

Continuous-variable Measurement Device Independent MIMO Quantum Key Distribution for THz Communications

Leixin Wu, Congtian Deng, Jiayu Pan, Lingtao Zhang, Yanyan Feng, Runbo Zhao, Yang Shen, Yuying Zhang, Jian Zhou

Abstract—Although multiple-input multiple-output (MIMO) terahertz (THz) continuous-variable quantum key distribution (CVQKD) is theoretically secure, practical vulnerabilities may arise due to detector imperfections. This paper explores a CV measurement-device-independent (MDI) QKD system operating at THz frequencies within a MIMO framework. In this system, measurement is delegated to an untrusted third party, Charlie, rather than the receiver, eliminating all detector attacks and significantly enhancing the system's practical security. Using transmit-receive beamforming techniques, the system transforms MIMO channels into multiple parallel lossy quantum channels, enabling robust key distribution between Alice and Bob. This study examines entanglement-based and prepare-and-measure protocols, deriving secret key rates for both asymptotic and finite code scenarios. Simulations reveal the critical role of multiple antenna configurations and efficient homodyne detection in mitigating free-space path loss and maximizing key rates. Results indicate that system performance is optimized at lower THz frequencies for long-range transmissions and higher frequencies for short-range applications. The proposed protocol offers a scalable solution for secure quantum communications in next-generation wireless networks, demonstrating potential for deployment in both indoor and outdoor environments.

Index Terms—B5G and 6G communications, Multiple-input multiple-output, Continuous-variable quantum key distribution, Measurement device independent, Finite code analysis, Terahertz wave, Indoor and outdoor wireless communications

I. INTRODUCTION

The research was funded by the National Natural Science Foundation of China grant numbers 62201620, 62272483 and 62402435, the Science Fund for Distinguished Young Scholars of Hunan Province grant number 2023JJ10078, the Young Fund of the Natural Science Foundation of Hunan Province grant number 2023JJ41059, the Scientific research startup fund project of introduced talents of Central South University of Forestry and Technology grant number 2021YJ0050, the Ningbo Yongjiang Talent Programme grant number 2023A-398-G and Natural Science Foundation of Ningbo grant number 2024J205.

(Corresponding authors: Lingtao Zhang)

Leixin Wu, Lingtao Zhang, Yanyan Feng and Yang Shen are with College of Electronic Information and Physics, Central South University of Forestry and Technology, Changsha 410004, PR China (e-mail: 874067703@qq.com; zhang@csuft.edu.cn; fengyanyanhenu@163.com; 2632804120@qq.com).

Congtian Deng is with James Watt School of Engineering, University of Glasgow, Glasgow G12 8QQ, UK (e-mail: timd56541@gmail.com).

Jiayu Pan is with the School of Software Technology, Zhejiang University, Ningbo 315100, PR China (e-mail: jiayupan26@zju.edu.cn)

Runbo Zhao, Yuying Zhang and Jian Zhou are with College of Computer and Mathematics, Central South University of Forestry and Technology, Changsha 410004, PR China (e-mail: 1538038647@qq.com; 3118454087@qq.com; 13142153489@163.com).

The fifth generation of mobile communication technology (5G) has now been extensively adopted in a variety of applications, prompting researchers to investigate new cases and solutions for beyond 5G (B5G) and 6G systems [1], [2], [3], [4], [5]. The objective of these next-generation technologies is to achieve higher data transmission rates and lower latency compared to 5G [6], [7], [8]. The overarching objective is to facilitate the interconnectivity of multiple devices, enable real-time end-to-end communications and support advanced artificial intelligence applications [3], [4], [5], [6], [7], [8], [9], [10].

In this context, THz frequencies have emerged as a key enabler for short-range, high-capacity wireless links envisioned in 6G networks [11], [12]. While current systems predominantly operate in the microwave bands, the THz spectrum offers several compelling advantages—such as ultra-wide bandwidth, terabit-per-second data rates, and high spatial resolution—making it particularly well-suited for 6G communication scenarios, including ultra-fast wireless access, high-capacity backhaul, and secure device-to-device communication in dense urban or indoor environments [13], [14], [15]. However, the deployment of THz communication systems faces critical challenges, notably high path loss and molecular absorption. These impairments significantly degrade signal quality over distance, making channel estimation and detection more susceptible to eavesdropping and tampering [16], [17].

Quantum key distribution (QKD) provides a method for securely generating encryption keys between two users, with its security based on the principles of quantum physics [18], [19], [20]. QKD has been demonstrated its ability to directly implement encryption for communication in 6G networks, including the one-time-pad [21], [22]. QKD is categorized into discrete-variable (DV) QKD and continuous-variable (CV) QKD [23], [24], [25]. DVQKD primarily encodes information through the polarization or phase of single-photon pulses and has found extensive application in areas such as national defense and satellite communications [26], [27], while CVQKD systems are rapidly moving from the laboratory stage to field applications and prototype development [28], [29]. These systems are compatible with existing telecommunications technology and can employ multiplexing to enhance key rates, positioning them favorably for short-range wireless networks [25], [29].

However, many current QKD implementations rely on optical frequencies for point-to-point communications, for which precise positioning and tracking are required. This approach

does not meet the mobility demands of B5G and 6G communication applications [30], [31]. A newly proposed THz CVQKD system for mobile devices addresses these challenges [32], [33]. Unlike optical links, THz waves does not require meticulous alignment and can generate stable keys even in adverse weather conditions, such as fog and dust, ensuring reliable internet access in extreme environments [32].

Recently, Kundu et al. have proposed a multiple-input multiple-output (MIMO) CVQKD scheme designed for the THz frequency band [34]. This scheme employs transmit-receive beamforming techniques to transform the MIMO channel into parallel lossy quantum channels, improving both the secret key rate and the effective transmission distance compared to traditional single-antenna QKD schemes [34], [35]. Furthermore, they have proposed a least-squares-based channel estimation method to improve the security and efficiency of these systems [35]. The input-output relationship between Alice and Bob during the key generation phase has been analyzed, while accounting for the additional noise introduced by channel estimation errors and detector noise [35]. Additionally, to further improve the security of the MIMO QKD protocol, eavesdropping restrictions are also discussed [36].

Building upon these advancements, a reconfigurable intelligent surface (RIS)-based wireless communication system has been proposed to further enhance the MIMO CVQKD system [37]. In this setup, communication occurs via two paths: a direct path between Alice and Bob and a wireless path facilitated by the RIS [37]. Simulations show that the RIS plays a crucial role in improving both the secret key rate and the transmission distance, particularly by ensuring secure communication in scenarios where Eve attempts to measure the additional modes in the RIS-Bob channel. A comprehensive analysis of the associated channel estimation and secret key rate for the RIS is presented in [38], underscoring its potential to substantially enhance the performance of MIMO-based CVQKD systems.

In parallel, Liu et al. have recently investigated orthogonal frequency division multiplexing (OFDM) and orthogonal time frequency space (OTFS) based CVQKD systems operating over doubly selective THz fading channels, which are representative of high-mobility scenarios [39]. Their work introduces a multi-carrier framework integrated with low-density parity-check (LDPC) codes and a modified multi-dimensional reconciliation algorithm, demonstrating that OTFS-based MIMO CVQKD can effectively mitigate the Doppler-induced inter-carrier interference and outperform its OFDM counterpart in mobile wireless environments. It highlight the importance of jointly considering advanced waveform design, powerful reconciliation algorithms, and MIMO techniques for enabling practical THz CVQKD under realistic wireless conditions.

Despite the potential advantages of MIMO THz QKD, several practical challenges remain. First, atmospheric absorption in the THz frequency band, mainly caused by water vapor, imposes a major limitation on the system of achievable secret key rate per channel use [34]. Second, imperfections in current detection devices render the system susceptible to detector-side eavesdropping attacks [40]. To address these challenges, we propose a CV measurement-device-independent (MDI) MIMO THz QKD scheme. In this approach, an untrusted third party is

introduced to perform the necessary measurements, allowing two users to establish secret keys without relying on their own detection devices. Consequently, the MDI technique provides resilience against potential attacks targeting the detector-side channels. The effectiveness of MDI QKD has been demonstrated in conventional optical fiber networks [40], [41], [42] and its potential for strengthening 6G communications over atmospheric channels is particularly promising. Furthermore, the proposed scheme offers strong potential for enabling high-speed and secure wireless communication in both indoor and outdoor environments. The main contributions of this work are summarized as follows:

- 1) We propose a MDI MIMO CVQKD approach to improve the THz QKD system based on an transmit-receive beamforming scheme using singular value decomposition. A transmit-receive beamforming technique is employed by Alice, Bob and Charlie to transform the MIMO channels into multiplexed SISO channels.
- 2) We describe the communication procedures of the MDI MIMO QKD protocol, including the details of the prepare-and-measure (PM) and entanglement-based (EB) protocols. In addition, we analyze the influence of Gaussian collective attacks on the MIMO channel.
- 3) We derive the asymptotic and finite code key rates for the proposed CVMDI QKD protocol with reverse reconciliation (RR). The asymptotic analysis is performed under the assumption of infinite data block size, which provides an upper bound on the achievable secret key rate. For finite code analysis, the maximum likelihood estimation (MLE) [43], [44], [45] is employed instead of the least-squares method used in [35]. In the MLE method, critical steps such as privacy amplification and channel estimation are considered, which are integral to the practical implementation of the MDI MIMO CVQKD protocol. The key parameters are estimated based on block size, resulting in more accurate parameter estimation. This approach has been widely adopted in different CVQKD systems [46], [47], [48].
- 4) Through extensive simulations, we evaluate the performance of the MIMO QKD scheme against a baseline single-input single-output (SISO) scheme. We also investigate the maximum transmission distance for the proposed protocol with different MIMO configurations in the range of 0.1-1 THz and explore the effect of the homodyne detection efficiency on the SISO and MIMO protocol. Moreover, we compare the secret key rate and maximum transmission distance of the proposed protocol with the other MIMO QKD schemes and identify the frequency intervals over which a positive key rate can be maintained.

