = M^N \).

\[ \lambda^2 \]

The \( i \)-th singular value of \( M^N \), \( \tau = \text{diag} (\lambda^2_0, \ldots, \lambda^2_{d-1}) \).

\[ A \]

A \( d \)-dimensional vector of the averaged transmittance coefficients, evaluated as

\[
A = \left( \frac{1}{T} \sum_{i=0}^{t-1} F(T_{0,i}(\mathcal{N}_{0,i})) \right)^\dagger, \ldots, \frac{1}{T} \sum_{i=0}^{t-1} F(T_{d-1,i}(\mathcal{N}_{d-1,i})) \right)^\dagger \right)^T.
\]

\[ z \in \mathbb{C}N(0,K_z) \]

A \( d \)-dimensional input CV vector to transmit valuable information.

\[ z'^T \]

A \( d \)-dimensional noisy output vector,

\[
z'^T = A^\dagger z + \left( F^d(\Delta) \right)^T = (z'_0, \ldots, z'_{d-1}), \quad \text{where}
\]

\[
z'_j = \left( \frac{1}{t} \sum_{i=0}^{t-1} F(T_{j,i}(\mathcal{N}_{j,i})) \right) z_j + F(\Delta) \in \mathbb{C}N\left(0,2\left(\sigma^2_{\omega_0} + \sigma^2_N\right)\right).
\]

\[ G_{uv} \]

An orthogonal matrix, \( uv \) indexes the row and column.

\[ \mathcal{H}_{Az_A}, \mathcal{H}_{Az_B} \]

Hyperplanes of the decision region, while \( Az_A, Az_B \in \mathcal{C} \) and \( z'_A, z'_B \in \mathcal{C} \) are complex scalar quantities.

\[ \mu_{Az_A}, \mu_{Az_B} \in \mathcal{C} \]

Expected means of \( \Gamma \), complex variables.

\[ U_k \]

Identifies user \( U_k \) in a multiuser scenario.

\[ (K_{in}, K_{out}) \]

Multiuser setting, number of transmitter and receiver users.

\[ z'^T \]

A \( d \)-dimensional output in a multiuser setting, evaluated as

\[
(z'_{U_0})^T + \ldots + (z'_{U_{K_{out}}})^T
\]

\[
= A^\dagger_{U_0} z_0 + \left( F^0_{U_0}(\Delta) \right)^T + \ldots + A^\dagger_{U_{K_{out}-1}} z_{K_{out}-1} + \left( F^0_{U_{K_{out}-1}}(\Delta) \right)^T.
\]

\[ \tilde{z}_k \]

The \( r_k \)-dimensional codeword of user \( U_k \), diagonal matrix, \( r_k \leq d \), \( \sum_{k=1}^{K_{out}} r_k = d \).
\[
\tilde{z}_k = \text{diag}(\hat{z}_{U_k,0}, \ldots, \hat{z}_{U_k,r_k-1}) \in \mathcal{CN}\left(0, K_{z_{U_k}}\right),
\]
where \(\hat{z}_{U_k,j} \in \mathcal{CN}\left(0, 2\sigma^2_{c_{U_k}}\right)\).

