MIMO Terahertz Quantum Key Distribution Under Restricted Eavesdropping

NEEL KANTH KUNDU[1] (Member, IEEE),
MATTHEW R. MCKAY[1,2] (Fellow, IEEE), ANDREA CONTI[3] (Fellow, IEEE),
RANJAN K. MALLIK[4] (Fellow, IEEE), AND MOE Z. WIN[5] (Fellow, IEEE)

[1]Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology, Kowloon, Hong Kong
[2]Department of Electrical and Electronic Engineering, University of Melbourne, Melbourne, VIC 3010, Australia
[3]Department of Engineering and the National Inter-University Consortium for Telecommunications (CNIT), University of Ferrara, 44122 Ferrara, Italy
[4]Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi 110016, India
[5]Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, MA 02139 USA

Corresponding author: Ranjan K. Mallik (e-mail: rkmallik@ee.iitd.ernet.in).

ABSTRACT Quantum key distribution (QKD) can provide unconditional security to next-generation communication networks guaranteed by the laws of quantum physics. This article studies the secret key rate (SKR) of a continuous variable QKD (CV-QKD) system using multiple-input multiple-output (MIMO) transmission and operating at terahertz (THz) frequencies. Distinct from previous works, we consider a practical "restricted" eavesdropping scenario in which Eve can collect only a fraction of photons lost in the environment. We propose a system model for the MIMO THz CV-QKD system that accounts for restricted eavesdropping via a lossy wireless channel between Alice and Eve. We derive for this system new SKR expressions for both coherent-state-based and squeezed-state-based CV-QKD protocols. Our results show that previous analysis assuming unrestricted eavesdropping leads to overly pessimistic SKRs, and that in practice, the achievable SKR can be significantly increased under restricted eavesdropping. The increase in the SKR is quantified by the simplified SKR expansions derived in this article. Our results also reveal that squeezing is beneficial for improving the SKR only for unrestricted eavesdropping. However, in a practical setting with restricted eavesdropping, increased squeezing leads to a reduction in the SKR.

INDEX TERMS Multiple-input multiple-output (MIMO), quantum cryptography, quantum key distribution (QKD), restricted eavesdropping, sixth-generation (6G), terahertz (THz).

I. INTRODUCTION

With the deployment of commercial fifth-generation (5G) services since 2020 [1], [2], [3], researchers have started investigating new use cases and required technologies for the upcoming beyond 5G (B5G) or 6G communication networks for 2030 and beyond [4], [5], [6], [7], [8], [9]. In the recent years, quantum information technology (QIT) has also been rapidly evolving; this includes advances in quantum communications and quantum computing [10], [11], [12], [13]. QIT is expected to play a key role in B5G/6G

networks for enhanced security, privacy, and optimal wireless resource management [14], [15]. Recent works have investigated quantum communication technologies including quantum state discrimination [16], quantum enhanced modulation schemes [17], [18], quantum entanglement distribution [19], [20], [21], [22], [23], and quantum key distribution (QKD) [24]. Among these, QKD is a promising technology that may play an important role in securing the data of next-generation communication networks [25], [26], [27], [28]. Unlike classical cryptography algorithms, such as

Rivest–Shamir–Adleman (RSA), advanced encryption standard (AES), and Diffie–Hellman (DH), whose security relies on a computationally hard problem, QKD is a hardware solution whose security is guaranteed by the laws of quantum physics [29], [30]. The rapid advancement in quantum computing poses a threat to the security of classical encryption algorithms, such as RSA/AES/DH, since the prime factorization problem and discrete logarithm problem can be solved in polynomial time by running Shor's algorithm on a quantum processor [31], [32], [33].

QKD is a promising quantum secure technology developed for distributing secret keys between two legitimate users, say Alice and Bob, in the presence of eavesdroppers [24]. Any eavesdropping attack can be detected by Alice and Bob with provable guarantees. The eavesdropper Eve tries to steal the key information between Alice and Bob by intercepting their quantum communication, injecting entangled quantum states, and then carrying out any general operation allowed by the laws of quantum physics. Quantum secure keys distributed by QKD can be used for physical layer security in a one-time-pad-based encryption scheme, as well as for higher layer symmetric key encryption schemes. Hence, QKD is a promising technology for quantum secure data transmission in B5G/6G wireless networks [34], [35], [36], [37].