Notation: $\mathbf{V}^\dagger$ is the conjugate transpose of $\mathbf{V}$, $\mathbf{0}_{A \times B}$ is an $A \times B$ all-zero matrix, $\mathcal{N}(A, B)$ is a Gaussian distribution with mean A and variance B , χ^2 is a chi-square distribution, $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ are Pauli matrices, $N_{T_{A,B}}$ indicates that Alice and Bob have the same transmitter antenna node and $N_{R_{A,B}}$ indicates that Alice and Bob have the same receiver

antenna node.

II. SYSTEM MODEL

A. Channel model

In MDI MIMO protocol, Alice and Bob communicate with Charlie through a MIMO THz wireless channel, where Alice and Bob are equipped with N_{TA} and N_{TB} transmitter antenna nodes and Charlie captures the THz waves transmitted by Alice and Bob with N_{RA} and N_{RB} receiver antenna nodes respectively. In this paper, we assume that Charlie's two antenna arrays are sufficiently separated in space to ensure negligible inter-array interference. The corresponding MIMO THz channel matrix $\mathbf{H}_A \in \mathbb{C}^{N_{RA} \times N_{TA}}$ and $\mathbf{H}_B \in \mathbb{C}^{N_{RB} \times N_{TB}}$ can be obtained by [34], [49]

$$\begin{aligned} \mathbf{H}_A &= \sum_{l=1}^{L_A} \sqrt{\gamma_{A_l}} e^{j2\pi f_c \tau_l} \psi_{N_{RA}}(\phi_l^{RA}) \psi_{N_{TA}}^\dagger(\phi_l^{TA}), \\ \mathbf{H}_B &= \sum_{l=1}^{L_B} \sqrt{\gamma_{B_l}} e^{j2\pi f_c \tau_l} \psi_{N_{RB}}(\phi_l^{RB}) \psi_{N_{TB}}^\dagger(\phi_l^{TB}). \end{aligned} \quad (1)$$

where $\psi_{N_{RA}}$ and $\psi_{N_{RB}}$, which express the array response vector of uniform linear array, are formulated as [34]

$$\begin{aligned} \psi_{N_{RA}}(\theta) &= \frac{1}{\sqrt{N_{RA}}} \left[1, e^{j\frac{2\pi}{\lambda} d_a \sin \theta}, \dots, e^{j\frac{2\pi}{\lambda} d_a (N_{RA}-1) \sin \theta} \right]^T, \\ \psi_{N_{RB}}(\theta) &= \frac{1}{\sqrt{N_{RB}}} \left[1, e^{j\frac{2\pi}{\lambda} d_a \sin \theta}, \dots, e^{j\frac{2\pi}{\lambda} d_a (N_{RB}-1) \sin \theta} \right]^T, \end{aligned} \quad (2)$$

where d_a is inter-antenna spacing, L_A and L_B are multipath components, γ_{A_l} and γ_{B_l} are the path losses of the l -th multipath between Alice, Bob and Charlie. When antenna element G_a is set to 30 and Rayleigh roughness factor is set to 1, the path losses γ_{A_l} and γ_{B_l} for line-of-sight (LOS) and non-LOS (NLOS) component can be modeled by [21]

$$\begin{aligned} \gamma_{A_l} &= 900 N_{RA} N_{TA} \left(\frac{\lambda}{4\pi d_{AC}} \right)^2 10^{-\frac{\delta_1 d_{AC}}{10}}, \\ \gamma_{B_l} &= 900 N_{RB} N_{TB} \left(\frac{\lambda}{4\pi d_{BC}} \right)^2 10^{-\frac{\delta_2 d_{BC}}{10}}. \end{aligned} \quad (3)$$

where d_{AC} and d_{BC} are the shortest transmission distance between the senders and receiver, the $\delta_{1,2}$ are free-space path loss per kilometer, whose value is related to the transmission frequency f_c . The wavelength signal λ is inversely proportional to the transmission frequency f_c . Definitions of other parameters not directly relevant to this work can be found in [35]. In the singular-value decomposition scheme, the channel matrixs are denoted as [36]

$$\begin{aligned} \mathbf{H}_A &= \mathbf{U}_A \Sigma_A \mathbf{V}_A^\dagger, \\ \mathbf{H}_B &= \mathbf{U}_B \Sigma_B \mathbf{V}_B^\dagger. \end{aligned} \quad (4)$$

where $\mathbf{U}_A \in \mathbb{C}^{N_{RA} \times N_{RA}}$, $\mathbf{U}_B \in \mathbb{C}^{N_{RB} \times N_{RB}}$, $\mathbf{V}_A \in \mathbb{C}^{N_{TA} \times N_{TA}}$ and $\mathbf{V}_B \in \mathbb{C}^{N_{TB} \times N_{TB}}$ are unitary matrices and the associated matrixs Σ_A and Σ_B are formulated as [41]

$$\begin{aligned} \Sigma_A &= \begin{bmatrix} \text{diag} \left\{ \sqrt{T_{A_1}}, \dots, \sqrt{T_{A_{r_1}}} \right\} & \mathbf{0}_{r_1 \times (N_{TA}-r_1)} \\ \mathbf{0}_{(N_{RA}-r_1) \times r_1} & \mathbf{0}_{(N_{RA}-r_1) \times (N_{TA}-r_1)} \end{bmatrix}, \\ \Sigma_B &= \begin{bmatrix} \text{diag} \left\{ \sqrt{T_{B_1}}, \dots, \sqrt{T_{B_{r_2}}} \right\} & \mathbf{0}_{r_2 \times (N_{TB}-r_2)} \\ \mathbf{0}_{(N_{RB}-r_2) \times r_2} & \mathbf{0}_{(N_{RB}-r_2) \times (N_{TB}-r_2)} \end{bmatrix}. \end{aligned} \quad (5)$$

where r_1 and r_2 are the rank of the MIMO channel matrixs $\mathbf{H}_A$ and $\mathbf{H}_B$, and $\sqrt{T_{A_x}} (x = 1, 2, \dots, r_1)$ and $\sqrt{T_{B_y}} (y = 1, 2, \dots, r_2)$ are the i -th nonzero singular value of the matrix.

B. Prepare-and-measure scheme

The CVMDI MIMO protocol can be interpreted from two complementary perspectives. To explore the impact of MIMO antenna technology within the MDI framework, we first present the PM model, as illustrated in Figure 1. This model emphasizes the practical implementation of the protocol. In addition, we also present the EB equivalent model in the next section. These two representations are operationally equivalent and jointly provide a comprehensive understanding of the protocol. The corresponding steps of the PM scheme are as follows:

- *Step 1:* Alice and Bob each select $r = \min(r_1, r_2)$ random sequences $\{x_{A_i}, p_{A_i}\}$ ($i = 1, 2, \dots, r$) and $\{x_{B_i}, p_{B_i}\}$ from Gaussian distribution. They then prepare the corresponding r coherent states $|x_{A_i} + ip_{A_i}\rangle$ and $|x_{B_i} + ip_{B_i}\rangle$, which are transmitted using transmit beamforming techniques through THz waves from N_{TA} and N_{TB} transmitter antenna nodes to N_{RA} and N_{RB} receiver antenna nodes, respectively. The transmission of the THz wireless channel and the noise variance are T_{A_i}, T_{B_i} and W_{A_i}, W_{B_i} respectively.
- *Step 2:* Charlie employs receive beamforming to collect the $2r$ coherent states transmitted by Alice and Bob and subsequently performs Bell state measurement on the combined signals, producing $2r$ output modes. The homodyne detection is used to measure the x -quadrature of Alice's mode and the p -quadrature of Bob's mode. The corresponding measurement outcomes, denoted by X_{C_i} and P_{D_i} , are subsequently forwarded to Alice's and Bob's transmitter nodes for further processing [41].
- *Step 3:* After receiving the measurement results published by Charlie, Bob corrects his data: $X_{B_i} = g_i X_{C_i} + x_{B_i}$, $P_{B_i} = g_i P_{D_i} - p_{B_i}$ [40], while Alice retains her original data $\{x_A, p_A\}$, where g_i is the gain of the displacement operation. Once Bob completes the data correction, entanglement swapping between Alice and Bob is effectively accomplished with the assistance of Charlie, resulting in strong correlations between their respective data.
- *Step 4:* Alice randomly selects portions of the retained data for parameter estimation and publishes them over a trusted channel. Bob uses this data to estimate parameters such as channel transmission, modulation variance and noise variance. He then evaluates the secret key rate. If the secret key rate is less than zero, they will terminate the session and initiate a restart of the key distribution.
- *Step 5:* Alice and Bob perform post-processing, including data reconciliation and privacy amplification, to obtain the final secret key rate. There are two methods for data reconciliation: direct reconciliation (DR) and RR [50]. Previous studies have shown that the DR scheme can only support short-distance QKD, so this paper focuses exclusively on the RR scheme [51].