| \(A_{U_k}\) | An \(r_k\)-dimensional vector that contains the \(\frac{1}{l} \sum_{j=0}^{l-1} F_{U_{k}}\left(T_{j,i}\left(N_{j,i}\right)\right)\) averaged \(F_{U_{k}}\) Fourier transformed sub-channel coefficients of \(\hat{z}_j\) for \(U_k, j = 0, \ldots, r_k - 1\). |
|---|---|
| \(\kappa(\cdot)\) | A suboptimal operation for the pre-decoding \(d\)-dimensional \(z'\) in the phase space. |
| \(\eta_{U_k}^{r_k}\) | The resulting \(r_k\)-dimensional scaled noise vector \(\eta_{U_k}^{r_k}\), \(\eta_{U_k}^{r_k} = A^{-1} F^d (\Delta) \in \mathcal{CN}\left(0, K_{\eta_{U_k}}\right)\). The \(\eta_{U_k}\) projected noise is a \(\mathcal{CN}\left(0, \sigma^2_{U_k}\right)\) distributed independent random variable, evaluated as \(\kappa(z') = A^{-1} z' = A^{-1} (A z + F^d (\Delta)) = z + A^{-1} F^d (\Delta)\). |
| \(\partial_{U_k}\) | An \(r_k\)-dimensional vector of user \(U_k\), expressed \(\partial_{U_k} = \frac{1}{A_{U_k}} - (A^*_{U_k})\), where operator \(-\) inverts the sign of some corresponding terms of \(A^*_{U_k}\), where \(*\) is the complex conjugate. |
| \(\Omega(\Delta) \in \mathcal{CN}\left(0, \sigma^2_{\Delta}\right)\) | Random variable (scaled noise), independent from the noise \(F_{U_k}(\Delta)\) of \(z'_{U_k}\) of \(U_k\), derived as \(\mathcal{P}(\kappa(z'_{U_k})) = \tilde{z}_{U_k}^{'} = (\partial_{U_k} A_{U_k}) \tilde{z}_{U_k} + \Omega(\Delta)\). |
| \(\text{SNR}_{U_k}\) | The SNR quantity of \(U_k\). |
| \(p_{err}(p_x' | \tilde{z} (F(v(N))))\) | Conditional error probability of decoding pilot CV \(p_x'\) using the linear estimate \(\zeta(F(v(N)))\). |
| \(E\) | An error event, defined as \(E : |\zeta(F(v(N)))|^2 < \frac{1}{\text{SNR}}\). |
| Variable | Description |
|----------|-------------|
| $A_j$ | Complex variable, $A_j = \frac{1}{l} \left( \sum_{i=0}^{l-1} F \left( T_{j,i} \left( N_{j,i} \right) \right) \right) \in \mathcal{C}$, the averaged transmittance coefficient of the single-carrier channel $N_j$. |
| $\chi(\cdot)$ | Function that separately identifies the $x$ position or $p$ momentum quadrature components as $\text{Re}(\cdot)$ and $\text{Im}(\cdot)$, respectively. |
| $\vartheta$ | Variable to identify the noise of the estimation process on the $x$ position and $p$ momentum quadrature components, $\vartheta = \frac{\left| \chi(C)^T \chi(q_j) \right|^2 \mathbb{E} \left[ \chi(|A_j|^2) \right]}{|\chi(C)|^4 \sigma_{\chi}^2}$. |
| $\{C_{z_A}, C_{z_B}\}, \{C_{p_A}, C_{p_B}\}$ | Phase-space constellations of $z_A, z_B$, and private codewords $p_A, p_B$. |
| $U_{K_{\text{out}}}$ | The unitary CVQFT operation, $U_{k_{\text{out}}} = \frac{1}{\sqrt{K_{\text{out}}}} e^{i2\pi k} K_{\text{out}}^{-1}$, $i, k = 0, \ldots, K_{\text{out}} - 1$, $K_{\text{out}} \times K_{\text{out}}$ unitary matrix. |
| $U_{K_{\text{in}}}$ | The unitary inverse CVQFT operation, $U_{k_{\text{in}}} = \frac{1}{\sqrt{K_{\text{in}}}} e^{i2\pi k} K_{\text{in}}^{-1}$, $i, k = 0, \ldots, K_{\text{in}} - 1$, $K_{\text{in}} \times K_{\text{in}}$ unitary matrix. |
