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

Laszlo Gyongyosi¹,²,³ · Sandor Imre²

Received: 6 June 2019 / Accepted: 24 September 2019 © The Author(s) 2019

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

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

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

The relevant performance attributes of experimental CVQKD (i.e., secret key rates, transmission distances, tolerable excess noise, etc.) still require significant improvements [6, 11–14, 17, 49, 58, 59]. The multicarrier CVQKD has been recently introduced through the adaptive quadrature division modulation (AMQD) [15]. The multicarrier CVQKD scheme injects several additional degrees of freedom into the transmission, which are not available for a standard (single carrier) CVQKD setting [15, 17, 18, 20–24, 27–31, 64, 65]. These results also made possible to utilize several significant phenomena for CVQKD that are unavailable in a standard CVQKD protocol [16–18, 21–23, 28, 29]. The secret key rates of multicarrier CVQKD confirm the...
multimode bounds of [7] (see the results on fundamental rate-loss scaling in quantum optical communications in [7]). Further information on the bounds of private quantum communications can be found in [8].

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

The novel contributions of our manuscript are as follows:

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

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

Multiuser quadrature allocation (MQA)

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

\[
\mathcal{M}_{U_k} = [\mathcal{N}_{U_{k,0}}, \ldots, \mathcal{N}_{U_{k,m-1}}]^T,
\]

where \(\mathcal{N}_{U_{k,j}}^j\) is the \(j\)th sub-channel of \(\mathcal{M}_{U_k}\). For a detailed description of MQA for multi-carrier CVQKD, see [20].

Private Classical Rate Curves

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

\[
\mathcal{S} = \{R_{\text{min}}(\mathcal{N}_i^i), R(q), R_{\text{max}}(\mathcal{N}_i^i)\}, q = 0 \ldots r - 1. \tag{2}
\]

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

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

\[
R_{\text{min}}(\mathcal{N}_i^i) < R(0) \ldots < R(r - 1) < R_{\text{max}}(\mathcal{N}_i^i), \tag{3}
\]

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

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

\[
R(q) \leq P(\mathcal{N}_i^i) = \lim_{n \to \infty} \frac{1}{n} \max_{\eta \in P_i, \rho_i} \left(\chi_{AB}(\mathcal{N}_i^i) - \chi_{BE}(\mathcal{N}_i^i)\right), \tag{4}
\]

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

Secret Key Rate Adaption with Minimized Error Rate

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

\textbf{Proof} The proof focuses on a single sub-channel \(\mathcal{N}_i^i\) for the private transmission of a single quadrature component \(x_i^i\) or \(p_i^i\), which refers to a \(x_i^i \in \mathcal{N}(0, \sigma^2_m)\) position or a \(p_i^i \in \mathcal{N}(0, \sigma^2_m)\) momentum quadrature of the \(i\)th subcarrier, respectively.
Let
\[ v_i(N_i) = \frac{\sigma_i^2}{\left| F(T_i(N_i)) \right|^2}, \]  
\[ (5) \]
of the \( i \)-th, \( i = 0, \ldots, I - 1 \) sub-channel \( N_i \).

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

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

From \( R_{\min}(N_i) \) and \( R_{\max}(N_i) \), an adaption region \( A \) can be characterized with \( r \) rate curves inside the region. Define \( r \) rate curves for the transmission of \( x_i \) in the region of \( A \)
\[ A = [R_{\min}(N_i), R_{\max}(N_i)], \]  
\[ (6) \]
as
\[ R(q), q = 0 \ldots r - 1, \]  
\[ (7) \]
such that (3) holds.

Precisely, at a given private rate \( R(N_i) \), (5) is referred to as \( v_i(R(N_i)) \).

\[ v_i(R(N_i)) = \frac{\sigma_i^2}{\left| F(T_i(N_i)) \right|^2}, \]  
\[ (8) \]
where \( \sigma_i^2 \) is the noise variance of \( N_i \) at \( R(N_i) \), while \( F(T_i(N_i)) \) is the transmittance coefficient of \( N_i \) at \( R(N_i) \). Note that in function of (8), after a scaling the rate curves of (7) are almost parallel to \( R_{\min}(N_i) \). By theory, at \( R(N_i) = 0 \)
\[ (8) \]is directly defined from \( \sigma_i^2 \) is the noise variance and \( T_i(N_i) \) is the transmittance coefficient of \( N_i \), as given in (5).

In function of \( v_i(R(N_i)) \), the SNR of \( N_i \) at a given \( R(N_i) \) is expressed as [55]
\[ \text{SNR}(R(N_i)) = 10 \log_{10} \frac{1}{v_i(R(N_i))}. \]  
\[ (9) \]
To step forward, we have to focus on the behavior of parameter \( v_i(\cdot) \) at an increased transmission rate.

Particularly, let \( R(N_i) \) be the current private rate and \( \tilde{R}(N_i) \) be the target private rate for a sub-channel \( N_i \), such that \( R(N_i) < R(N_i) < \tilde{R}(N_i) \). Then, let \( \delta_i(\tilde{R}(N_i)) \) identify the cumulative \( v_i(R(N_i)) \) parameter of \( N_i \) at an increased (target) private rate \( R(N_i) \), evaluated via the following iteration:
\[ \delta_i(\tilde{R}(N_i)) = \delta_i(R(N_i)) + \Delta_i(R(N_i), \tilde{R}(N_i)), \]  
\[ (10) \]
where \( \Delta_i \) identifies the difference of \( v_i \) at \( R(N_i) \) and \( \tilde{R}(N_i) \) as
\[ \Delta_i = v_i(R(N_i)) - v_i(\tilde{R}(N_i)), \]  
\[ (11) \]
the iteration (10) at no transmission, \( R(N_i) = 0 \), identifies \( v_i(N_i) \) as
\[ \delta_i(R(N_i)) = 0 = v_i(N_i). \]  
\[ (12) \]
while for any \( R(N_i) > R(N_i) > 0 \),
\[ v_i(R(N_i)) < v_i(R(N_i)). \]  
\[ (13) \]
To conclude, from (10) follows that a rate increment from \( R(N_i) \) to \( \tilde{R}(N_i) \) also increases \( \delta_i(R(N_i)) \) by \( \Delta_i(R(N_i), \tilde{R}(N_i)), \) thus for any \( R(N_i) > R(N_i), \) the following relation holds [55]:
\[ \delta_i(R(N_i)) > \delta_i(R(N_i)). \]  
\[ (14) \]
Let us then define \( r \) private transmission curves in the adaption region \( A \) of \( N_i \). The aim of the iterative secret key adaption scheme is to provide a rate increment in each step by selecting that sub-channel \( N_i \), for which (10) is minimal. Specifically, it is a convenient approach because this sub-channel provides the best condition for the transmission.