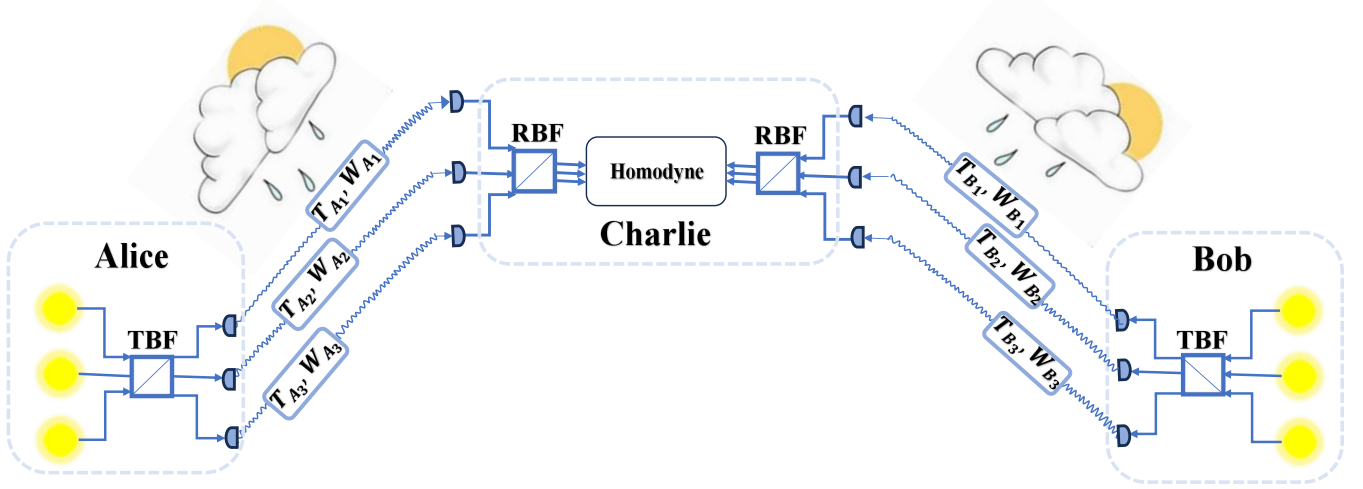


Fig. 1. Schematic diagram of CVMDI protocol of the 3×3 MIMO configuration with the PM scheme where Alice and Bob's transmitter antenna nodes are connected to Charlie's receiver antenna nodes via the free space channel with the transmission of the THz wireless channel T_{A_i}, T_{B_i} and the noise variance W_{A_i}, W_{B_i} . Alice (Bob) and Charlie employ transmit-receive beamforming techniques to decompose the original MIMO channel into multiple parallel SISO channels. The TBF and RBF are transmit and receive beamforming, respectively.

Alice and Bob employ orthogonal quadratures to achieve optimal entanglement swapping, thereby ensuring a strong correlation between Alice's retained data and the corrected data obtained after Bob's displacement operation [40]. Moreover, the MDI MIMO protocol delegates the measurement to an untrusted third party instead of the receiver, effectively preventing detector-side attacks. As a result, the protocol remains secure with imperfect detectors.

C. Gaussian collective attacks

In quantum communication, third-party eavesdroppers can attack quantum channels during transmission. Three main types of attacks are recognized: Gaussian individual attack, Gaussian collective attack and Gaussian coherent attack. In this paper, only the collective attack is discussed. According to quantum mechanics, Gaussian collective attacks are the most effective threat to CVQKD with standard RR protocols [50]. Considering the CVQKD protocol under Gaussian collective attack can evaluate the security of the protocol. To illustrate the effect of Gaussian collective attacks, the 2×2 MIMO channels are used as an example. Based on Ref. [35], the conclusion reached in the 2×2 model can be extended to the $N_{R,A,B} \times N_{T,A,B}$ MIMO model. Alice and Bob's two transmitted modes are first combined through a beam splitter. For the sake of simplicity, we assume that Alice and Bob transmit signals from the j -th transmitter node directly to Charlie's j -th receiver node. The input-output relationship for the j -th beam splitter is defined as follows: [36]

$$\begin{bmatrix} \hat{s}_{\text{out},A(B)_1} \\ \hat{s}_{\text{out},A(B)_2} \end{bmatrix} = \mathbf{B}_{T_{A(B)}} \begin{bmatrix} \hat{s}_{\text{in},A(B)_1} \\ \hat{s}_{\text{in},A(B)_2} \end{bmatrix}, \quad (6)$$

where the matrix of the beam-splitter are [52]

$$\mathbf{B}_{T_{A(B)}} = \begin{bmatrix} \sqrt{T_{A(B)}} & \sqrt{1-T_{A(B)}} \\ -\sqrt{1-T_{A(B)}} & \sqrt{T_{A(B)}} \end{bmatrix}. \quad (7)$$

Eve prepares 4 auxiliary states consisting of EPR pairs with variance $W_{A(B)_j}$, and $j = 1, 2$, denoted as $\{e_{A_j}, E_{A_j}\}$ and

$\{e_{B_j}, E_{B_j}\}$, where the E_{A_j} and E_{B_j} are stored in the quantum memory, and the other modes e_{A_j} and e_{B_j} are mixed by the splitter and sent to Charlie. Following the announcement of the relevant information by Alice and Bob via a classical communication channel, Eve retrieves the output modes $\hat{e}_{A_j}$ and $\hat{e}_{B_j}$ and stores them in the quantum memory. Finally, Eve measures the auxiliary modes in the quantum memory, $\{\hat{e}_{A_j}, E_{A_j}\}$ and $\{\hat{e}_{B_j}, E_{B_j}\}$, to extract valuable information. This combined strategy enables the optimization of the amount of information acquired during the transmission process.

III. SECURITY ANALYSIS

A. Entanglement-based scheme

In the process of deriving the cryptographic key, an EB model is commonly used, which is equivalent to the PM model. Specifically:

- *Step 1:* Alice and Bob each prepare r two-mode squeezed vacuum (TMSV) states. Each TMSV state is then split into two modes using a 50:50 beam splitter. The modes A_i and B_i are retained locally by Alice and Bob, while the corresponding other modes A'_i and B'_i are transmitted to an untrusted third party, Charlie, via a MIMO channel employing transmit beamforming at the sender sides of Alice and Bob. The variances of the two-mode squeezed states are defined as follows: for Alice's mode, $V_{A_i} = V_{AM_i} + V_{AO_i}$ ($i = 1, 2, \dots, r$); for Bob's mode, $V_{B_i} = V_{BM_i} + V_{BO_i}$. The thermal noise variance is $V_{A(B)_i} = 2\bar{n} + 1$ and $\bar{n} = \frac{1}{\exp(hf_c/k_B T_k) - 1}$ [53], [54], the T_k is the atmospheric temperature and the h and k_B are the Planck and Boltzmann constants, respectively.
- *Step 2:* Charlie employs receive beamforming to coherently combine the incoming signals from multiple antennas. Subsequently, Bell-state measurements are performed on the received modes A'_i and B'_i from Alice and Bob using homodyne detection, yielding measurement

results X_{C_i} and P_{D_i} . The measurement results X_{C_i} and P_{D_i} are then publicly reported.

- *Step 3:* When receiving the measurement results, a displacement operation $D(\beta)$ is performed on Bob's retained mode to get mode B_i''' , which becomes entangled with Alice's mode A_i [40], where $\beta = g_i \sqrt{\frac{V_{B_i}+1}{V_{B_i}-1}} (X_{C_i} + iP_{D_i})$ [40]. The homodyne detection is then employed to measure mode B_i''' , yielding the measurement result P_{B_i} . Alice also measures her retained mode with homodyne detection, yielding the result X_{A_i} .

The subsequent steps, including data correction, parameter estimation and post-processing, follow the same procedures as the PM model, resulting in the generation of a secure shared key.

B. Asymptotic key analysis

The asymptotic key rate of the proposed protocol is derived in this subsection. In this case, Alice and Bob can easily access their respective channel transmission and modulation variance without any reserved data for evaluation. We extend the method in [34] to compute the key rate for the CVMDI MIMO protocol. The core idea of this approach is to transform the key of MIMO into the sum of the key rate of multiple SISO channels, which is given by [35]

$$K_{\text{MIMO}}^{\text{Ar}} = \sum_{i=1}^r K_i^A, \quad i = 1, 2, \dots, r, \quad (8)$$

where r is the minimum of the rank of the channel matrices $\mathbf{H}_A$ and $\mathbf{H}_B$. Since the proposed protocol employs a two-way scheme, the computation of its key rate can be quite challenging. Fortunately, previous work [40] has identified that the covariance matrix used in a single-channel protocol can be effectively utilized to characterize the quantum state in the two-way protocol. This method enables us to determine the secret key limit of the proposed protocol under collective attacks.

When THz waves are transmitted in a MIMO channel, the equivalent one-way transmission T_i of the CVMDI QKD protocol is [41]

$$T_i = \frac{1}{2} g_i^2 T_{A_i} \quad (9)$$

For the following derivation, it is necessary to characterize the relationship between Alice's and Bob's respective channel excess noise and noise variance [53]

$$\varepsilon_{A_i} = \frac{W_{A_i}(1 - T_{A_i}) - 1}{T_{A_i}} + 1 \quad (10)$$

and

$$\varepsilon_{B_i} = \frac{W_{B_i}(1 - T_{B_i}) - 1}{T_{B_i}} + 1. \quad (11)$$

Since Charlie's detectors are untrusted in the MDI protocol, the noise introduced by the two homodyne detections is attributed as excess noise. The total equivalent excess noise at the output is [41]

$$\varepsilon_i = \frac{T_{B_i}}{T_{A_i}} \left(\sqrt{\frac{2}{T_{B_i} g_i^2}} \sqrt{V_{B_i} - 1} - \sqrt{V_{B_i} + 1} \right)^2 + \varepsilon_{A_i} + \frac{2 + (\varepsilon_{B_i} - 2)T_{B_i}}{T_{A_i}} + \frac{1 - \eta_{D_{B_i}}}{\eta_{D_{B_i}}} + \frac{1 - \eta_{D_{A_i}}}{\eta_{D_{A_i}}}. \quad (12)$$

To minimize excess noise, we set $g_i^2 = [2(V_{B_i} - 1)]/[T_B(V_{B_i} + 1)]$. The T_i and ε_i are rewritten as

$$T_i = \frac{T_{A_i}(V_{B_i} - 1)}{T_{B_i}(V_{B_i} + 1)}, \quad (13)$$

$$\varepsilon_i = \varepsilon_{A_i} + \frac{2 + (\varepsilon_{B_i} - 2)T_{B_i}}{T_{A_i}} + \frac{1 - \eta_{D_{A_i}}}{\eta_{D_{A_i}}} + \frac{1 - \eta_{D_{B_i}}}{\eta_{D_{B_i}}}. \quad (14)$$