There are two main categories of QKD protocols depending on the type of quantum states used. These are discrete variable-QKD (DV-QKD) and continuous variable-QKD (CV-QKD) schemes [24], [29]. In DV-QKD, the key information is encoded in the polarization of photons [38], whereas in CV-QKD, the key information is encoded in the quadratures of the continuous-variable quantum states [39], [40], [41], [42]. The security of DV-QKD is guaranteed by the no-cloning theorem, whereas the security of CV-QKD is guaranteed by Heisenberg's uncertainty principle. Since DV-QKD requires single-photon sources or weak coherent sources for encoding the qubits and single photon detectors at the receiver, it is difficult to integrate DV-QKD with the current telecommunication infrastructure. On the other hand, CV-QKD requires coherent optical sources and homodyne/heterodyne detectors, which are compatible with the classical coherent optical communication technology. Therefore, it is expected that CV-QKD could be more easily integrated with current and upcoming B5G/6G telecommunication systems [30], [33]. The terahertz (THz) frequency spectrum offers a number of advantages over the optical frequencies, for example, mobility of users, less delicate pointing, immunity to ambient light, cloud, and fog [43], [44], [45], [46], [47], [48], [49]. Therefore, recent works have investigated the feasibility of CV-QKD systems operating at THz frequencies [50], [51], [52], [53], [54], [55]. Moreover, the THz band is also a potential candidate for B5G/6G wireless systems [43], [44], [45], [46], [47], [48], [49], [56], which further motivates the applicability of THz CV-QKD. Although in the classical communication literature THz band refers to the frequency range of 0.1–10 THz,

for quantum communications higher frequencies upto 15 THz are required since the preparation thermal noise and atmospheric absorption losses are lower at these frequencies that can support CV-QKD [50], [51], [52]. THz CV-QKD can be implemented using bidirectional optical-to-THz converters [52]. In this article, we focus on THz CV-QKD systems for future B5G/6G wireless communication networks.

In order to guarantee unconditional security, a general QKD protocol assumes that Eve has unlimited computational power and can carry out any operation allowed by the laws of quantum mechanics [24]. Furthermore, it is assumed that Eve has full control over the quantum states transmitted by Alice and can carry out any joint quantum operation on them. In CV-QKD protocol where the quantum channel is modeled using a beamsplitter, the general eavesdropping model assumes that Eve has control over the entire environment; i.e., Eve can collect all photons that are lost in the environment during propagation from Alice to Bob [24]. This unrestricted eavesdropping is a very pessimistic assumption, and in practice, Eve can collect only a fraction of the lost photons due to the lossy wireless link between Alice and Eve. This is the restricted eavesdropping scenario where Eve does not have control over the entire quantum channel and can collect only a fraction of photons lost in the environment. Some recent works have studied the achievable secret key rate (SKR) under restricted eavesdropping for single-input-single-output (SISO) CV-QKD systems [57], [58]. The authors of [57] incorporated the effect of the lossy quantum channel between Eve and the main channel, and derived upper bounds on the SKR using the relative entropy of entanglement for a SISO CV-QKD system. The authors of [58] considered a different restricted eavesdropping scenario where Eve has an imperfect quantum memory, and analyzed the SKR under an optimal hybrid attack by Eve.

This article extends our previous work on multiple-input-multiple-output (MIMO) CV-QKD [50], [51], and analyzes the SKR under restricted eavesdropping by incorporating the effect of the channel transmittance of the wireless lossy link between Alice and Eve. The analysis of practically achievable SKR under restricted eavesdropping is important for practical MIMO THz CV-QKD system deployment. The following points summarize the main contributions of this article.