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

Applying (10) for a \( R_{\min}(N_i) \) private rate is as follows. An \( R_{\min}(N_i) \) target private rate over \( N_i \), \( v_i(R_{\min}(N_i)) \) is yielded via \( v_i(N_i) \) and \( \Delta_i(R_{\min}(N_i), R(0)) \) derived from \( R(0) \in A \) as
\[ \delta_i(R_{\min}(N_i)) = v_i(N_i) + \Delta_i(R_{\min}(N_i), R(0)). \]  
\[ (15) \]
Applying (10) to the \( r \) rate curves \( R(q) \in A, q = 0 \ldots r - 2 \) at a target rate \( R(q) \) results in \( \delta_i(R(q)) \) as
where \( R(1) \in A \). While, for \( q = r - 1 \), (10) results in

\[
\delta_{\nu_i}(R(r-1)) = \delta_{\nu_i}(R(r-2)) + \Delta_{\nu_i}(R(r-1), R_{\max}(N_i)) \nonumber
\]

\[
= \left( \nu_i(N_i) + \Delta_{\nu_i}(R_{\min}(N_i), R(0)) + \sum_{k=0}^{r-2} \Delta_{\nu_i}(R(k), R(k+1)) + \Delta_{\nu_i}(R(r-1), R_{\max}(N_i)) \right),
\]

where \( R(k) \in A, k = 0 \ldots r - 2 \). For \( R_{\max}(N_i) \), by definition \( \delta_{\nu_i}(R_{\max}(N_i)) = +\infty \) [55].

The distribution of a sample set \( \delta_{\nu_i}(R(q)) \) for \( m \) sub-channels, \( i = 0, \ldots, m - 1 \), in a low-SNR CVQKD scenario is illustrated in Fig. 1a. The SNR in Fig. 1b is derived from the \( \delta_{\nu_i}(R(q)) \) set of the \( m \) sub-channels as

\[
\text{SNR} = 10 \log_{10} \left( \frac{1}{\nu_i(R(q))} \right).
\]

Next, we show that for an arbitrary target private rate \( R^*(N_i) > 0 \), the iterative condition on \( \delta_{\nu_i}(R^*(N_i)) \) (see (16)) provides a minimized error rate over the selected \( N_i \).

Let \( B \) be the bit error rate (BER), and let

\[
B(R(q)_{\delta_{\nu_i}(R(q))})
\]

refer to the bit error rate of \( N_i \) at target private rate \( R(q) \), at an actual rate \( R(q - 1) \), and \( \delta_{\nu_i}(R(q - 1)) \). Then, at a given \( R(q) \), selecting that \( N_i, i = 0, \ldots, l - 1 \) from the total \( l \), for which \( \delta_{\nu_i}(R(q - 1)) \) is minimal, as

\[
\xi(R(q - 1)) = \min_{\nu_i} \delta_{\nu_i}(R(q - 1))
\]

yields a minimized bit error rate at a given \( R(q) \) over the selected \( N_i \) as

\[
B(R(q)_{\xi(R(q))}) = B(R_{\min}(N_i)_{\delta_{\nu_i}(R(q))}),
\]

where

\[
B(R_{\min}(N_i)_{\delta_{\nu_i}(R(q))})
\]

is defined as

\[
\frac{1}{2} \text{erfc} \bigg( \nu_i(N_i) + \left( \Delta_{\nu_i}(R_{\min}(N_i), R(0)) + \sum_{k=0}^{q-1} \Delta_{\nu_i}(R(k), R(k+1)) \right) \bigg) + \Delta_{\nu_i}(R(q-1), R(q))
\]

where function \( \text{F}() \) is evaluated as

\[
\delta_{\nu_i}(R(q))
\]

\[
\text{SNR}
\]

\[
\text{Data unit index}
\]

(a) (b)

**Fig. 1** a The distribution of a low-SNR set \( \delta_{\nu_i}(R(q)) \), \( i = 0, \ldots, m - 1 \), for \( m = 1000 \) sub-channels. b The SNR is derived from \( \delta_{\nu_i}(R(q)) \) for all sub-channels.
\[ F(v_i(N_i) + \Delta v_i(R_{\min}(N_i), R(0)) + \cdots + \Delta v_i(R(q-1), R(q))) \]
\[ = \left[ \text{SNR}(v_i(N_i)) \right] - \left[ \text{SNR}(v_i(R(0))) - \text{SNR}(v_i(R_{\min}(N_i))) \right] \]
\[ = \frac{1}{\sqrt{\pi}} \int_{x}^\infty e^{-t^2} \, dt. \tag{23} \]

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

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

First, we apply (19) to the minimal rate \( R_{\min}(N_i) \) by the selection of that \( N_i \), for which \( v_i(N_i) \) is minimal, thus
\[ \xi(0) = \min \Delta v_i(0) = \min v_i, \tag{24} \]
which yields
\[ B(R_{\min}(N_i)\xi(0)) = B(R_{\min}(N_i)v_i(N_i)). \tag{25} \]

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

In particular, due to the iterative determination of \( \delta_{v_i}(R_{\min}(N_i)) \), the corresponding \( B(R(0)\xi(R_{\min}(N_i))) \) is yielded as
\[ B(R(0)\xi(R_{\min}(N_i))) = B(R_{\min}(N_i)v_i(N_i) + \Delta v_i(R_{\min}(N_i), R(0))). \tag{26} \]

Precisely, for \( R(q), q = 1 \ldots r-1 \), therefore, in each step, that sub-channel selected for the transmission, for which \( \xi(R(q-1)) \) is minimal, ensures that the resulting \( B(R(q)\xi(R(q-1))) \) is evaluated as
\[ B(R(q)\xi(R(q-1))) = B(R_{\min}(N_i)\delta_{v_i}(R(q-2)) + \Delta v_i(R(q-1), R(q))). \tag{27} \]

Putting the pieces together, the utilization of (27) for \( q = 1 \) is as
\[ B(R(1)\xi(R(0))) = B(R_{\min}(N_i)\delta_{v_i}(R_{\min}(N_i)) + \Delta v_i(R(0), R(1))), \tag{28} \]
while for \( q = r-1 \),
\[ B(R(r-1)\xi(R(r-2))) = B(R_{\min}(N_i)\delta_{v_i}(R(r-3)) + \Delta v_i(R(r-2), R(r-1))), \tag{29} \]
and, finally, for \( R_{\max}(N_i) \), the corresponding error rate is
\[ B(R_{\max}(N_i)\xi(R(r-1))) = B(R_{\min}(N_i)\delta_{v_i}(R(r-2)) + \Delta v_i(R(r-1), R_{\max}(N_i))). \tag{30} \]

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

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

Algorithm 1 Iterative secret key rate adaption for multicarrier CVQKD.

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

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

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

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

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

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

Secret Key Rate Adaption in Multiuser Multicarrier CVQKD

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

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

Fig. 3 The $B$ bit error rate of secret key adapting for a sub-channel $N_i$, in function of $v_i(R(x)) = 10^{-5}\text{SNR}(v_i(R(x))/10}$. The adaption is made via $r$ rate curves $R(q), q = 0 \ldots r - 1$, $R_{\text{min}}(N_i) < R(0) < \ldots < R(r - 1) < R_{\text{max}}(N_i)$ in the $\Lambda = [R_{\text{min}}(N_i), R_{\text{max}}(N_i)]$ adaption region (shaded area).
**Proof** The proof focuses on a given logical channel \( \mathcal{M}_{U_k} = \left[ N_{U_i,0}, \ldots, N_{U_i,m-1} \right]^T \) of a user \( U_k \), where \( N_{U_i,j}, i = 0, \ldots, m - 1 \) is the \( i \)th sub-channel.