The equivalent one-way noise variance can be given by [53]

$$\widehat{W}_i = \frac{T_i(\varepsilon_i - 1) + 1}{1 - T_i}. \quad (14)$$

After transmission and the impact of noise, the covariance matrix $\widehat{\gamma}_{AB_i}'''$ is modified as [55], [56]

$$\widehat{\gamma}_{AB_i}''' = \begin{pmatrix} V_{A_i} \mathbf{I} & \sqrt{T_i(V_{A_i}^2 - 1)} \mathbf{Z} \\ \sqrt{T_i(V_{A_i}^2 - 1)} \mathbf{Z} & [T_i V_{A_i} + (1 - T_i) \widehat{W}_i] \mathbf{I} \end{pmatrix}. \quad (15)$$

In the proposed protocol, we focus only on the RR scheme, as it demonstrates a higher secret key rate and longer transmission distance compared to the DR scheme. The secret key rate of the i -th parallel channel K_i^A with RR is given by [34]

$$K_i^A(V_A, V_B, T_{A_i}, T_{B_i}, W_{A_i}, W_{B_i}) = \beta S(A_i : B_i) - I(B : E_i), \quad (16)$$

where $\beta \in [0, 1]$ is the efficiency of RR and $S(A_i : B_i)$ is the mutual information between the transmitted quantum states from Alice to Bob over the i -th channel, which is described by [57]

$$S(A_i : B_i) = \frac{1}{2} \log_2 \left[1 + \frac{T_i V_{A_i}}{\Lambda_i(V_{A_i}, \widehat{W}_i)} \right], \quad (17)$$

where $\Lambda_i(X, Y) = T_i X + (1 - T_i)Y$. The $I(B_i : E_i)$ denotes the Holevo bound, which quantifies the information accessible to eavesdropper Eve over the i -th channel and is described by [28]

$$I(B_i : E_i) = S(\rho_E) - \sum_{x_B} p(x_B) S(\rho_{E|x_B}) = f(\lambda_1^i) + f(\lambda_2^i) - f(\lambda_3^i) - f(\lambda_4^i), \quad (18)$$

where

$$f(x) = \left(\frac{x+1}{2} \right) \log_2 \left(\frac{x+1}{2} \right) - \left(\frac{x-1}{2} \right) \log_2 \left(\frac{x-1}{2} \right). \quad (19)$$

and λ_{1-4}^i are the symplectic eigenvalues. When signal variance $V_{A(B)M_i} \gg$ thermal noise variance $V_{A(B)O_i}$, λ_{1-4}^i are quantified as [57]

$$\lambda_1^i = \widehat{W}_i, \lambda_2^i = \Lambda_i(\widehat{W}_i, V_{A_i})$$

$$\lambda_{3,4}^i = \sqrt{\frac{1}{2} (A \pm \sqrt{A^2 - 4B})}, \quad (20)$$

where

$$A = \frac{V_{A_i} \widehat{W}_i \Lambda(\widehat{W}_i, V_{A_i}) + \widehat{W}_i \Lambda(\widehat{W}_i V_{A_i}, 1)}{\Lambda(V_{A_i}, \widehat{W}_i)},$$

$$B = \frac{V_{A_i} \widehat{W}_i^2 \Lambda(\widehat{W}_i, V_{A_i}) \Lambda(\widehat{W}_i V_{A_i}, 1)}{\Lambda^2(V_{A_i}, \widehat{W}_i)}, \quad (21)$$

Eventually, the expression for the secret key rate of the CVMDI protocol is calculated by

$$K_{\text{MIMO}}^{\text{Ar}} = \sum_{i=1}^r \frac{1}{2} \log_2 \left(1 + \frac{T_i V_{\text{AM}}}{T_i V_{\text{AO}_i} + T_i (\varepsilon_i - 1) + 1} \right) - f(\hat{W}_i) - f(\Lambda_i(\hat{W}_i, V_{A_i})) + f(\lambda_3^i) + f(\lambda_4^i). \quad (22)$$

C. Finite code rate analysis

The finite code phenomenon plays a critical role in QKD systems, mainly because it influences parameter estimation and privacy amplification. Moreover, in practical quantum communication, the block size is inherently finite, which means that the ideal performance predicted for infinite data block size cannot be achieved. To make the simulation closer to reality, we extend the analysis of the finite code effect, originally studied in Gaussian and discrete modulation QKD protocols, to the CVMDI MIMO THz protocol [43], [58]. Taking into account the effect of finite code under collective attacks, the finite code rate expression for the CVMDI QKD protocol can be formulated as [43], [44]:

$$K_{\text{MIMO}}^{\text{Fr}} = \sum_{i=1}^r \frac{N}{M} [\beta K_i^F(V_A, V_B, T_{LA_i}, T_{LB_i}, W_{UA_i}, W_{UB_i}) - \Delta(N)] \quad (23)$$

where M is the total data block size exchanged by Alice and Bob in the i -th parallel channel and only N data are valid encryption keys. The $\Delta(N)$ is linked to the privacy amplification process, whose value varies with the data block size [48].

$$\Delta(N) = (2\dim H_X + 3) \sqrt{\frac{\log_2(2/\tilde{\varepsilon})}{N}} + \frac{2}{N} \log_2(1/\epsilon_{PA}), \quad (24)$$

where the $(2\dim H_X + 3) \sqrt{\frac{\log_2(2/\tilde{\varepsilon})}{N}}$ represents the convergence speed of the independent and identically distributed minimum entropy and the $\dim H_X = 2$ is the dimension of the Hilbert space of the x and p vectors in the original key. The $\tilde{\varepsilon}$ is the smoothness parameter and ϵ_{PA} is the failure probability of the privacy amplification. Their optimal values are both 10^{-10} [43].

In this model, the block size parameter $l = M - N$ is estimated by sampling the relevant variables. We assume that before the detector, the signals sent by Alice and Bob in the i -th parallel channel are represented by y'_{A_i} and y'_{B_i} respectively. Since the variables of Alice, Bob and Charlie follow a Gaussian distribution, the following relationships exist between the data received by Charlie's node and the original data of Alice and Bob [43], [47]:

$$\begin{aligned} y'_{A_i} &= t'_{A_i} x_{A_i} + z_{A_i}, \\ y'_{B_i} &= t'_{B_i} x_{B_i} + z_{B_i}. \end{aligned} \quad (25)$$

where the z_{A_i} and z_{B_i} follow a Gaussian distribution with mean 0 and unknown variance $\sigma_{A_i}^{\prime 2} = 1 + T_{A_i} \varepsilon_{A_i}$, $\sigma_{B_i}^{\prime 2} =$

$1 + T_{B_i} \varepsilon_{B_i}$ and $t'_{A_i} = \sqrt{T_{A_i}}$, $t'_{B_i} = \sqrt{T_{B_i}}$. Their MLE are respectively [43]

$$\begin{aligned} \hat{t}'_{A_i} &= \frac{\sum_{j=1}^k x_{A_{ij}} y'_{A_{ij}}}{\sum_{j=1}^k x_{A_{ij}}^2}, \hat{t}'_{B_i} = \frac{\sum_{j=1}^k x_{B_{ij}} y'_{B_{ij}}}{\sum_{j=1}^k x_{B_{ij}}^2}, \\ \hat{\sigma}_{A_i}^{\prime 2} &= \frac{1}{k} \sum_{j=1}^k (y'_{A_{ij}} - \hat{t}'_{A_i} x_{A_{ij}})^2, \\ \hat{\sigma}_{B_i}^{\prime 2} &= \frac{1}{k} \sum_{j=1}^k (y'_{B_{ij}} - \hat{t}'_{B_i} x_{B_{ij}})^2, \end{aligned} \quad (26)$$

where $\hat{t}'_{A_i}$, $\hat{t}'_{B_i}$, $\hat{\sigma}_{A_i}^{\prime 2}$ and $\hat{\sigma}_{B_i}^{\prime 2}$ of independent estimators follow the following distribution [43]

$$\begin{aligned} \hat{t}'_{A_i} &\sim N(t'_{A_i}, \frac{\sigma_{A_i}^{\prime 2}}{\sum_{j=1}^k x_{A_{ij}}^2}), \hat{t}'_{B_i} \sim N(t'_{B_i}, \frac{\sigma_{B_i}^{\prime 2}}{\sum_{j=1}^k x_{B_{ij}}^2}), \\ \frac{l \hat{\sigma}_{A_i}^{\prime 2}}{\sigma_{A_i}^{\prime 2}}, \frac{l \hat{\sigma}_{B_i}^{\prime 2}}{\sigma_{B_i}^{\prime 2}} &\sim \chi^2(l-1). \end{aligned} \quad (27)$$

Due to the limit of block size l and probability $\epsilon_{PE/2}$, Alice and Bob can evaluate these parameters at confidence intervals, which are given by [48]

$$\begin{aligned} t'_{A_i} &\in \left[\hat{t}'_{A_i} - z_{\epsilon_{PE/2}} \sqrt{\frac{\hat{\sigma}_{A_i}^{\prime 2}}{l V_A}}, \hat{t}'_{A_i} + z_{\epsilon_{PE/2}} \sqrt{\frac{\hat{\sigma}_{A_i}^{\prime 2}}{l V_A}} \right], \\ t'_{B_i} &\in \left[\hat{t}'_{B_i} - z_{\epsilon_{PE/2}} \sqrt{\frac{\hat{\sigma}_{B_i}^{\prime 2}}{l V_B}}, \hat{t}'_{B_i} + z_{\epsilon_{PE/2}} \sqrt{\frac{\hat{\sigma}_{B_i}^{\prime 2}}{l V_B}} \right], \\ \sigma_{A_i}^{\prime 2} &\in \left[\hat{\sigma}_{A_i}^{\prime 2} - z_{\epsilon_{PE/2}} \frac{\hat{\sigma}_{A_i}^{\prime 2} \sqrt{2}}{\sqrt{l}}, \hat{\sigma}_{A_i}^{\prime 2} + z_{\epsilon_{PE/2}} \frac{\hat{\sigma}_{A_i}^{\prime 2} \sqrt{2}}{\sqrt{l}} \right], \\ \sigma_{B_i}^{\prime 2} &\in \left[\hat{\sigma}_{B_i}^{\prime 2} - z_{\epsilon_{PE/2}} \frac{\hat{\sigma}_{B_i}^{\prime 2} \sqrt{2}}{\sqrt{l}}, \hat{\sigma}_{B_i}^{\prime 2} + z_{\epsilon_{PE/2}} \frac{\hat{\sigma}_{B_i}^{\prime 2} \sqrt{2}}{\sqrt{l}} \right], \end{aligned} \quad (28)$$

where $z_{\epsilon_{PE/2}} = 6.5$ and ϵ_{PE} is the failure probability of the parameter estimation process. For any modulated variance $V_{A(B)}$, the first order derivative of K_i^F with respect to $t_{A(B)}$ and $\sigma_{A(B)i}^2$ are related as follows:

$$\frac{\partial K_i^F}{\partial t_{A(B)i}} \big|_{V_{A(B)}} > 0 \quad (29)$$

and

$$\frac{\partial K_i^F}{\partial \sigma_{A(B)i}^2} \big|_{V_{A(B)}} < 0. \quad (30)$$