| $z \in \mathcal{CN} \left( 0, \sigma_z^2 \right)$ | The variable of a single-carrier Gaussian CV state, $|\varphi_z\rangle \in \mathcal{S}$. Zero-mean, circular symmetric complex Gaussian random variable, $\sigma_z^2 = \mathbb{E} \left[ |z|^2 \right] = 2\sigma_z^2$, with i.i.d. zero mean, Gaussian random quadrature components $x, p \in \mathcal{N} \left( 0, \sigma_{\chi}^2 \right)$, where $\sigma_{\chi}^2$ is the variance. |
| $\Delta \in \mathcal{CN} \left( 0, \sigma_\Delta^2 \right)$ | The noise variable of the Gaussian channel $\mathcal{N}$, with i.i.d. zero-mean, Gaussian random noise components on the position and momentum quadratures $\Delta_x, \Delta_p \in \mathcal{N} \left( 0, \sigma_\Delta^2 \right)$, $\sigma_\Delta^2 = \mathbb{E} \left[ |\Delta|^2 \right] = 2\sigma_\Delta^2$. |
| $d \in \mathcal{CN} \left( 0, \sigma_d^2 \right)$ | The variable of a Gaussian subcarrier CV state, $|\varphi_d\rangle \in \mathcal{S}$. Zero-mean, circular symmetric Gaussian random variable, $\sigma_d^2 = \mathbb{E} \left[ |d|^2 \right] = 2\sigma_d^2$, with i.i.d. zero mean, Gaussian ran- |
| Expression | Description |
|------------|-------------|
| $F^{-1}(\cdot) = \text{CVQFT}^\dagger(\cdot)$ | The inverse CVQFT transformation, applied by the encoder, continuous-variable unitary operation. |
| $F(\cdot) = \text{CVQFT}(\cdot)$ | The CVQFT transformation, applied by the decoder, continuous-variable unitary operation. |
| $F^{-1}(\cdot) = \text{IFFT}(\cdot)$ | Inverse FFT transform, applied by the encoder. |
| $\sigma^2_{w_i}$ | Single-carrier modulation variance. |
| $\sigma^2_w = \frac{1}{i} \sum_i \sigma^2_{w_i}$ | Multicarrier modulation variance. Average modulation variance of the $l$ Gaussian sub-channels $\mathcal{N}_i$. |
| $|\phi_i\rangle = \text{IFFT}(z_{k,i}) = F^{-1}(z_{k,i}) = |d_i\rangle.$ | The $i$-th Gaussian subcarrier CV of user $U_k$, where IFFT stands for the Inverse Fast Fourier Transform, $|\phi_i\rangle \in S$, $d_i \in \mathbb{C}N\left(0, \sigma^2_{d_i}\right)$, $\sigma^2_{d_i} = \mathbb{E}\left[|d_i|^2\right]$, $d_i = x_{d_i} + ip_{d_i}$, $x_{d_i} \in \mathbb{N}\left(0, \sigma^2_{\omega_p}\right)$, $p_{d_i} \in \mathbb{N}\left(0, \sigma^2_{\omega_y}\right)$ are i.i.d. zero-mean Gaussian random quadrature components, and $\sigma^2_{\omega_y}$ is the variance of the Fourier transformed Gaussian state. |
| $|\varphi_{k,i}\rangle = \text{CVQFT}(|\phi_i\rangle)$ | The decoded single-carrier CV of user $U_k$ from the subcarrier CV, expressed as $F(|d_i\rangle) = F\left(F^{-1}(z_{k,i})\right) = |z_{k,i}\rangle$. |
| $\mathcal{N}$ | Gaussian quantum channel. |
| $\mathcal{N}_i, i = 0, \ldots, n - 1$ | Gaussian sub-channels. |
| $T(\mathcal{N})$ | Channel transmittance, normalized complex random variable, $T(\mathcal{N}) = \text{Re}\ T(\mathcal{N}) + i \text{Im}\ T(\mathcal{N}) \in \mathbb{C}$. 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 $\mathcal{N}_i$, $T_i(\mathcal{N}_i) = \text{Re}\ (T_i(\mathcal{N}_i)) + i \text{Im}\ (T_i(\mathcal{N}_i)) \in \mathbb{C}$, quantifies the position and momentum quadrature transmission, with (normalized) real and imaginary parts. |
\[
\begin{align*}
0 \leq \text{Re} T_i(N_i) & \leq 1/\sqrt{2}, \quad 0 \leq \text{Im} T_i(N_i) \leq 1/\sqrt{2}, \quad \text{where} \\
\text{Re} T_i(N_i) &= \text{Im} T_i(N_i).
\end{align*}
\]