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

Let

\[
v_i(\mathcal{N}_{U_{ij}}) = \frac{\sigma_{N_{U_{ij}}}^2}{\left| F(T(\mathcal{N}_{U_{ij}})) \right|^2},
\]

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

\[
v_i(R(\mathcal{N}_{U_{ij}})) = \frac{\sigma_{R(\mathcal{N}_{U_{ij}})}^2}{\left| F(T(R(\mathcal{N}_{U_{ij}}))) \right|^2},
\]

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

\[
S'(\mathcal{M}_{U_k}) \leq \sum_{i=0}^{m-1} R(\mathcal{N}_{U_{ij}}).
\]

Apply the steps for all transmit users \( U_k \) for their \( \mathcal{M}_{U_k} \) sets of \( m \) sub-channels. Therefore, one can utilize (27) at a given \( R(\mathcal{N}_{U_{ij}}) = R(q) \), where \( R(q) \) refers to the \( R(q) \) curve of \( \mathcal{N}_{U_{ij}} \), and from (12) follows \( R_i(0) = v_i(\mathcal{N}_{U_{ij}}, i = 0, \ldots, m - 1 \) yields the error rate for \( \mathcal{N}_{U_{ij}} \) of \( \mathcal{M}_{U_k} \) as

\[
B(R(\mathcal{N}_{U_{ij}}), R(q) - i) = B(\min(\mathcal{N}_{U_{ij}}, i) + \Delta, (\min(\mathcal{N}_{U_{ij}}, i) + \sum_{i=1}^{m} \Delta_i(R(q) + 1)))\).
\]

\( \forall \) (34)

**Theorem 2** For all \( U_k, k = 0, \ldots, K - 1 \), the error rate of the \( \mathcal{N}_{U_{ij}}, i = 0, \ldots, m - 1 \) sub-channels of \( \mathcal{M}_{U_k} \) of user \( U_k \) can be equally minimized via \( \delta_{\alpha} = \sigma_{\alpha}^2 + \Delta_{\alpha} \) modulation variance correction, where \( \Delta_{\alpha} > 0 \).

**Proof** Let

\[
R_i(\mathcal{N}_{U_{ij}}) = R_i(q) - i, q = 0, \ldots, r - 1, \quad (35)
\]

and \( R(\mathcal{N}_{U_{ij}}) \) be the target private rate,

\[
R(\mathcal{N}_{U_{ij}}) = R_i(q), \quad (36)
\]

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

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

\[
\xi_{U_k} = \min_{\forall U_k \in \mathcal{M}_{U_k}} \delta_i(R(\mathcal{N}_{U_{ij}})).
\]

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

\[
\Delta_{\alpha} = \delta_i(R(\mathcal{N}_{U_{ij}})) - \xi_{U_k}, \quad (38)
\]

yielding a modulation variance increment

\[
\delta_{\alpha}^2 = \sigma_{\alpha}^2 + \Delta_{\alpha} \quad (39)
\]

for the input of \( \mathcal{N}_{U_{ij}} \).

In particular, using (39), the \( \varphi_{\delta} \) \( R(\mathcal{N}_{U_{ij}}) \) resulting \( \delta_i \) parameter for \( \mathcal{N}_{U_{ij}} \) at a target rate \( R(\mathcal{N}_{U_{ij}}) \) is, therefore,

\[
\varphi_{\delta_i}(R(\mathcal{N}_{U_{ij}})) = \delta_i(R(\mathcal{N}_{U_{ij}})) - \xi_{U_k}, \quad (40)
\]

from which the \( \Delta_{\text{SNR}} \) parameter \( \varphi_{\delta_i}(R(\mathcal{N}_{U_{ij}})) \) SNR increment of \( \mathcal{N}_{U_{ij}} \) at a given \( R(\mathcal{N}_{U_{ij}}) = R(q) \) is as

\[
\Delta_{\text{SNR}} \left( \varphi_{\delta_i}(R(\mathcal{N}_{U_{ij}})) \right) = 10\log_{10} \frac{1}{\delta_{\alpha}} - \mathcal{F}(v_i(\mathcal{N}_{U_{ij}}) + \Delta_i, v_i(\min(\mathcal{N}_{U_{ij}}, i), R(q) + 1)),
\]

(41)

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

---

**Variance Adaption for an Equalized Error Rate**

In this section, we propose a modulation variance adaption method to achieve an equally minimized error rate for the sub-channels of a given user. The results can be extended to an arbitrary number of users.
Therefore, the $\mathcal{B}(R(\mathcal{N}_{U_{k}}), \xi_{U_{k}})$ error rate for all $\mathcal{N}_{U_{k}}$ at an arbitrary $R(\mathcal{N}_{U_{k}})_{k_{i}}(R(\mathcal{N}_{U_{k}}))$ is equally minimized by $\xi_{U_{k}}$ via (21) as

$$
\mathcal{B}
 = \min_{\forall i \in \mathcal{M}_{U_{k}}} \mathcal{B}
\left(R(\mathcal{N}_{U_{k}})_{k_{i}}(R(\mathcal{N}_{U_{k}})) \right),
$$

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

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

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

The proof is concluded here. \hfill \Box

**Numerical Evidence**

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

**Parameters**

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

The single-carrier inputs of user $U_{k}$,

$$
x_{U_{k},i} \in \mathcal{N}(0, \sigma_{0}^{2}),
$$

have a modulation variance of $\sigma_{0}^{2}$ and formulate a $d$-dimensional input vector $x_{U_{k},i}$.

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

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

$$
x_{U_{k},i,j} \in \mathcal{N}(0, \sigma_{i}^{2}),
$$

and has a modulation variance of $\sigma_{i}^{2}$.

The $m$ sub-channels,

$$\mathcal{N}_{U_{k},i,j}, i = 0, \ldots, m - 1,$$

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

$$\mathcal{M}_{U_{k}} = [\mathcal{N}_{U_{k},0}, \ldots, \mathcal{N}_{U_{k},m-1}]^{T}.$$ 

The $\Delta_{x_{i}} \in \mathcal{N}(0, \sigma^{2}_{\mathcal{N}_{U_{k},i}})$ noise of $\mathcal{N}_{U_{k},i}$ is added to the subcarriers, where $\sigma^{2}_{\mathcal{N}_{U_{k},i}}$ is the noise variance of $\mathcal{N}_{U_{k},i}$.

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

The $\delta v_{i}(R(\mathcal{N}_{U_{k},i,j}))$ of $\mathcal{N}_{U_{k},i,j}$ parameters are determined from $v_{i}(\mathcal{N}_{U_{k},i,j})$ for all sub-channels via the iterative method of Theorem 2.