To enhance the security of the protocol, we analyze one of the fastest scenarios, where Alice and Bob always estimate the lower bound of the $\hat{t}_{LA(B)i}$ and the upper bound of $\hat{\sigma}_{UA(B)i}^{\prime 2}$. We have

$$\begin{aligned} \hat{t}'_{LA_i} &= \hat{t}'_{A_i} - z_{\epsilon_{PE/2}} \sqrt{\frac{\hat{\sigma}_{A_i}^{\prime 2}}{l V_A}}, \\ \hat{t}'_{LB_i} &= \hat{t}'_{B_i} - z_{\epsilon_{PE/2}} \sqrt{\frac{\hat{\sigma}_{B_i}^{\prime 2}}{l V_B}}, \end{aligned} \quad (31)$$

and

$$\begin{aligned}\hat{\sigma}_{UA_i}^{\prime 2} &= \hat{\sigma}_{A_i}^{\prime 2} + z_{\epsilon_{PE}/2} \frac{\hat{\sigma}_{A_i}^{\prime 2} \sqrt{2}}{\sqrt{l}}, \\ \hat{\sigma}_{UB_i}^{\prime 2} &= \hat{\sigma}_{B_i}^{\prime 2} + z_{\epsilon_{PE}/2} \frac{\hat{\sigma}_{B_i}^{\prime 2} \sqrt{2}}{\sqrt{l}}.\end{aligned}\quad (32)$$

By association of the equations $\hat{\sigma}_{UA_i}^{\prime 2} = 1 + T_{A_i} \epsilon_{UA_i}$, $\hat{\sigma}_{UB_i}^{\prime 2} = 1 + T_{B_i} \epsilon_{UB_i}$, $\hat{l}_{LA_i} = \sqrt{T_{LA_i}}$ and $\hat{l}_{LB_i} = \sqrt{T_{LB_i}}$, we have

$$\begin{aligned}T_{LA_i} &= (\sqrt{T_{A_i}} - z_{\epsilon_{PE}/2} \sqrt{\frac{1 + T_{A_i} \epsilon_{A_i}}{lV_A}})^2, \\ T_{LB_i} &= (\sqrt{T_{B_i}} - z_{\epsilon_{PE}/2} \sqrt{\frac{1 + T_{B_i} \epsilon_{B_i}}{lV_B}})^2.\end{aligned}\quad (33)$$

and

$$\begin{aligned}\epsilon_{UA_i} &= \epsilon_{A_i} + z_{\epsilon_{PE}/2} \frac{(1 + T_{A_i} \epsilon_{A_i}) \sqrt{2}}{T_{A_i} \sqrt{l}}, \\ \epsilon_{UB_i} &= \epsilon_{B_i} + z_{\epsilon_{PE}/2} \frac{(1 + T_{B_i} \epsilon_{B_i}) \sqrt{2}}{T_{B_i} \sqrt{l}}.\end{aligned}\quad (34)$$

The estimated noise variance W_{UA_i} and W_{UB_i} are given by [53]

$$\begin{aligned}W_{UA_i} &= \frac{T_{LA_i} \epsilon_{UA_i}}{1 - T_{LA_i}} + 1, \\ W_{UB_i} &= \frac{T_{LB_i} \epsilon_{UB_i}}{1 - T_{LB_i}} + 1.\end{aligned}\quad (35)$$

When $T_{A(B)i}$ are replaced by $T_{LA(B)i}$ and $W_{A(B)i}$ by $W_{UA(B)i}$, using an similar approach with asymptotic key rate, we derive the finite code key rate $K_{\text{MIMO}}^{\text{Fr}}$ for the CVMDI MIMO protocol.

IV. SIMULATION AND PERFORMANCE EVALUATION

Next, an evaluation of the performance of both MIMO and SISO CVMDI protocols over atmospheric channels is conducted. To achieve the maximum spatial multiplexing gain, we set multipath components $L_A = \min(N_{T_A}, N_{R_A})$ and $L_B = \min(N_{T_B}, N_{R_B})$ [59], [60]. In this case, The channel matrices $\mathbf{H}_A$ and $\mathbf{H}_B$ are full-rank matrices. The analysis is centered on a symmetric scenario, where the number of transmitter antenna nodes $N_{T_{A,B}}$ is equal to the number of receiver antenna nodes $N_{R_{A,B}}$, the MIMO channel connecting Alice and Charlie is identical to the one between Bob and Charlie and Charlie is in the middle of Alice and Bob. The total transmission distance is $d_{AB} = d_{AC} + d_{BC} = 2d_{AC}$. There exists a correlation between atmospheric loss and THz frequency. Accordingly, in this paper, we assume atmospheric losses $\delta_{1,2}$ are assumed to be 0.6dB/km, 5dB/km, 50dB/km and 100dB/km for the frequency bands 0.1THz, 0.25THz, 0.5THz and 1THz, respectively [25], [57]. Detailed values and definitions of the relevant parameters are provided in Table I.

We first identify the conditions under which the proposed protocol achieves a positive secret key rate. Figure 2 shows the secret key rate versus frequency for different MIMO configurations at room temperature when the transmission distance approaches zero. As the frequency increases moderately from 0.1 THz to 1 THz, the initial key rate(bits/channel use)

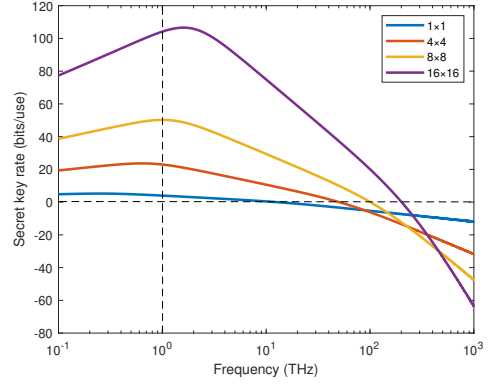


Fig. 2. Key rate as a function of operating frequency for multiple MIMO configurations at room temperature when transmission distance approaches zero.

of the CVMDI MIMO QKD protocol improves. However, further increases in frequency lead to a significant degradation in system transmission, resulting in a reduction in the key rate. Notably, for frequencies above 300 THz, the protocol fails to generate a positive key rate. The subsequent analysis focuses on the frequency range of [0.1 THz, 1 THz]. Both the simulation of the asymptotic key rate and finite code key rate are considered.

A. Asymptotic key rate simulation

In the asymptotic regime, we consider an ideal scenario in which key distribution is error-free, and both communicating parties can achieve their respective channel transmissions and modulation variances without requiring additional data for parameter estimation. This assumption provides an upper bound on the secret key rate for the proposed protocol. Based on the derived expression in Eq. (22), we can evaluate the performance of the MDI MIMO THz QKD protocol. The relevant simulation parameters of the asymptotic key are presented in rows 1 through 13 of Table I.

In Figure 3, we investigate the maximum transmission distance as a function of the asymptotic key rate $K_{\text{MIMO}}^{\text{Ar}}$ over frequencies ranging from 0.1 THz to 1 THz for various MIMO configurations ($N_{T_{A,B}} \times N_{R_{A,B}}$). Our results show that MIMO techniques significantly improve both the key rate and the maximum achievable transmission distance. According to Figure 3 (a), (b), (c), (d), we can find the CVMDI QKD system performs optimally at 100 GHz for long distance transmission, where the interplay between thermal noise, transmission and the frequency of THz wave is most favorable. When the frequency decreases from 1 THz to 0.1 THz, thermal noise increases, which negatively affects the secret key rate. However, the transmission efficiency improves and the path loss is reduced, both of which are beneficial for key generation. The positive impact outweighs the negative impact of increased noise, resulting in an overall enhancement of the transmission distance. Consequently, we conclude that the optimal frequency for achieving the maximum transmission distance of CVMDI MIMO protocol lies at the lower limit of the THz channel (0.1 THz). By appropriately adjusting the number

TABLE I
RELEVANT PARAMETERS

Order	Symbol	Description	Value
1	$N_{T,A,B}$	Transmitter antenna node	Independent variable
2	$N_{R,A,B}$	Receiver antenna node	Independent variable
3	$L_{A(B)}$	multipath components	Independent variable
4	$V_{A(B)M}$	Modulation variance	100000 [41]
5	β	Reconciliation efficiency	1
6	$W_{A(B)i}$	Noise variance	1 [52]
7	$\delta_{1,2}$	Atmospheric loss	Independent variable
8	k_B	Boltzmann constant	1.38×10^{-23}
9	h	Planck constant	6.626×10^{-34}
10	f_c	Frequency	Independent variable
11	T_k	Temperature	300K
12	$\eta_{D_{A(B)i}}$	Detector efficiency	Independent variable
13	G_a	antenna element	30 [21]
14	M	Block size	Independent variable
15	N	Valid encryption keys	Independent variable
16	$\dim Hx$	Hilbert space dimension	2 [43]
17	$\tilde{\epsilon}$	Smoothness parameter	10^{-10} [43]
18	ϵ_{PA}	Failure probability of privacy amplification	10^{-10} [44]
19	$z\epsilon_{PE/2}$	Probability error	6.5 [43]
20	l	Block size for parameter estimation	Independent variable