1) We propose a MIMO CV-QKD system model with restricted eavesdropping that incorporates the effects of the lossy link between Alice and Eve.
2) We derive new SKR expressions for the MIMO CV-QKD system under restricted eavesdropping with both coherent-state-based and squeezed-state-based CV-QKD protocols for both reverse reconciliation (RR) and direct reconciliation (DR) schemes.
3) We derive simplified expansions of the SKR, which quantify the performance of the proposed MIMO CV-QKD system with restricted eavesdropping relative

to unrestricted eavesdropping considered previously in [50] and [51].
4) We demonstrate that squeezing is beneficial to improve the SKR only for the unrestricted eavesdropping model.

Our results indicate that unlike the unrestricted eavesdropping model, in the restricted eavesdropping model positive SKRs are achievable for the DR scheme even when the transmittance of the main channel is less than 0.5, due to the lossy channel between Alice and Eve. This is important in practice since the transmittances of the main channel are generally expected to be less than 0.5 at THz frequencies due to the significant path loss and atmospheric-absorption loss at such frequencies. Our simulation results show that the SKR improves significantly in the restricted eavesdropping scenario where Eve can collect only a fraction of the lost photons. Furthermore, our results reveal that in a restricted eavesdropping setting, squeezing does not help to improve the SKR, indicating that coherent states are the preferred quantum states to be used.

The rest of this article is organized as follows. Section II describes the system model of the proposed MIMO CV-QKD scheme with restricted eavesdropping. Sections III and IV present the SKR analysis for coherent-state-based and squeezed-state-based CV-QKD protocols, respectively. Section V provides the numerical results. Finally, Section VI concludes this article.

Notation: Boldface upper case ($\mathbf{A}$) and lower case ($\mathbf{a}$) letters denote matrices and vectors, respectively. $\mathbf{A}^\dagger$ and $\mathbf{A}^T$ denote the conjugate transpose and transpose of a matrix $\mathbf{A}$, respectively. The inverse and determinant of a matrix $\mathbf{A}$ are denoted as $\mathbf{A}^{-1}$ and $\det(\mathbf{A})$, respectively. A real Gaussian distribution with mean μ and variance σ^2 is denoted as $\mathcal{N}(\mu, \sigma^2)$. The expectation and variance of a random variable X are denoted as $\mathbb{E}\{X\}$ and $\mathbb{V}\{X\}$, respectively. The annihilation and creation operators of a quantized electromagnetic field are denoted as $\hat{a}$, $\hat{a}^\dagger$, respectively. Furthermore, $[x]^+ = \max(0, x)$ denotes the positive part of x.

II. SYSTEM MODEL

We consider a quantum communication system operating at THz frequencies, where Alice transmits Gaussian coherent states to Bob for establishing a quantum secure key. The quantum secure key is extracted by carrying out postprocessing over an additional classical authenticated channel. Similar to [50], we consider a MIMO scenario where Alice has N_t transmit antennas and Bob has N_r receive antennas, and the MIMO wireless channel between them is represented by $\mathbf{H} \in \mathbb{C}^{N_r \times N_t}$. The MIMO THz channel model is given by [49], [50], [51]

$$\mathbf{H} = \sum_{m=1}^{M} \sqrt{\gamma_m} e^{j2\pi f_c \tau_m} \boldsymbol{\psi}_R\left(\phi_m^r\right) \boldsymbol{\psi}_T^\dagger\left(\phi_m^t\right) \quad (1)$$

where f_c denotes the frequency of the carrier signal, M denotes the total number of multipath components, γ_m models

the path-loss of the mth multipath component given by [[51], Eq. (3)], and τ_m denotes the propagation time delay of the mth multipath component. The angle of arrival at Bob's uniform linear array (ULA) of antennas and the angle of departure at Alice's ULA for the mth multipath component are denoted by ϕ_m^r and ϕ_m^t, respectively. Furthermore, the array response vectors at Bob's and Alice's ULA of antennas for the mth multipath component are denoted by $\boldsymbol{\psi}_R(\phi_m^r)$ and $\boldsymbol{\psi}_T^\dagger(\phi_m^t)$, respectively [[51], Eq. (2)].