**Modulation Variance Adaption**

The analysis focuses on a low-SNR CVQKD scenario. An initial low-SNR set of $\delta v_{i}(R(\mathcal{N}_{U_{k},i,j})), i = 0, \ldots, m - 1$ of user $U_{k}$ from a low-SNR scenario is illustrated in Fig. 4a. The minimum of the set is $\xi_{U_{k}} = \min \delta v_{i}(R(\mathcal{N}_{U_{k},i,j}))$, from which the modulation variance correction for $\mathcal{N}_{U_{k},i,j}$ is

$$\Delta_{\sigma_{i}} = \delta v_{i}(R(\mathcal{N}_{U_{k},i,j})) - \xi_{U_{k}}.$$ 

The corresponding $\Delta_{\sigma_{i}}$ (see (38)), $i = 0, \ldots, m - 1$ values determined from the $\delta v_{i}(R(\mathcal{N}_{U_{k},i,j}))$ elements are depicted in Fig. 4b.

In a low-SNR setting due to the value range of $\delta v_{i}(R(\mathcal{N}_{U_{k},i,j}))$, $i = 0, \ldots, m - 1$, the required $\Delta_{\sigma_{i}}$ variance correction for the subcarriers is, therefore, negligible.

The $x_{U_{k},i,j}, i = 0, \ldots, m - 1$ input quadratures of user $U_{k}$ with a constant variance $\sigma_{0}^{2}$ are illustrated in Fig. 5a. Applying the result of $\Delta_{\sigma_{i}}$, the $x_{U_{k},i,j}, i = 0, \ldots, m - 1$ input quadratures of user $U_{k}$ at the $\tilde{\sigma}_{i}^{2} = \sigma_{0}^{2} + \Delta_{\sigma_{i}}$ increased variance are depicted in Fig. 5b.

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

**SNR Differences**

The effects of the $\Delta_{\sigma_{i}}$ variance correction and the resulting $\varphi_{\delta v_{i}}(R(\mathcal{N}_{U_{k},i,j}))$ can be expressed in terms of the resulting SNR change.

The $\Delta_{\text{SNR}}(\sigma_{i}) = \text{SNR}(\sigma_{i}^{2}) - \text{SNR}(\sigma_{0}^{2})$. $i = 0, \ldots, m - 1$, SNR difference for the input quadratures of $\{x_{U_{k},i,j}, \tilde{x}_{U_{k},i,j}\}$ at $\sigma_{0}^{2}$ and $\tilde{\sigma}_{i}^{2} = \sigma_{0}^{2} + \Delta_{\sigma_{i}}$ is depicted in Fig. 6a. The $\Delta_{\text{SNR}}(\varphi_{\delta v_{i}}(R(\mathcal{N}_{U_{k},i,j})))$ SNR differences (see (41)) achieved
at a given $\delta_{\nu_i}(R(N_{Uk,i}))$, $i = 0, \ldots, m - 1$, are illustrated in Fig. 6b.

The $\Delta_{\text{SNR}}(\sigma^2_{\omega_i})$ input SNR difference results in an improved $\Delta_{\text{SNR}}(\varphi_{\delta_{\nu_i}}(R(N_{Uk,i})))$ parameter via $\varphi_{\delta_{\nu_i}}(R(N_{Uk,i}))$ for all $i$.

**Error Rate Minimization**

The BER values for the initial low-SNR set and for the set of $\delta_{\nu_i}(R(N_{Uk,i}))$ are compared in Fig. 2. The BER of $N_{Uk,i}$ at the initial low-SNR set of $\delta_{\nu_i}(R(N_{Uk,i})), i = 0, \ldots, m - 1$, is illustrated in Fig. 7a. The BER of the $m$ sub-channels $N_{Uk,i}, i = 0, \ldots, m - 1$, at $\varphi_{\delta_{\nu_i}}(R(N_{Uk,i}))$, is depicted in Fig. 7b.

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

---

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

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

---

**SN Computer Science**

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

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

**Conclusions**

![Graphs showing SNR and BER](image)

**Figures**

**Fig. 6** a The $\Delta_{\text{SNR}}\left(\sigma_m^2, \tilde{\sigma}_m^2\right)$ parameter for $i = 0, \ldots, m-1, m = 1000$ at $\sigma_m^2$ and $\tilde{\sigma}_m^2$. b The $\varphi_{\delta_i}\left(R(N_{U_i})\right)$ parameter, $i = 0, \ldots, m-1, m = 1000$

**Fig. 7** a The BER for the initial low-SNR set $\delta_{\varphi_i}(R(N_{U_i})), i = 0, \ldots, m-1, m = 1000$ (the minimum of the set is depicted by the green solid line). b The BER values for $\varphi_{\delta_i}(R(N_{U_i})), i = 0, \ldots, m-1, m = 1000$
Author Contributions LGY designed the protocol and wrote the manuscript. LGY and SI analyzed the results. All authors reviewed the manuscript.

Funding We have no competing financial interests.

Data Availability This work does not have any experimental data.

Compliance with Ethical Standards

Conflict of Interest We have no competing interests.

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

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

Appendix

Multicarrier CVQKD

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

In the single-carrier modulation scheme, the $j$th input single-carrier state $|\phi_j\rangle = |x_j + ip_j\rangle$ is a Gaussian state in the phase space $\mathcal{S}$, with i.i.d. Gaussian random position and momentum quadratures $x_j \sim \mathcal{N}(0, \sigma_{x_0}^2)$, $p_j \sim \mathcal{N}(0, \sigma_{p_0}^2)$, where $\sigma_{x_0}^2$ is the modulation variance of the quadratures. (For simplicity, $\sigma_{x_0}^2$ is referred to as the single-carrier modulation variance, throughout.) Particularly, this Gaussian single carrier is transmitted through a Gaussian quantum channel $\mathcal{N}_i$. In the multicarrier scenario, the information is carried by Gaussian subcarrier CVs, $|\phi_j\rangle = |x_j + ip_j\rangle$, $x_j \sim \mathcal{N}(0, \sigma_{x_0}^2)$, $p_j \sim \mathcal{N}(0, \sigma_{p_0}^2)$, where $\sigma_{x_0}^2$ is the modulation variance of the subcarrier quadratures, which are transmitted through a noisy Gaussian sub-channel $\mathcal{N}_i$. 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 $j$ refers to the single carriers throughout the manuscript.) The single-carrier state $|\phi_j\rangle$ in the phase space $\mathcal{S}$ can be modeled as a zero-mean, circular symmetric complex Gaussian random variable $z_j \sim \mathcal{C}\mathcal{N}(0, \sigma_{z_0}^2)$, with variance $\sigma_{z_0}^2 = \mathbb{E}\left[|z_j|^2\right]$, and with i.i.d. real and imaginary zero-mean Gaussian random components $\Re(z_j) \sim \mathcal{N}(0, \sigma_{\Re z_0}^2)$, $\Im(z_j) \sim \mathcal{N}(0, \sigma_{\Im z_0}^2)$.

In the multicarrier CVQKD scenario, let $n$ be the number of Alice’s input single-carrier Gaussian states. The $n$ input coherent states are modeled by an $n$-dimensional, zero-mean, circular symmetric complex random Gaussian vector $\mathbf{z} = \mathbf{x} + \mathbf{i}\mathbf{p} = (z_1, \ldots, z_n)^T \sim \mathcal{C}\mathcal{N}(0, \mathbf{K}_x)$ (47) where each $z_j$ can be modeled as a zero-mean, circular symmetric complex Gaussian random variable $z_j \sim \mathcal{C}\mathcal{N}(0, \sigma_{z_0}^2)$.