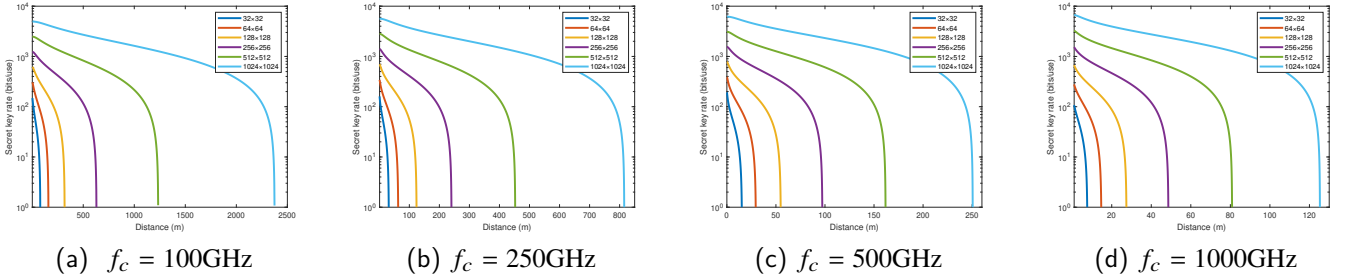


Fig. 3. Asymptotic key rate as a function of the transmission distance for the various MIMO configurations with different frequencies. As the frequency decreases from 1THz to 0.1THz, the maximum transmission distance in 1024×1024 MIMO configuration gradually increases from 125m to 2374m. This trend also applies to other MIMO configurations. $\eta_{D_{A(B)i}} = 1$, atmospheric loss $\delta_{1,2}$: 0.6dB/km for 0.1THz, 5 dB/km for 0.25THz, 50dB/km for 0.5THz and 100dB/km for 1THz.

of antennas and the frequency of the THz wave, proposed protocol can meet the requirements for both short-distance indoor and long-distance outdoor wireless communication.

In Figure 4, a three-dimensional surface plot shows the relationship between the key rate, homodyne detection efficiency $\eta_{D_{A(B)i}}$ and maximum transmission distance for different MIMO configurations. In each subplot, the MIMO configurations are represented from top to bottom as 16×16 , 8×8 and 4×4 , respectively. The results indicate that insufficient detector efficiency significantly degrades both the asymptotic key rate and the achievable transmission distance. This highlights the critical role of near-ideal detectors in enabling high-rate, long-distance key distribution, as poor detection performance can severely compromise key stability and overall protocol reliability—an issue largely overlooked in prior MIMO QKD studies.

When $N_{T,A,B} \times N_{R,A,B}$ configuration is set to 1×1 , the MIMO protocol is changed to the SISO protocol. Figures 5 and 6 provide a quantitative evaluation of the SISO protocol. Figure 5 shows how the key rate varies with the transmission distance in different THz scenarios. In comparison to larger MIMO configurations, the SISO protocol demonstrates suboptimal

performance, with a maximum transmission distance of almost 250 cm. However, an interesting observation from Figure 5 is that the SISO protocol exhibits a positive correlation between key rate and frequency at short ranges (0-4cm). This finding serves as a critical note: it shows that higher frequencies play a key role in short-distance transmission, potentially improving the key rate for indoor communications. Conversely, for long-distance outdoor communications, it is imperative to maintain the frequency of the THz wave at low frequency (100 GHz) to ensure optimal performance.

Figure 6 further investigates the effect of homodyne detector efficiency on the SISO protocol at 100 GHz. In Figure 6, the conclusion can be observed that as the detector efficiency decreases from its optimal value to 0.6, the effective maximum transmission distance also decreases from 248 cm to 92 cm. The decrease in transmission distance is primarily due to the increase in excess noise. Meanwhile, in Figure 4(a), we find that the rate of decrease of the MIMO protocol with a 16×16 configuration is significantly lower than that of the SISO protocol within the same interval [0.6, 1]. It indicates that the MIMO technique improves the resistance of the MDI protocol to noise variance, underscoring the merits of the

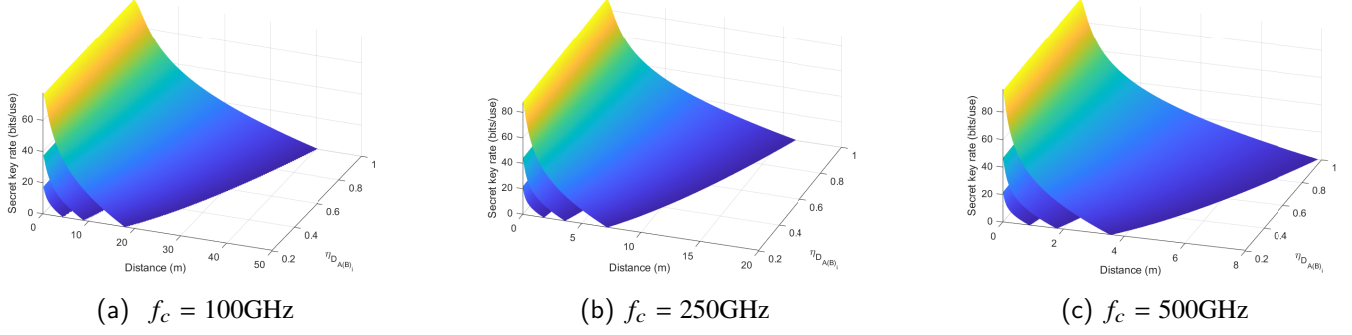


Fig. 4. A three-dimensional surface plot showing the relationship between the $K_{\text{MIMO}}^{\text{Ar}}$, homodyne detector efficiency and the transmission distance with different frequencies. All subplots, arranged from top to bottom, represent the 16×16 , 8×8 and 4×4 MIMO configurations, respectively. atmospheric loss $\delta_{1,2}$: 0.6dB/km for 0.1THz, 5dB/km for 0.25THz and 50dB/km for 0.5THz

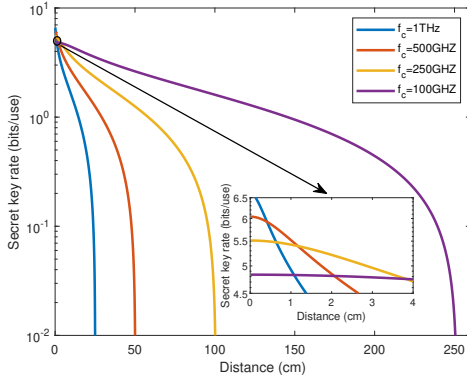


Fig. 5. Secret key rate as a function of transmission distance for different frequencies in SISO protocol. It can be observed that, at shorter distances, higher frequency THz waves yield higher key rates. $\eta_{D(A|B)_i} = 1$, atmospheric loss $\delta_{1,2}$: 0.6dB/km for 0.1THz, 5dB/km for 0.25THz, 50dB/km for 0.5THz and 100dB/km for 1THz.

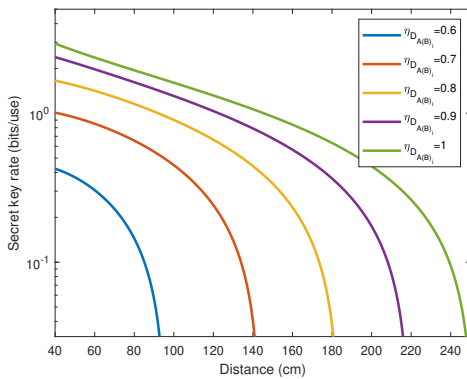


Fig. 6. Asymptotic key rate as a function of transmission distance for different homodyne detector efficiency in the SISO protocol. The maximum transmission distance is less than half of the optimal case when the detector efficiency is 0.6. $f_c = 100\text{GHz}$, $\delta_{1,2} = 0.6\text{dB/km}$.

MIMO approach.

B. Finite code rate simulation

Based on the derivation of Eq. (23), we now have sufficient

information to evaluate the impact of finite code on both MDI MIMO and SISO protocols. In our analysis, we assume that the data block size used by Alice and Bob during the parameter estimation phase is half of the total data block size, i.e. $l = N = 0.5M$. As determined in the previous subsection, the optimal frequency for long distance transmission in this protocol is 100 GHz, so we adopt $f_c = 100\text{GHz}$. We continue to restrict our analysis to the symmetric models. All simulation parameters are outlined in Table I.

Figure 7 shows the maximum transmission distance as a function of the finite code rate $K_{\text{MIMO}}^{\text{Fr}}$ at 0.1 THz and room temperature, for various MIMO configurations and block sizes. The lower subplots display configurations of 8×8 , 16×16 , 32×32 and 64×64 , while the upper subplots include 128×128 , 256×256 , 512×512 and 1024×1024 . In each subplot, a discernible trend emerges: as the block size increases, both the key rate and the maximum achievable transmission distance show a corresponding improvement. This is because, as the block size increases, the estimators $T_{LA(B)_i}$ and $W_{UA(B)_i}$ in Eqs. (33) and (35) become closer to the true values $T_{A(B)_i}$ and $W_{A(B)_i}$. At the same time, the amount of data allocated for privacy amplification (see Eq. 24) decreases, leading to an increase in the key rate of the proposed protocol. When the block size approaches infinity, Alice and Bob can accurately estimate the channel parameters and the data reserved for privacy amplification becomes negligible. However, since only a fraction $\frac{N}{M}$ of the all signals are actually encoded, the secret key rate under finite-size conditions remains lower than the asymptotic key rate. Notably, when the block size reaches $M = 2 \times 10^6$, the performance in terms of secret key rate and transmission distance approaches that of an infinite block size. Therefore, a block size of $M = 2 \times 10^6$ provides a favorable balance between practical constraints and performance, making it well-suited for the implementation of the CVMDI MIMO protocol.