Alice and Bob use the spatial multiplexing and beamforming capability of the MIMO CV-QKD system by employing singular value decomposition (SVD)-based transmit beamforming at Alice and receive combining at Bob. Alice generates N_t coherent states using Gaussian modulation, which are then transmitted from the N_t transmit antennas to Bob [50], [51]. To steal the secret key information, Eve introduces Gaussian modes during the transmission. We assume that Eve uses a Gaussian entangling attack where she generates a pair of two mode squeezed vacuum states (TMSV) for each transmit mode of Alice. Eve keeps one of the modes in her quantum memory and mixes the other mode with the incoming coherent state from Alice. For a 2×2 MIMO CV-QKD system, the effective MIMO channel can be pictorially depicted, as shown in Fig. 1. In Fig. 1, $\mathbf{B}_\eta$ is a 2×2 matrix that relates the annihilation operators at the input and output modes in a 2-port beamsplitter with transmissivity η, given by

$$\begin{bmatrix} \hat{a}_{\text{out},1} \\ \hat{a}_{\text{out},2} \end{bmatrix} = \underbrace{\begin{bmatrix} \sqrt{\eta} & \sqrt{1-\eta} \\ -\sqrt{1-\eta} & \sqrt{\eta} \end{bmatrix}}_{\mathbf{B}_\eta} \begin{bmatrix} \hat{a}_{\text{in},1} \\ \hat{a}_{\text{in},2} \end{bmatrix}. \quad (2)$$

Consider $\mathbf{H} = \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^\dagger$ as the SVD of the MIMO channel. Alice uses $\mathbf{V}$ as the beamforming matrix and Bob uses $\mathbf{U}^\dagger$ as the combining matrix, as shown in Fig. 1. In order to steal the key information, Eve generates two pairs of TMSV $\{e_1, E_1\}$ and $\{e_2, E_2\}$, of which the first modes (e_1, e_2) are stored in Eve's quantum memory, whereas the other two modes (E_1, E_2) are mixed with the modes transmitted by Alice. In contrast to the unrestricted eavesdropping model (worst case scenario), the output modes E_1', E_2' are not accessible to Eve. Instead, E_1', E_2' get mixed with environmental thermal vacuum modes (v_1, v_2) on a beam-splitter of transmissivity κ, as depicted in Fig. 1. Note that κ models the fraction of photons (lost during the transmission from Alice to Bob) that are accessible to Eve. Therefore, only the output modes E_1'', E_2'' are accessible to Eve for joint measurement with the stored ancilla modes (e_1, e_2) for carrying out eavesdropping. In a practical setting, κ can represent the channel transmittance of the quantum wiretap channel from Alice to Eve. In the beamsplitter model, the first input mode is the signal mode and the second input mode is the noise introduced by Eve (E_i) or the environmental thermal mode (v_i). Therefore, the beamsplitter matrices in the top part of Fig. 1 are transposed in ordered to be consistent with the input–output relation of the beamsplitter model. The beamsplitter model of the
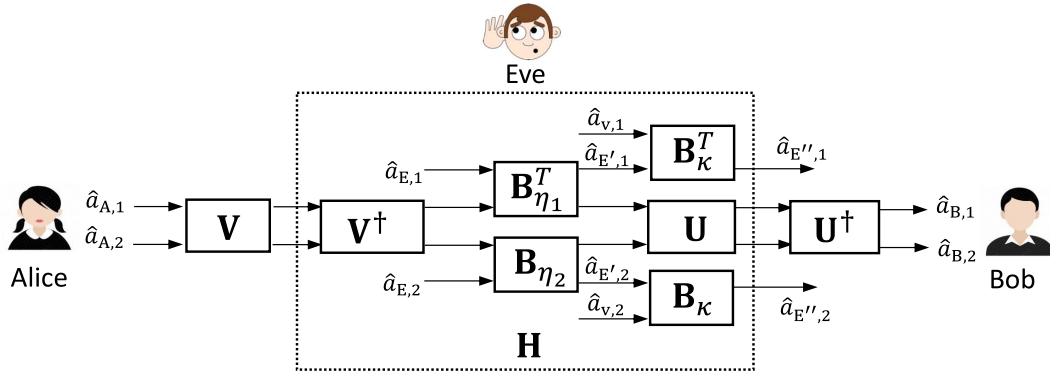
FIGURE 1. Schematic diagram showing the beam-splitter model for a 2 × 2 MIMO channel with restricted eavesdropping.