Specifically, the real and imaginary variables (i.e., 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

$$f(z_j) = \frac{1}{\sigma_{z_0} \sqrt{2\pi}} e^{-\frac{|z_j|^2}{2\sigma_{z_0}^2}}, \quad f(p_j) = \frac{1}{\sigma_{p_0} \sqrt{2\pi}} e^{-\frac{p_j^2}{2\sigma_{p_0}^2}}, \quad (50)$$

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

$$\mathbf{K}_x = \mathbb{E}[\mathbf{zz}^T],$$

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

For vector $\mathbf{z}$, $\mathbb{E}[|\mathbf{z}|] = \mathbb{E}[e^{\mathbf{y}^T \mathbf{z}}] = \mathbb{E}[e^{\mathbf{y}^T \mathbf{z}}]$. (51) holds, and

$$\mathbb{E}[\mathbf{zz}^T] = \mathbb{E}[e^{\mathbf{y}^T \mathbf{z}(\mathbf{y}^T \mathbf{z})^T}] = \mathbb{E}[e^{2\mathbf{y}^T \mathbf{zz}^T}],$$

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

$$f(\mathbf{z}) = \frac{1}{\det(\mathbf{K}_x)} e^{-\mathbf{z}^T \mathbf{K}_x^{-1} \mathbf{z}}. \quad (53)$$

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

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

The Fourier transformation $F(\cdot)$ of the $n$-dimensional Gaussian random vector $\mathbf{z} = (z_1, \ldots, z_n)^T$ results in the $n$-dimensional Gaussian random vector $\mathbf{m} = (m_1, \ldots, m_n)^T$, as:
In the first step of AMQD, Alice applies the inverse FFT (fast Fourier transform) operation to vector $z$, which results in an $n$-dimensional zero-mean, circular symmetric complex Gaussian random vector $d$, as

$$d = F^{-1}(z) = e^{-\frac{m^T A m}{2}} = e^{-\frac{\sigma_{\omega_0}^2 (m_1^2 + \ldots + m_n^2)}{2}}. \quad (55)$$

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

$$\Delta = (\Delta_1, \ldots, \Delta_n)^T \in \mathcal{CN}(0, K_\Delta), \quad (66)$$

where

$$K_\Delta = E[\Delta \Delta^*]. \quad (67)$$

with independent, zero-mean Gaussian random components

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

and

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

with variance $\sigma_{\Delta_i}^2$, 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 $S$.

The CVQFT-transformed noise vector can be rewritten as

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

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

$$K_{F(\Delta)} = E[F(\Delta)F(\Delta)^*], \quad (71)$$

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

$$\frac{1}{n} \sum_{i=1}^{n} \sigma_{\omega_i}^2 = \sigma_{\omega_0}^2, \quad (72)$$

where $\sigma_{\omega_0}^2$ is the modulation variance of the quadratures of the subcarrier $|\phi_i\rangle$ transmitted by sub-channel $\mathcal{N}_i$. Assuming $l$ good Gaussian sub-channels from the $n$ with constant quadrature modulation variance $\sigma_{\omega_i}^2$, where $\sigma_{\omega_0}^2 = 0$ for the $i$th unused sub-channel

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

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

$$|T_{AMQD}(\mathcal{N}_i)|^2 \sigma_{\omega_0}^2 > |T(\mathcal{N})|^2 \sigma_{\omega_0}^2, \quad (74)$$
where \(|T(\mathcal{N})|^2\) is the transmittance of \(\mathcal{N}\) in a single-carrier scenario, and

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

(A.2) Notations

The notations of the manuscript are summarized in Table 1.