For completeness, we also include a three-dimensional graph for SISO in Figure 8, which illustrates the relationship between block size, transmission distance and key rate. As expected, the finite code effect reduces the maximum transmission distance of the SISO protocol and this limitation can be mitigated by increasing the block size. In comparison

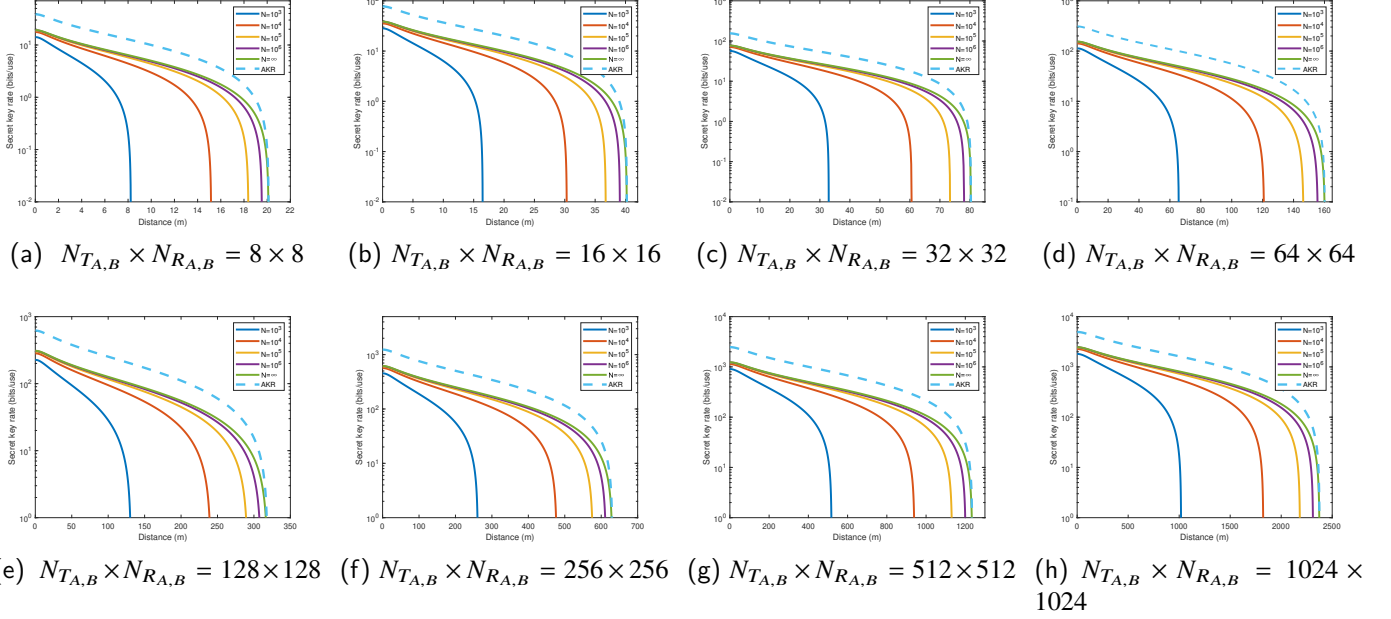


Fig. 7. Finite code rate as a function of transmission distance for the different MIMO configurations with different data block sizes. When the data block size is below 2×10^5 , the effective transmission distance of the CVMDI MIMO protocol decreases significantly. However, when the data block size reaches 2×10^6 , the effective transmission distance approaches that of an infinite range, offering an optimal balance between cost and performance. The AKR curve represents the asymptotic key rate for this MIMO configuration. $M = 2N$, $f_c = 100\text{GHz}$, $\eta_{D_{A(B)_i}} = 1$, $\delta_{1,2} = 0.6\text{dB/km}$.

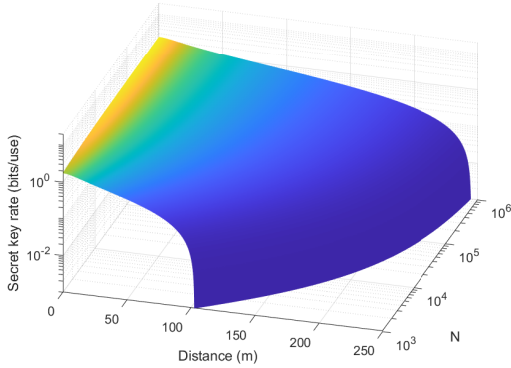


Fig. 8. A three-dimensional surface plot illustrating the relationship between $K_{\text{MIMO}}^{\text{Fr}}$, valid data block size N and the transmission distance. $M = 2N$, $f_c = 100\text{GHz}$, $\eta_{D_{A(B)_i}} = 1$, $\delta_{1,2} = 0.6\text{dB/km}$.

with Figure 7, it is evident that the SISO protocol consistently underperforms relative to the MIMO protocol under identical block size conditions. This further emphasizes the importance of antenna technology in enhancing system performance.

C. Comparison with other literature

To comprehensively assess the performance of the proposed CVMDI MIMO protocol, we compare it with several representative CVQKD schemes reported in recent literature, as summarized in Table II. The comparison criteria include transmission distance, MIMO configuration, atmospheric temperature, operating frequency and the consideration of finite-size effects. Our protocol supports secure communication over long

distances in room temperature. Specifically, under a 0.1THz frequency and a 1024×1024 MIMO configuration, it enables secure key distribution over a distance of 2374m. Although prior work [57] demonstrated long-distance transmission using MIMO-based CVQKD, its implementation requires a low-temperature environment, and the lack of an MDI framework leaves it vulnerable to detector-side attacks. It is noteworthy that the CVQKD protocol based on OTFS-MIMO achieves transmission over 500 meters even with a low-configuration MIMO setup, demonstrating its robustness against the severe path loss [39]. This result underscores the potential of combining advanced multi-carrier waveforms with spatial diversity to enable long-distance quantum communications in practical scenarios.

A key distinguishing feature of our protocol is its MDI architecture, which inherently mitigates all detector-side channel attacks—an essential security guarantee absent in the compared literature. Additionally, our analysis incorporates finite-size effects using the MLE method, further enhancing the practicality and real-world applicability of the proposed scheme.

V. CONCLUSION

We have discussed the MIMO CVMDI QKD system operating at THz frequencies and provided a detailed description of the communication steps for both the EB and PM schemes. The secret key rate of the asymptotic and finite code for the proposed protocol is derived under the Gaussian collective attacks. The protocol is designed to effectively minimize noise and other adverse factors, thereby ensuring consistent performance in complex environments. The relevant analysis

TABLE II
PERFORMANCE COMPARISON BETWEEN MDI MIMO AND EXISTING MIMO-BASED QKD PROTOCOLS

Document	Transmission distance	MIMO configuration	Temperature	Frequency	Finite code
[34]	250m	1024×1024	room temperature	15THz	NO
[35]	close 100m	256×256	room temperature	15THz	least-square
[36]	over 100m	512×512	room temperature	15THz	least-square
[37]	130m	512×512	low temperature	15THz	NO
[38]	over 100m	256×256	room temperature	15THz	least-square
[39]	over 500m	8×8	room temperature	15THz	NO
[57]	over 8000m	1024×1024	low temperature	0.1THz	NO
[57]	over 3000m	1024×1024	low temperature	0.2THz	NO
MDI MIMO	20m	8×8	room temperature	0.1THz	NO
MDI MIMO	2374m	1024×1024	room temperature	0.1THz	NO
MDI MIMO	125m	1024×1024	room temperature	1THz	NO
MDI MIMO	316m	128×128	room temperature	0.1THz	NO
MDI MIMO	307m	128×128	room temperature	0.1THz	MLE

provides a solid theoretical foundation for understanding the protocol and ensures the reliability and security of the system.

The MIMO architecture enhances the MDI THz system's resilience to jamming and ensures reliable key transmission in free-space scenarios. By adjusting key parameters, including the THz wave frequency and homodyne detection efficiency, the proposed protocol can be flexibly adapted to QKD systems with different channel lengths. By appropriately configuring the number of antenna nodes in the CVMDI MIMO protocol, the proposed protocol can be effectively applied to both indoor and outdoor wireless communication. When the data block size is set to 2×10^6 , nearly infinite block size performance can be achieved at a low cost, which greatly enhances the practicality and economic feasibility of MIMO MDI THz QKD.