2×2 MIMO CV-QKD system depicted in Fig. 1 can be extended for an arbitrary $N_r \times N_t$ MIMO model, since an arbitrary $M \times M$ unitary matrix can be represented as a mesh of interconnected 2-port beamsplitters, as shown in [59].

After using SVD-based transmit beamforming and receive combining, the effective MIMO channel between Alice and Bob decomposes into parallel SISO bosonic thermal channels. The annihilation operators of the input–output modes at Alice ($\hat{a}_{A,i}$) and Bob ($\hat{a}_{B,i}$) for the ith parallel channel are related as

$$\hat{a}_{B,i} = \sqrt{T_i}\,\hat{a}_{A,i} + \sqrt{1-T_i}\,\hat{a}_{E,i}\,, \quad i = 1, 2, \ldots, r \quad (3)$$

where the ith nonzero singular value of $\mathbf{H}$ is denoted by $\sqrt{T_i}$ and the rank of the MIMO channel is denoted by r. The annihilation operator of the output mode accessible to Eve is given by

$$\hat{a}_{E'',i} = \sqrt{\kappa}\,\hat{a}_{E',i} + \sqrt{1-\kappa}\,\hat{a}_{v,i}\,, \quad i = 1, 2, \ldots, r \quad (4)$$

where κ models the transmissivity of the wireless link between Alice and Eve, $\hat{a}_{v,i}$ is the annihilation operator of the vacuum thermal mode, and $\hat{a}_{E',i}$ admits

$$\hat{a}_{E',i} = -\sqrt{1-T_i}\,\hat{a}_{A,i} + \sqrt{T_i}\,\hat{a}_{E,i}\,, \quad i = 1, 2, \ldots, r. \quad (5)$$

Eve performs general quantum measurements (positive operator value measure) on the stored ancilla modes e_i and the received modes E''_i in order to extract the maximum key information. The quadrature of the ancilla mode accessible to Eve is given by

$$X_{E'',i} = \sqrt{\kappa}\,X_{E',i} + \sqrt{1-\kappa}\,X_{v,i}\,, \quad i = 1, 2, \ldots, r \quad (6)$$

where $X_{E',i}$ admits

$$X_{E',i} = -\sqrt{1-\hat{T}_i}\,X_{A,i} + \sqrt{\hat{T}_i}\,X_{E,i}\,, \quad i = 1, 2, \ldots, r. \quad (7)$$

Here, $X_{A,i}$ is the quadrature of the coherent state transmitted by Alice, and $X_{E,i}$ is the quadrature of the TMSV state injected by Eve for stealing the key information. Note that $X_{Z,i}$ denotes either the real or imaginary quadrature of the Gaussian quantum state corresponding to mode Z. The variance of the Gaussian noise injected by Eve is $\mathbb{V}\{X_{E,i}\} = W$

shot-noise units (SNU), and the variance of the environment thermal mode, which arises due to the lossy bosonic channel between Alice and Eve, is given by $\mathbb{V}\{X_{v,i}\} = W'$ SNU.

A. CHANNEL ESTIMATION

The input–output relation of the annihilation operators at Alice and Bob in (3) assumes the availability of perfect channel state information (CSI) at both ends. However, CSI is estimated in practice to realize the SVD-based beamforming and combining at Alice and Bob, respectively. Alice and Bob can carry out a channel estimation protocol prior to the key generation protocol as proposed in [51]. Alice transmits pilot symbols and Bob uses a least squares (LS) channel estimator to estimate the MIMO channel matrix $\mathbf{H}_{LS}$ using [51, Eq. (8)]. The signal-to-noise ratio (SNR) during the channel estimation phase is defined as $\Gamma = \gamma_l V_p/(\gamma_l V_0 + \sigma_{\det}^2)$, where γ_l is the path loss of the line-of-sight component of the MIMO channel, V_p is the pilot power in SNU, V_0 is the preparation thermal noise power in SNU, and $\sigma_{\det}^2$ is the detector noise in SNU. The estimated channel matrix is then fed back to Alice using a classical authenticated communication (CAC) channel. The CAC channel is also necessary for carrying out the information reconciliation and error correction steps of the QKD protocol.