| \( T_{\text{Eve}} \) | Eve’s transmittance, \( T_{\text{Eve}} = 1 - T(N) \). |
| \( T_{\text{Eve,i}} \) | Eve’s transmittance for the \( i \)-th subcarrier CV. |

\[
z = x + ip = (z_0, \ldots, z_{d-1})^T
\]

A \( d \)-dimensional, zero-mean, circular symmetric complex random Gaussian vector that models \( d \) Gaussian CV input states, \( \mathcal{CN}(0, K_z) \), \( K_z = \mathbb{E}[zz^\dagger] \), where \( z_i = x_i + ip_i \), \( x = (x_0, \ldots, x_{d-1})^T \), \( p = (p_0, \ldots, p_{d-1})^T \), \( x_i \in \mathcal{N}(0, \sigma^2_{\omega_0}) \), \( p_i \in \mathcal{N}(0, \sigma^2_{\omega_0}) \) i.i.d. zero-mean Gaussian random variables.

\[
d = F^{-1}(z)
\]

An \( l \)-dimensional, zero-mean, circular symmetric complex random Gaussian vector, \( \mathcal{CN}(0, K_d) \), \( K_d = \mathbb{E}[dd^\dagger] \), \( d = (d_0, \ldots, d_{l-1})^T \), \( d_i = x_i + ip_i \), \( x_i, p_i \in \mathcal{N}(0, \sigma^2_{\omega_p}) \) are i.i.d. zero-mean Gaussian random variables, \( \sigma^2_{\omega_p} = 1/\sigma^2_{\omega_0} \). The \( i \)-th component is \( d_i \in \mathcal{CN}(0, \sigma^2_d) \), \( \sigma^2_d = \mathbb{E}[|d_i|^2] \).

\[
y_k \in \mathcal{CN}(0, \mathbb{E}[y_ky_k^\dagger])
\]

A \( d \)-dimensional zero-mean, circular symmetric complex Gaussian random vector.

\[
y_{k,m}
\]

The \( m \)-th element of the \( k \)-th user’s vector \( y_k \), expressed as \( y_{k,m} = \sum_i F(T_i(N_i))F(d_i) + F(\Delta_i) \).

\[
F(T(N))
\]

Fourier transform of \( T(N) = [T_0(N_0), \ldots, T_{l-1}(N_{l-1})]^T \in \mathbb{C}^l \), the complex transmittance vector.

\[
F(\Delta)
\]

Complex vector, expressed as \( F(\Delta) = e^{-F(\Delta)^T K_F(\Delta) F(\Delta)/2} \), with covariance matrix \( K_{F(\Delta)} = \mathbb{E}[F(\Delta)F(\Delta)^\dagger] \).

\[
y[j]
\]

AMQD block, \( y[j] = F(T(N))F(d)[j] + F(\Delta)[j] \).

\[
\tau = \|F(d)[j]\|^2
\]

An exponentially distributed variable, with density \( f(\tau) = (1/2\sigma^2_\omega)e^{-\tau/2\sigma^2_\omega} \), \( \mathbb{E}[\tau] \leq n\sigma^2_\omega \).

\[
T_{\text{Eve,i}}
\]

Eve’s transmittance on the Gaussian sub-channel \( N_i \).
\[ T_{\text{Eve},i} = \text{Re}T_{\text{Eve},i} + i\text{Im}T_{\text{Eve},i} \in \mathcal{C}, \quad 0 \leq \text{Re}T_{\text{Eve},i} \leq 1/\sqrt{2}, \]
\[ 0 \leq \text{Im}T_{\text{Eve},i} \leq 1/\sqrt{2}, \quad 0 \leq |T_{\text{Eve},i}|^2 < 1. \]

\[ d_i \]
A \( d_i \) subcarrier in an AMQD block.

\[ \nu_{\text{min}} \]
The min \( \{\nu_0, \ldots, \nu_{l-1}\} \) minimum of the \( \nu_i \) sub-channel coefficients, where \( \nu_i = \sigma^2_{\mathcal{N}}/|F(T_i(\mathcal{N}_i))|^2 \) and \( \nu_i < \nu_{\text{Eve}} \).

\[ \sigma^2_\omega \]
Modulation variance, \( \sigma^2_\omega = \nu_{\text{Eve}} - \nu_{\text{min}}G(\delta)_{p(x)} \), where
\[ \nu_{\text{Eve}} = \frac{1}{\lambda}, \quad \lambda = \left|F(T^*_\mathcal{N})\right|^2 = \frac{1}{n} \sum_{i=0}^{n-1} \left| \sum_{k=0}^{n-1} T^*_k e^{-ik\pi_0} \right|^2 \]
and \( T^*_\mathcal{N} \) is the expected transmittance of the Gaussian sub-channels under an optimal Gaussian collective attack.

S.2 Abbreviations

| Abbreviation | Description |
|--------------|-------------|
| AMQD         | Adaptive Multicarrier Quadrature Division |
| CV           | Continuous-Variable |
| CVQFT        | Continuous-Variable Quantum Fourier Transform |
| CVQKD        | Continuous-Variable Quantum Key Distribution |
| DV           | Discrete Variable |
| FFT          | Fast Fourier Transform |
| IFFT         | Inverse Fast Fourier Transform |
| MQA          | Multiuser Quadrature Allocation |
| QKD          | Quantum Key Distribution |
| SNR          | Signal to Noise Ratio |