Table 1 Summary of notations

| Notation       | Description                                                                 |
|----------------|----------------------------------------------------------------------------|
| \(l\)          | 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, \(|\phi_j\rangle = x_j + ip_j\). |
| \(l\)          | Number of Gaussian sub-channels \(\mathcal{N}_i\) for the transmission of the Gaussian subcarriers. The overall number of the sub-channels is \(n\). The remaining \(n-l\) sub-channels do not transmit valuable information. |
| \(x_i, p_i\)   | Position and momentum quadratures of the \(i\)-th Gaussian subcarrier, \(|\phi_i\rangle = x_i + ip_i\). |
| \(x'_j, p'_j\) | Noisy position and momentum quadratures of Bob’s \(i\)-th noisy subcarrier Gaussian CV, \(|\phi'_j\rangle = x'_j + ip'_j\). |
| \(x_j, p_j\)   | Position and momentum quadratures of the \(j\)-th Gaussian single-carrier \(|\phi_j\rangle = x_j + ip_j\). |
| \(x'_j, p'_j\) | Noisy position and momentum quadratures of Bob’s \(j\)-th recovered single-carrier Gaussian CV \(|\phi'_j\rangle = x'_j + ip'_j\). |
| \(s_{\text{AMQD}} - p_{\text{AMQD}}\) | Alice’s quadratures in the transmission of the \(i\)-th subcarrier. |
| \(|\phi_j\rangle, | Transmitted and received Gaussian subcarriers. |
| \(|\phi_j\rangle, | \(\mathbf{z}\) \(\mathbf{z}^T\) \(\mathbf{M}\) \(\mathbf{S}\) \(\mathbf{R}(q)\) \(\mathbf{R}(q-1)\) \(\mathbf{P}(\mathcal{N}_i)\) \(\mathcal{Z}_{\text{AB}}(\mathcal{N}_i)\) \(\mathcal{Z}_{\text{BE}}(\mathcal{N}_i)\) \(\mathbf{S}^*(\mathcal{N})\) \(\mathbf{A}\) \(\mathbf{SNR}(\mathcal{R}(\mathcal{N}_i))\) \(\mathbf{SNR}(\mathcal{R}(\mathcal{N}_i))\) \(\mathbf{\delta}_i(\mathcal{R}(\mathcal{N}_i))\) \(\mathbf{\delta}_i(\mathcal{R}(\mathcal{N}_i))\) \(\mathbf{\delta}_i(\mathcal{R}(\mathcal{N}_i))\) \(\mathbf{\delta}_i(\mathcal{R}(\mathcal{N}_i))\) \(\mathbf{\delta}_i(\mathcal{R}(\mathcal{N}_i))\) \(\mathbf{\delta}_i(\mathcal{R}(\mathcal{N}_i))\) \(\mathbf{\delta}_i(\mathcal{R}(\mathcal{N}_i))\) \(\mathbf{\delta}_i(\mathcal{R}(\mathcal{N}_i))\) \(\mathbf{\delta}_i(\mathcal{R}(\mathcal{N}_i))\) \(\mathbf{\delta}_i(\mathcal{R}(\mathcal{N}_i))\) \(\mathbf{\delta}_i(\mathcal{R}(\mathcal{N}_i))\) \(\mathbf{\delta}_i(\mathcal{R}(\mathcal{N}_i))\) \(\mathbf{\delta}_i(\mathcal{R}(\mathcal{N}_i))\) \(\mathbf{\delta}_i(\mathcal{R}(\mathcal{N}_i))\) \(\mathbf{\delta}_i(\mathcal{R}(\mathcal{N}_i))\) |
| Notation | Description |
|----------|-------------|
| $\Delta_i$ | Difference of $v_i$ at $R(N_i)$ and $R(N_i')$, $R(N_i) > R(N_i') > 0$. |
| $\Delta_i = v_i(R(N_i)) - v_i(R(N_i'))$. | |
| $B$ | Bit error rate of $N_i$. At target rate $R(q)$ at a current rate $R(q-1)$, and $\delta_i(R(q-1))$, is expressed as $B(R(q)_{\delta_i(R(q-1))})$. |
| $\xi(R(q-1))$ | Identifies that $N_i$, $i = 0, \ldots, l-1$ from the total $l$, for which $\delta_i(R(q-1))$ is minimal at a given $R(q)$. $\xi(R(q-1)) = \min_i \delta_i(R(q-1))$. |
| $R(q)_{\delta_i(R(q-1))}$ | A target private rate $R(q)$ over $N_i$ at a current $\delta_i(R(q-1))$. |
| $B(R_{\min}(N_i))$ | Minimal bit error rate, achievable at $R_{\min}(N_i)$, at a given $\delta_i(R(q-1))$. |
| $\mathcal{F}(\cdot)$ | Function, evaluates SNR quantities from the input $v_i(\cdot)$ parameters, defined as $\mathcal{F}(v_i(N_i) + \Delta_i(R_{\min}(N_i), R(0)) + \cdots + \Delta_i(R(q-1), R(q)))$. |
| $\text{erfc}(\cdot)$ | Complementary error function, $\text{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-t^2} dt$. |
| $U_k$ | A $k$-th user, $k = 0, \ldots, K - 1$. |
| $\mathcal{M}_{U_i}$ | Logical channel of user $U_i$, $k = 0, \ldots, K - 1$, where $K$ is the number of total users, $\mathcal{M}_{U_i} = [N_{U_i,0}, \ldots, N_{U_i,m-1}]^T$. |
| $S^*(\mathcal{M}_{U_i})$ | Target secret key rate of $\mathcal{M}_{U_i}$. |
| $S^*(\mathcal{M}_{U_i}) = \sum_{m=0}^{m-1} R(N_{U_i,m})$. | where $R(N_{U_i,m})$ is the private rate of $N_{U_i,m}$. |
| $R(N_{U,i},j)$ | A current private rate of $N_{U,i,j}, R(N_{U,i,j}) = R(q-1)$. |
| $R(N_{U,i})$ | A target private rate of $N_{U,i}, R(N_{U,i}) = R(q)$ where $R_i(q)$ refers to the $R(q)$ rate of $N_{U,i}$, with relation $R_i(q-1) < R_i(q), R_i(q-1) = R_{\min}(N_{U,i}),$ and $R_i(q) = R_{\max}(N_{U,i})$. |
| $\delta_i(R(q))$ | Parameter $\delta_i$ of $N_{U,i}$ at private rate $R(N_{U,i})$. |
| $\tilde{\xi}_{U_i}$ | Identifies the minimal $\delta_i(R(N_{U,i}))$ parameter for the $N_{U,i}, i = 0, \ldots, m - 1$ subchannels of the set $\mathcal{M}_{U_i}$, as $\tilde{\xi}_{U_i} = \min_{i \in \mathcal{M}_{U_i}} \delta_i(R(N_{U,i}))$. |
| $\Delta_{\xi_{U_i}}$ | Modulation variance adaption at rate $R(N_{U,i})$. |
| $\Delta_{\xi_{U_i}} = \delta_i(R(N_{U,i})) - \tilde{\xi}_{U_i}$. | |
| $\tilde{\sigma}_0^2$ | A corrected modulation variance, $\tilde{\sigma}_0^2 = \sigma_0^2 + \Delta_{\xi_{U_i}}$, where $\sigma_0^2$ is the initial input subcarrier modulation variance, and $\Delta_{\xi_{U_i}} = \delta_i(R(N_{U,i})) - \tilde{\xi}_{U_i}$. |
| $\varphi_{\delta_i}(R(N_{U,i}))$ | The resulting $\delta_i$ parameter for $N_{U,i}$ at a target rate $R(N_{U,i}), \varphi_{\delta_i}(R(N_{U,i})) = \delta_i(R(N_{U,i})) - \tilde{\xi}_{U_i}$. |
| $\Delta_{\text{SNR}}(\varphi_{\delta_i}(R(N_{U,i})))$ | SNR increment of $N_{U,i}$, achieved by $\Delta_{\text{SNR}}$ at a given $R(N_{U,i}) = R(q)$. |
| $B\left(R(N_{U,i})\right)$ | An equally minimized bit error rate for all $N_{U,i}$ at an arbitrary $R(N_{U,i}) \delta_i \left(g(N_{U,i})\right)$. |
| $F$ | Fourier transform (FFT). |
### Table 1 (continued)