Bob randomly performs homodyne measurement on the received mode and measures one of the quadratures to extract the quantum secure keys. Accounting for imperfect CSI and detector noise at Bob, the input–output relation of the quadratures between Alice and Bob obtained from homodyne measurement is given by [51]

$$X_{B,i} = \sqrt{\hat{T}_i}\,X_{A,i} + \sqrt{1-\hat{T}_i}\,X_{E,i} - n_{h,i} + n_{\det,i}, \quad i = 1, \ldots, r \quad (8)$$

where $\sqrt{\hat{T}_i}$ denotes the ith nonzero singular value of $\mathbf{H}_{LS}$. Furthermore, $n_{h,i}$ denotes the additional noise term due to channel estimation error, which is distributed as $n_{h,i} \sim \mathcal{N}(0, \sigma_{h,i}^2)$, with $\sigma_{h,i}^2 = 0.5\mathbf{C}_h(i, i)$, where the matrix $\mathbf{C}_h$ is given by [51, Eq. (21)], and $n_{\det,i}$ denotes the detector noise distributed as $n_{\det,i} \sim \mathcal{N}(0, \sigma_{\det}^2)$, where $\sigma_{\det}^2 = v_{el}$ SNU for

a homodyne detector and $\sigma_{\mathrm{det}}^2 = 2v_{\mathrm{el}} + 1$ SNU for a hetero-dyne detector with v_{el} being the electronic noise in SNU.

There can be two types of CV-QKD protocols depending on the type of Gaussian quantum states used by Alice: coherent-state-based and squeezed-state-based. We consider each of these protocols in the sections that follow.

III. COHERENT-STATE-BASED CV-QKD PROTOCOL

In this section, we describe the coherent-state-based CV-QKD protocol and analyze the SKR of the system with restricted eavesdropping by Eve. For the ith transmit antenna, Alice first generates two independent zero-mean Gaussian random variables x_i, p_i of variance V_s, and then creates a displaced Gaussian coherent state $|\alpha_i\rangle$ such that $\alpha_i = x_i + Jp_i$, where $J = \sqrt{-1}$. The variance of each quadrature transmitted by Alice is given by $\mathbb{V}\{X_{\mathrm{A},i}\} = V_a = V_s + V_0$ SNU, where V_0 is the variance of the preparation thermal noise given by $V_0 = 2\bar{n} + 1$ with $\bar{n} = [\exp(hf_c/\kappa_{\mathrm{B}}T_e) - 1]^{-1}$, where κ_{B} is Boltzmann's constant, h is the Planck's constant, and T_e is the environmental temperature in Kelvin.

The coherent-state-based CV-QKD protocol can further be classified into two categories depending on the type of detection scheme used by Bob: homodyne detection to randomly measure one of the quadratures or heterodyne detection to simultaneously measure both quadratures (albeit with a higher detection noise) of the received quantum state. The homodyne detector gives one real-valued measurement outcome for each received quantum state, whereas the heterodyne detector gives two real-valued measurement outcomes, which can be used for generating the quantum secure keys. It was shown in [51] that at practical transmission distances, the SKR performance of the homodyne and heterodyne detection-based schemes are almost the same, due to the higher detector noise in the heterodyne case. Here, we focus on the homodyne detection scheme for the coherent-state-based CV-QKD protocol. After exchanging the quantum states, Alice and Bob carry out a sifting procedure where Bob declares over the CAC channel, which of the two quadratures was measured by Bob, and consequently Alice keeps either x_i or p_i for the ith mode depending on Bob's choice of the quadrature measurement. Therefore, Alice uses only one of the two random variables x_i or p_i for generating the secret key. After this, Alice and Bob carry out information reconciliation, classical error correction, and privacy amplification in order to extract the secret keys. In particular, there are two types of reconciliation schemes: (i) RR where Bob's data is used as a reference for classical

error correction, and (ii) DR where Alice's data is used as a reference for classical error correction. We present the SKR of the coherent-state-based MIMO CV-QKD system with restricted eavesdropping for both RR and DR schemes in the following.