REFERENCES

- [1] Tang F, Chen X, Zhao M. The Roadmap of Communication and Networking in 6G for the Metaverse. *IEEE Wireless Communications*, 2022, 30(4): 72-81.
- [2] Zhang X, Li H, Gao J, et al. Progressive Freezing Low-complexity Belief Propagation Decoder of Polar Codes for 6G Wireless Communications[J]. *IEEE Transactions on Vehicular Technology*, 2024.
- [3] Cai L, Dai Y, Hu Q. Bayesian Game-Driven Incentive Mechanism for Blockchain-Enabled Secure Federated Learning in 6 G Wireless Networks. *IEEE Transactions on Network Science and Engineering*, 2024.
- [4] Chen W, Lin X, Lee J. 5G-advanced toward 6G: Past, present, and future. *IEEE Journal on Selected Areas in Communications*, 2023, 41(6): 1592-1619.
- [5] Chen Z, Zhang Z, Yang Z. Big AI models for 6G wireless networks: Opportunities, challenges, and research directions. *IEEE Wireless Communications*, 2024.
- [6] Khan M A, Kumar N, Mohsan S A H. Swarm of UAVs for network management in 6G: A technical review. *IEEE Transactions on Network and Service Management*, 2022, 20(1): 741-761.
- [7] Roy S, Chergui H, Verikoukis C. Toward bridging the FL performance-explainability tradeoff: A trustworthy 6G RAN slicing use-case[J]. *IEEE Transactions on Vehicular Technology*, 2024, 73(7): 10529-10538.
- [8] Ghafouri N, Vardakas J S, Ramantas K, et al. A multi-level deep rl-based network slicing and resource management for o-ran-based 6g cell-free networks[J]. *IEEE Transactions on Vehicular Technology*, 2024, 73(11): 17472-17484.
- [9] Park J, Sohrabi F, Ghosh A, et al. End-to-end deep learning for TDD MIMO systems in the 6G upper midbands. *IEEE Transactions on Wireless Communications*, 2024.
- [10] Khan A A, Laghari A A, Baqasah A M. ORAN-B5G: A next generation open radio access network architecture with machine learning for beyond 5G in industrial 5.0. *IEEE Transactions on Green Communications and Networking*, 2024.
- [11] Wang W, Tan Y J, Tan T C W. On-chip topological beamformer for multi-link terahertz 6G to XG wireless. *Nature*, 2024, 632(8025): 522-527.
- [12] Zhang Y, Li D, Qiao D, et al. Analysis of indoor THz communication systems with finite-bit DACs and ADCs[J]. *IEEE Transactions on Vehicular Technology*, 2021, 71(1): 375-390.
- [13] Xia Q, Hossain Z, Medley M, et al. A link-layer synchronization and medium access control protocol for terahertz-band communication networks[J]. *IEEE Transactions on Mobile Computing*, 2019, 20(1): 2-18.
- [14] He D, Guan K, Fricke A. Stochastic channel modeling for kiosk applications in the terahertz band. *IEEE Transactions on Terahertz Science and Technology*, 2017, 7(5): 502-513.
- [15] Eckhardt J M, Petrov V, Moltchanov D. Channel measurements and modeling for low-terahertz band vehicular communications. *IEEE Journal on Selected Areas in Communications*, 2021, 39(6): 1590-1603.
- [16] Lyu J, Guan Y L, Liu X, et al. Inter-orbital Inter-satellite communication link performance analysis at THz band considering gravity-induced antenna pointing error[J]. *IEEE Transactions on Vehicular Technology*, 2025.
- [17] Tong X, Chang B, Meng Z. Calculating terahertz channel capacity under beam misalignment and user mobility. *IEEE Wireless Communications Letters*, 2021, 11(2): 348-351.
- [18] Kong P Y. Secret Key Rate Over Multiple Relays in Quantum Key Distribution for Cyber-Physical Systems. *IEEE Transactions on Industrial Informatics*, 2024.
- [19] Wu L, Zhang L, Feng Y. Passive-state preparation continuous-variable quantum key distribution with an independent source. *Optics Communications*, 2025: 131536.
- [20] Liu X, Luo D, Luo Z. Reference-frame-independent quantum key distribution over 250 km of optical fiber. *Physical Review Applied*, 2024, 22(6): 064018.
- [21] Kundu N K, McKay M R, Murch R, et al. Intelligent reflecting surface-assisted free space optical quantum communications. *IEEE Transactions on Wireless Communications*, 2023, 23(5): 5079-5093.
- [22] Ai X, Malaney R. Optimised multithreaded CV-QKD reconciliation for global quantum networks. *IEEE Transactions on Communications*, 2022, 70(9): 6122-6132.
- [23] Ruiz, Lidia, and Juan Carlos Garcia-Escartin. Routing and wavelength assignment in hybrid networks with classical and quantum signals. *arXiv preprint arXiv:2311.10474* (2023).
- [24] Ghalaii M, Ottaviani C, Kumar R. Discrete-modulation continuous-variable Q enhanced by quantum scissors. *IEEE Journal on Selected Areas in Communications*, 2020, 38(3): 506-516.

- [25] Ottaviani C, Woolley M J, Erementschouk M, et al. Terahertz quantum cryptography. *IEEE Journal on Selected Areas in Communications*, 2020, 38(3): 483-495.
- [26] Sayat M, Shajilal B, Kish S P, et al. Satellite-to-ground continuous variable quantum key distribution: The Gaussian and discrete modulated protocols in low earth orbit. *IEEE Transactions on Communications*, 2024.
- [27] Kiktenko E O, Malyshev A O, Gavreev M A. Lightweight authentication for quantum key distribution. *IEEE Transactions on Information Theory*, 2020, 66(10): 6354-6368.
- [28] Wu L, Feng Y, Zhou J. The effect of acceleration on continuous-variable quantum key distribution with discrete modulation. *The European Physical Journal Plus*, 2023, 138(10): 963.
- [29] Notarnicola M N, Olivares S, Forestieri E. Probabilistic amplitude shaping for continuous-variable quantum key distribution with discrete modulation over a wiretap channel. *IEEE Transactions on Communications*, 2023.
- [30] Adnan M H, Ahmad Zukarnain Z, Harun N Z. Quantum key distribution for 5g networks: A review, state of art and future directions. *Future Internet*, 2022, 14(3): 73.
- [31] Muheidat F, Dajani K, Lo'ai A T. Security concerns for 5G/6G mobile network technology and quantum communication. *Procedia Computer Science*, 2022, 203: 32-40.
- [32] He Y, Mao Y, Huang D. Indoor channel modeling for continuous variable quantum key distribution in the terahertz band. *Optics Express*, 2020, 28(22): 32386-32402.
- [33] Liu C, Zhu C, Nie M, et al. Composable security for inter-satellite continuous-variable quantum key distribution in the terahertz band. *Optics Express*, 2022, 30(9): 14798-14816.
- [34] Kundu N K, Dash S P, McKay M R. MIMO terahertz quantum key distribution. *IEEE Communications Letters*, 2021, 25(10): 3345-3349.
- [35] Kundu N K, Dash S P, McKay M R. Channel estimation and secret key rate analysis of MIMO terahertz quantum key distribution. *IEEE Transactions on Communications*, 2022, 70(5): 3350-3363.
- [36] Kundu N K, McKay M R, Conti A. MIMO terahertz quantum key distribution under restricted eavesdropping. *IEEE Transactions on Quantum Engineering*, 2023, 4: 1-15.
- [37] Kumar S, Dash S P. RIS-Assisted THz MIMO Wireless System in the Presence of Direct Link for CV-QKD with Limited Quantum Memory. *arXiv preprint arXiv:2410.16731*, 2024.
- [38] Kumar S, Dash S P, Ghose D, et al. RIS-Assisted MIMO CV-QKD at THz Frequencies: Channel Estimation and SKR Analysis. *arXiv preprint arXiv:2412.18771*, 2024.
- [39] Liu X, Xu C, Ng S X, et al. OTFS-based CV-QKD systems for doubly selective THz channels[J]. *IEEE Transactions on Communications*, 2025.
- [40] Li Z, Zhang Y C, Xu F. Continuous-variable measurement-device-independent quantum key distribution. *Physical Review A*, 2014, 89(5): 052301.
- [41] Zhou J, Feng Y, Shi J. Plug-and-Play Continuous Variable Measurement-Device-Independent Quantum Key Distribution. *Annalen der Physik*, 2023, 535(5): 2200614.
- [42] Zhao R, Zhou J, Shi R. Continuous-variable measurement-device-independent multipartite quantum communication via a fast-fading channel. *Physical Review A*, 2025, 111(1): 012613.
- [43] Leverrier A, Grosshans F, Grangier P. Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A—Atomic, Molecular, and Optical Physics*, 2010, 81(6): 062343.
- [44] Kanitschar F, George I, Lin J. Finite-size security for discrete-modulated continuous-variable quantum key distribution protocols. *PRX Quantum*, 2023, 4(4): 040306.
- [45] Matsuura T, Maeda K, Sasaki T. Finite-size security of continuous-variable quantum key distribution with digital signal processing. *Nature communications*, 2021, 12(1): 252.
- [46] Wang P, Wang X, Li J, et al. Finite-size analysis of unidimensional continuous-variable quantum key distribution under realistic conditions. *Optics Express*, 2017, 25(23): 27995-28009.
- [47] Hosseini-dehaj N, Walk N, Ralph T C. Composable finite-size effects in free-space continuous-variable quantum-key-distribution systems. *Physical Review A*, 2021, 103(1): 012605.
- [48] Xu S, Li Y, Wang Y, et al. Security analysis of a passive continuous-variable quantum key distribution by considering finite-size effect. *Entropy*, 2021, 23(12): 1698.
- [49] Busari S A, Huq K M S, Mumtaz S. Terahertz massive MIMO for beyond-5G wireless communication[C]//ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019: 1-6.
- [50] Weedbrook C. Continuous-variable quantum key distribution with entanglement in the middle. *Physical Review A—Atomic, Molecular, and Optical Physics*, 2013, 87(2): 022308.
- [51] Weedbrook C, Pirandola S, Lloyd S. Quantum cryptography approaching the classical limit. *Physical review letters*, 2010, 105(11): 110501.
- [52] Leonhardt U. Quantum physics of simple optical instruments. *Reports on Progress in Physics*, 2003, 66(7): 1207.
- [53] Weedbrook C, Pirandola S, Ralph T C. Continuous-variable quantum key distribution using thermal states. *Physical Review A—Atomic, Molecular, and Optical Physics*, 2012, 86(2): 022318.
- [54] Zhang M, Huang P, Wang P. Experimental free-space continuous-variable quantum key distribution with thermal source. *Optics Letters*, 2023, 48(5): 1184-1187.
- [55] Wang Z, Malaney R, Green J. Inter-satellite quantum key distribution at terahertz frequencies//ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019: 1-7.
- [56] Continuous-variable quantum key distribution with Gaussian modulation—The theory of practical implementations,” *Advanced Quantum Technologies*, 2018, 1(1): 1800011
- [57] Zhang M, Pirandola S, Delfanazari K. Millimeter-waves to terahertz SISO and MIMO continuous variable quantum key distribution. *IEEE Transactions on Quantum Engineering*, 2023, 4: 1-10.
- [58] Scarani V, Renner R. Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing. *Physical review letters*, 2008, 100(20): 200501.
- [59] Telatar E. Capacity of multi-antenna Gaussian channels[J]. *European transactions on telecommunications*, 1999, 10(6): 585-595.
- [60] Bjornson E, Zetterberg P, Bengtsson M, et al. Capacity limits and multiplexing gains of MIMO channels with transceiver impairments[J]. *IEEE Communications Letters*, 2012, 17(1): 91-94.