| Notation | Description |
|----------|-------------|
| \( \Psi_{U_k} \) | A \( d \)-dimensional input vector of user \( U_k \), \( k = 0, \ldots, K-1 \), \( \Psi_{U_k} = (\varphi_{U_k,0}, \ldots, \varphi_{U_k,d-1})^T \), where \( \varphi_{U_k,j} \) refers to the \( j \)-th single-carrier CV, \( \varphi_{U_k,j} = x_{U_k,j} + ip_{U_k,j} \) and \( \{ x_{U_k,j}, p_{U_k,j} \} \) are Gaussian random quadratures. |
| \( \mathbf{s}_{U_k} \) | A \( d \)-dimensional vector of \( U_k \), \( \mathbf{s}_{U_k} = (x_{U_k,0}, \ldots, x_{U_k,d-1})^T \), where \( x_{U_k,j} \) is the quadrature component of \( \varphi_{U_k,j} \). |
| \( \mathbf{x}'_{U_k,j} \) | Noisy subcarrier, discrete variable, \( \mathbf{x}'_{U_k,j} = M(\varphi'_{U_k,j}) \), where \( M \) is a measurement operator, and \( \varphi'_{U_k,j} \) is the \( j \)-th noisy Gaussian subcarrier CV of \( U_k \). |
| \( z \) | The variable of a single-carrier Gaussian CV state, \( |\varphi_0| \in \mathcal{S}, \ z \in \mathcal{C} \mathcal{N}(0, \sigma_z^2) \). Zero-mean, circular symmetric complex Gaussian random variable, \( \sigma_z^2 = \mathbb{E}[|z|^2] = 2\sigma_{m_0}^2 \) with i.i.d. zero mean, Gaussian random quadrature components \( x,p \in \mathcal{N}(0, \sigma_m^2) \), where \( \sigma_{m_0}^2 \) is the variance. |
| \( \Delta \) | The noise variable of the Gaussian channel \( \mathcal{N}, \Delta \in \mathcal{C} \mathcal{N}(0, \sigma_\Delta^2) \), with i.i.d. zeromean, Gaussian random noise components on the position and momentum quadratures \( \Delta_x, \Delta_p \in \mathcal{N}(0, \sigma_\Delta^2) \), \( \sigma_\Delta^2 = \mathbb{E}[|\Delta|^2] = 2\sigma_{m_0}^2 \). |
| \( d \) | The variable of a Gaussian subcarrier CV state, \( |\varphi_0| \in \mathcal{S}, \ d \in \mathcal{C} \mathcal{N}(0, \sigma_d^2) \). Zero-mean, circular symmetric Gaussian random variable, \( \sigma_d^2 = \mathbb{E}[|d|^2] = 2\sigma_d^2 \), with i.i.d. zero mean, Gaussian random quadrature components \( x_d,p_d \in \mathcal{N}(0, \sigma_d^2) \), where \( \sigma_d^2 \) is the (constant) modulation variance of the Gaussian subcarrier CV state. |
| \( F^{-1}(\cdot) \) | The inverse CVQFT transformation, \( F^{-1}(\cdot) = \text{CVQFT}^{\dagger}(\cdot) \), applied by the encoder, continuous-variable unitary operation. |
| \( F(\cdot) \) | The CVQFT transformation, \( F(\cdot) = \text{CVQFT}(\cdot) \), applied by the decoder, continuous-variable unitary operation. |
| \( F^{-1}(\cdot) \) | Inverse FFT transform, \( F^{-1}(\cdot) = \text{IFFT}(\cdot) \), applied by the encoder. |
| \( \sigma_{m_0}^2 \) | Single-carrier modulation variance. |
| \( \sigma_{m_0}^2 \) | Multicarrier modulation variance, \( \sigma_{m_0}^2 = \frac{1}{\mathcal{N}} \sum_{i} \sigma_{m_0}^2 \). Average modulation variance of the \( \mathcal{N} \) Gaussian sub-channels \( \mathcal{N}_c \). |
| \( |\varphi_{i,k}| \) | The decoded single-carrier CV of user \( U_k \) from the subcarrier CV, \( |\varphi_{i,k}| = \text{CVQFT}(|\varphi_i|) \), expressed as \( F(|d_i|) = \left| F\left( F^{-1}(z_{i,k}) \right) \right| = \left| z_{i,k} \right| \). |
| \( \mathcal{N} \) | Gaussian quantum channel. |
| \( \mathcal{N}_c \) | An \( i \)-th Gaussian sub-channel, \( \mathcal{N}_c, i = 0, \ldots, n-1 \). |
| \( T_i(N) \) | Channel transmittance, normalized complex random variable, \( T_i(N) = \text{Re}T_i(N) + i\text{Im}T_i(N) \in \mathbb{C} \). The real part identifies the position quadrature transmission, the imaginary part identifies the transmittance of the position quadrature. |
| \( T_i(N) \) | Transmittance coefficient of Gaussian subchannel \( \mathcal{N}_c, T_i(N) = \text{Re}(T_i(N)) + i\text{Im}(T_i(N)) \in \mathbb{C} \), quantifies the position and momentum quadrature transmission, with (normalized) real and imaginary parts \( 0 \leq \text{Re}T_i(N) \leq 1/\sqrt{2} \), \( 0 \leq \text{Im}T_i(N) \leq 1/\sqrt{2} \), where \( \text{Re}T_i(N) = 1/\text{Im}T_i(N) \). |
| \( T_{Eve} \) | Eve’s transmittance, \( T_{Eve} = 1 - T(N) \). |
| \( T_{Eve,i} \) | Eve’s transmittance for the \( i \)-th subcarrier CV. |
| \( z \) | A \( d \)-dimensional, zero-mean, circular symmetric complex random Gaussian vector, \( z = x + ip = (z_0, \ldots, z_{d-1})^T \), that models \( d \) Gaussian CV input states, \( \mathcal{C} \mathcal{N}(0, \mathbf{K}_z), \mathbf{K}_z = \mathbb{E}[zz^H] \) where \( z_j = x_j + ip_j, x_j = (x_0, \ldots, x_{d-1})^T \). |
| \( d \) | An \( l \)-dimensional, zero-mean, circular symmetric complex random Gaussian vector, \( d = (d_0, \ldots, d_{l-1})^T \), \( d_i = x_i + ip_i, x_i, p_i \in \mathcal{N}(0, \sigma_{m_0}^2) \) i.i.d. zero-mean Gaussian random variables. |
| \( y_k \) | A \( d \)-dimensional zero-mean, circular symmetric complex Gaussian random vector, \( y_k = \mathcal{C} \mathcal{N}(0, \mathbb{E}[yy^H]) \). |
| \( y_{k,m} \) | The \( m \)-th element of the \( k \)-th user’s vector \( y_k \), expressed as \( y_{k,m} = \sum_j F(T_i(N_j))F(d_i) + F(\Delta_i) \). |
Fourier transform of $\mathbf{T}(\mathcal{N}) = \left[ T_0(\mathcal{N}_0), \ldots, T_{N-1}(\mathcal{N}_{N-1}) \right]^\dagger \in \mathbb{C}^l$, the complex transmittance vector.

$F(\Delta)$

Complex vector, expressed as $F(\Delta) = e^{-i\langle \Delta \mathcal{N}_0 \rangle} \mathbf{K}_{\mathcal{N}_0} F(\mathcal{N})$, with covariance matrix $\mathbf{K}_{\mathcal{N}_0} = \mathbb{E}[ F(\mathcal{N}) F(\mathcal{N})^\dagger ]$.

$y[\vec{\mathbf{d}}]$ AMQD block, $y[\vec{\mathbf{d}}] = F(\mathbf{T}(\mathcal{N})) F(\mathbf{d}) \langle \vec{\mathbf{d}} \rangle + F(\mathcal{N}) \langle \vec{\mathbf{d}} \rangle$.

$\tau$ An exponentially distributed variable, $\tau = \left\| F(\mathbf{d}) \right\|^2$ with density $f(\tau) = (1/2\tau^2)e^{-\tau/2\sigma_i^2}$, $\mathbb{E}[\tau] \leq n\sigma_i^2$.

$T_{\text{Eve}}$ Eve’s transmittance on the Gaussian sub-channel $\mathcal{N}_i$, $T_{\text{Eve}} = \text{Re} T_{\text{Eve}} + i\text{Im} T_{\text{Eve}} \in \mathbb{C}$, $0 \leq \text{Re} T_{\text{Eve}} \leq 1/\sqrt{2}$, $0 \leq \text{Im} T_{\text{Eve}} \leq 1/\sqrt{2}$, $0 \leq |T_{\text{Eve}}|^2 < 1$.

$d_i$ A $d_i$ subcarrier in an AMQD block.

$v_{\text{min}}$ The min $\{ v_i, \ldots, v_{i-1} \}$ minimum of the $v_i$ sub-channel coefficients, where $v_i = \sigma_i^2 \left\| F(T_i(N_i)) \right\|^2$ and $v_i < v_{\text{Eve}}$.

$\sigma_i^2$ Constant modulation variance, $\sigma_i^2 = v_{\text{Eve}} - v_{\text{min}} \mathbb{G}(6) / n$, $v_{\text{Eve}} = 1/2 \lambda \left( F(T_i(N_i)) \right)^2 = 1/n \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} T_{i}^k e^{-2\pi ik/\nu} \right\|^2$ and $T_{i}^k$ is the expected transmittance of the Gaussian sub-channels under an optimal Gaussian collective attack.