A. REVERSE RECONCILIATION

For the coherent-state-based CV-QKD protocol with RR, the SKR for the ith parallel SISO channel is given by [60]

$$R_{\mathrm{c}\,i}^{\mathrm{r}} = \left(1 - \frac{T_p}{T_c}\right)\left(\beta I\left(X_{\mathrm{A},i} : X_{\mathrm{B},i}\right) - \chi\left(X_{\mathrm{B},i} : e_i E_i''\right)\right),$$
$$i = 1, \ldots, r \qquad (9)$$

where $I(X_{\mathrm{A},i} : X_{\mathrm{B},i})$ is the classical Shannon's mutual information between the random variables obtained from quadrature measurements by Alice and Bob, and $\chi(X_{\mathrm{B},i} : e_i E_i'')$ is the information leaked to Eve, which can be upper bounded by the Holevo information between Bob's measurement outcome $X_{\mathrm{B},i}$ and the quantum state available to Eve $\rho_{e_i E_i''}$. Furthermore, $\beta \in (0, 1)$ denotes the reconciliation efficiency, and T_p, T_c denote the pilot length and the channel coherence block length, respectively. Note that T_c depends on the coherence bandwidth (B_c) and coherence time (τ_c) of the wireless channel, given by $T_c = \tau_c B_c$, and for the LS channel estimator the pilot length should satisfy $T_p \geq N_t$.

Proposition 1: The total SKR of the MIMO CV-QKD system in RR for the coherent-state-based protocol with restricted eavesdropping is given by (10) shown at the bottom of the page. In (10), $\Lambda_i(x, y) \triangleq \hat{T}_i x + (1 - \hat{T}_i)y$, $h(x)$ is the function defined in (31), V_s is the variance of the signal quadrature transmitted by Alice, and V_0, W are the variances of the quadratures of the preparation thermal noise and Eve's injected noise, respectively. Furthermore, ζ_i is the quantum correlations between the mode E_i'' accessible to Eve and Bob's measurement outcome given by $\zeta_i = \sqrt{\kappa \hat{T}_i(1 - \hat{T}_i)(W - V_a)}$ and $V_{\mathrm{E}'} = \Lambda_i(W, V_a)$ with $V_a = V_s + V_0$.

Proof: See Appendix A. ∎

Now, we present a simplified expression for the SKR in order to quantify the effect of the restricted eavesdropping parameter κ on the SKR.

Proposition 2: For small κ (i.e., $\kappa \to 0$), the SKR expression can be approximated as (11), shown at the bottom of the next page.

Proof: The proof follows from a first-order Taylor series expansion of (10) with respect to κ. ∎

$$R_{\mathrm{c\,MIMO}}^{\mathrm{r}} = \left(1 - \frac{T_p}{T_c}\right)\sum_{i=1}^{r}\left[\frac{\beta}{2}\log_2\left(1 + \frac{\hat{T}_i V_s}{\Lambda_i(V_0, W) + \sigma_{\mathrm{det}}^2 + \sigma_{\mathrm{h},i}^2}\right) - h\left(\kappa V_{\mathrm{E}_i'} + (1 - \kappa)W'\right)\right.$$
$$\left. + h\left(\sqrt{(\kappa V_{\mathrm{E}_i'} + (1 - \kappa)W')^2 - \frac{(\kappa V_{\mathrm{E}_i'} + (1 - \kappa)W')\zeta_i^2}{\Lambda_i(V_a, W) + \sigma_{\mathrm{det}}^2 + \sigma_{\mathrm{h},i}^2}}\right)\right]^+ \qquad (10)$$

From (11), we observe that κ introduces a linear penalty on the SKR. The information leaked to Eve, which is given by the Holevo information, increases as $\kappa \to 1$. Therefore, the SKR decreases and attains the lowest value for unrestricted eavesdropping with $\kappa = 1$.