---

**References**

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

2. Gyongyosi L, Imre S. A survey on quantum channel capacities. IEEE Commun Surv Tut. 2018;99:1. https://doi.org/10.1109/COMST.2017.2786748.

3. Biamonte J, et al. Quantum machine learning. Nature. 2017;549:195–202.

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

5. Grosshans F. Collective attacks and unconditional security in continuous variable quantum key distribution. Phys Rev Lett. 2005;94:2004.

6. Grosshans F, Cerf NJ, Wenger J, Tualle-Brouri R, Grangier P. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. Quant Inf Comput. 2003;3:535–52.

7. Pirandola S, Laurenza R, Ottaviani C, Banchi L. Theory of channel simulation and bounds for private communication. Quantum Sci Technol. 2018;3:35009. https://doi.org/10.1088/2058-9565/aac394.

8. Pirandola S, Laurenza R, Ottaviani C, Cope TPW, Spedalieri G, Banchi L. Fundamental limits of repeaterless quantum communications. Nat Commun. 2017;8:15043. https://doi.org/10.1038/ncomms15043.

9. Pirandola S, Laurenza R, Ottaviani C, Cope TPW, Spedalieri G, Banchi L. Fundamental limits of repeaterless quantum communications. Nat Commun. 2017;8:15043. https://doi.org/10.1038/ncomms15043.

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

11. Pirandola S, Braunstein SL, Lloyd S. Characterization of collective gaussian attacks and security of coherent-state quantum cryptography. Phys Rev Lett. 2008;101:200504.

12. Pirandola S, Garcia-Patron R, Braunstein SL, Lloyd S. Direct and reverse secret-key capacities of a quantum channel. Phys Rev Lett. 2009;102:50503.

13. Pirandola S, Mancini S, Lloyd S, Braunstein SL. Continuous-variable quantum cryptography using two-way quantum communication. Nat Phys. 2008;4:726–30.

14. Pirandola S, Serafini A, Lloyd S. Correlation matrices of two-mode bosonic systems. Phys Rev A. 2009;79:52327.

15. Gyongyosi L, Imre S. Adaptive multicarrier quadrature division modulation for long-distance continuous-variable quantum key distribution. In: Proc. SPIE 9123 Quantum Information and Computation XII, “912307,” from Conference Volume 9123 Quantum Information and Computation XII, Baltimore, Maryland, USA 2014. https://doi.org/10.1117/12.2050095.

16. Gyongyosi L, Imre S. Diversity space of multicarrier continuous-variable quantum key distribution. Int J Commun Syst. 2019. https://doi.org/10.1002/dac.4003.

17. Gyongyosi L, Imre S. Gaussian quadrature inference for multicarrier continuous-variable quantum key distribution. Quantum Stud Math Found. 2019. https://doi.org/10.1007/s40509-019-00183-9.

18. Gyongyosi L, Imre S. Statistical quadrature evolution by inference for multicarrier continuous-variable quantum key distribution. Quantum Stud Math Found. 2019. https://doi.org/10.1007/s40509-019-00202-9.

19. Gyongyosi L, Imre S. Geometrical analysis of physically allowed quantum cloning transformations for quantum cryptography. Inf Sci. 2014;285:1–23. https://doi.org/10.1016/j.ins.2014.07.010.

20. Gyongyosi L, Imre S. Multiple access multicarrier continuous-variable quantum key distribution. Chaos, Solitons Fractals. 2018;114:491–505. https://doi.org/10.1016/j.chaos.2018.07.006.

21. Gyongyosi L, Imre S. Secret key rate proof of multicarrier continuous-variable quantum key distribution. Int J Commun Syst. 2018. https://doi.org/10.1002/dac.3865.

22. Gyongyosi L. Singular value decomposition assisted multicarrier continuous-variable quantum key distribution. Theor Comput Sci. 2019. https://doi.org/10.1016/j.tcs.2019.07.029.

23. Gyongyosi L, Imre S. Secret key rates of free-space optical continuous-variable quantum key distribution. Int J Commun Syst. 2019. https://doi.org/10.1002/dac.4152.

24. Gyongyosi L, Imre S. Proceedings volume 8997 advances in photonics of quantum computing, memory, and communication “VII; “89970C;”. 2014. https://doi.org/10.1117/12.2038532.

25. Gyongyosi L, Imre S. Long-distance continuous-variable quantum key distribution with advanced reconciliation of a gaussian modulation. In: Proceedings of SPIE Photonics West OPTO. 2013; 2013.
26. Gyongyosi L, Imre S. Low-dimensional reconciliation for continuous-variable quantum key distribution. Appl Sci. 2018. https://doi.org/10.3390/app8010087 (ISSN 2076-3417).

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

28. Gyongyosi L, Imre S. Eigenchannel decomposition for continuous-variable quantum key distribution. In: Proceedings Volume 9377 advances in photonics of quantum computing, memory, and communication “VIII,” 937711. 2015. https://doi.org/10.1117/12.2076532.

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

30. Gyongyosi L, Imre S. Adaptive Gaussian quadrature detection for continuous-variable quantum key distribution. In: SPIE advances in photonics of quantum computing memory and communication IX, 2016.

31. Gyongyosi L, Imre S. Gaussian quadrature inference for multicharrier continuous-variable quantum key distribution. In: SPIE quantum information and computation XIV, 17–21 Apr 2016 Baltimore, Maryland, USA, 2016.

32. Gyongyosi L, Bacsardi L, Imre S. A survey on quantum key distribution. Infocommun J. 2019;XI(2):14–21.

33. Heinzel G, Rudiger A, Schilling R. Spectrum and spectral density estimation by the discrete Fourier transform (DFT), including a comprehensive list of window functions and some new at-top windows. 2002. http://hdl.handle.net/11858/00-001M-0000-0013-557A-5.

34. Imre S, Gyongyosi L. Advanced quantum communications—an engineering approach. New Jersey: Wiley-IEEE Press; 2012 (ISBN-10: 1118002369 ISBN-13: 978-11180023).

35. Imre S, Balazs F. Quantum computing and communications—an engineering approach. New Jersey: Wiley-IEEE Press; 2012 (ISBN-10: 1118002369 ISBN-13: 978-11180023).

36. Imre S, Gyongyosi L. Decentralized base-graph routing for the quantum internet. Sci Rep Nat. 2018. https://doi.org/10.1038/s41598-018-2147-8.

37. Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P, Diamanti E. Experimental demonstration of long-distance continuous-variable quantum key distribution. In: SPIE Proceedings Volume 9377 advances in photonics of quantum computing, memory, and communication “VIII,” 937711. 2015. https://doi.org/10.1117/12.2076532.

38. Kimble HJ. The quantum Internet. Nature. 2008;453:1023–30.

39. Kiktenko EO, Pozhar NO, Anufriev MN, Trushechkin AS, Yunusov RR, Kurochkin YV, Lvovsky AI, Fedorov AK. Quantum-noise-tolerant continuous-variable quantum key distribution. Phys Rev Lett. 2008;107:220501.

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