B. DIRECT RECONCILIATION

It is known that under the pessimistic assumption of unrestricted eavesdropping, positive SKR can be achieved in DR only under the constraint of $T_i > 0.5$ [60]. However, it is important to investigate if positive SKR could potentially be achieved in DR with $T_i < 0.5$ under a restricted eavesdropping scenario where only a fraction of the photons lost in the environment are accessible to Eve. In this section, we derive the SKR for the MIMO CV-QKD system with the DR scheme. For coherent-state-based CV-QKD protocols with DR, the SKR of the ith parallel SISO channel is given by [60]

$$R_{c\,i}^d = \left(1 - \frac{T_p}{T_c}\right)\left(\beta I\left(X_{A,i} : X_{B,i}\right) - \chi\left(X_{A,i} : e_i E_i''\right)\right)$$
$$i = 1, \ldots, r \tag{12}$$

where $I(X_{A,i} : X_{B,i})$ is given by (18) in Appendix A, and $\chi(X_{A,i} : e_i E_i'')$ denotes the maximum information leaked to Eve given Alice's quadrature measurement $X_{A,i}$.

Proposition 3: The total SKR of the MIMO CV-QKD system in DR for the coherent-state-based protocol with restricted eavesdropping is given by (13), shown at the bottom of the page, where $V_{E_i'|A} = \Lambda_i(W, V_0)$.

Proof: See Appendix B. ∎

As before, we now present a simplified expression for the SKR in DR in order to quantify the effect of the restricted eavesdropping parameter κ on the SKR.

Proposition 4: For small κ ($\kappa \to 0$) the SKR in DR can be approximated by

$$R_{c\,\text{MIMO}}^d$$
$$\approx \left(1 - \frac{T_p}{T_c}\right)\sum_{i=1}^{r}\left[\frac{\beta}{2}\log_2\left(1 + \frac{\hat{T}_i V_s}{\Lambda_i(V_0, W) + \sigma_{\det}^2 + \sigma_{h,i}^2}\right)\right.$$
$$\left. - \frac{\kappa(1 - \hat{T}_i)V_s}{4}\log_2\left(\frac{W' + 1}{W' - 1}\right)\right]^+. \tag{14}$$

Proof: The proof follows from a first-order Taylor series expansion of (13) with respect to κ. ∎

Similar to RR, it can be observed from (14) that the SKR for DR also decreases linearly as κ increases.

Remark: It is known that for the unrestricted eavesdropping model, positive SKR can be achieved only for $\hat{T}_i > 0.5$, which is generally not valid at THz frequencies due to significant path-loss and atmospheric absorption loss. However, for the restricted eavesdropping case the SKR can be positive even for $\hat{T}_i > 0.5$. This is because the information lost to Eve is reduced for $\kappa < 1$, as is evident from (14). For the restricted eavesdropping case, there exists a threshold $\kappa_{\max}$ above which positive SKR cannot be achieved in DR. This threshold value for κ can be determined from the approximate SKR expression in (14) by constraining the first term in the summation to be positive. Therefore, $\kappa_{\max}$ can be approximated as

$$\kappa_{\max} \approx \frac{\beta\log_2\left(1 + \frac{\hat{T}_1 V_s}{\Lambda_1(V_0, W) + \sigma_{\det}^2 + \sigma_{h,1}^2}\right)}{\kappa(1 - \hat{T}_1)V_s \log_2\left(\frac{W' + 1}{W' - 1}\right)} \tag{15}$$

where $\hat{T}_1$ is the maximum eigenvalue of $\mathbf{H}_{LS}^\dagger \mathbf{H}_{LS}$.

IV. SQUEEZED-STATE-BASED CV-QKD PROTOCOL

In the squeezed-state-based CV-QKD protocol, Alice uses a displaced squeezed quantum state. More specifically, for the ith transmit antenna mode, Alice first draws a zero-mean Gaussian random variable a_i of variance V_s. Alice prepares a squeezed vacuum state by applying a squeezing operation on one of the randomly chosen quadratures. Alice then displaces the squeezed quadrature by a_i [30]. This displaced squeezed quantum state is then transmitted from the ith transmit antenna. The variance of the squeezed quadrature in which the key information is encoded by Alice is given by $\mathbb{V}\{X_{A,i}\} = V_a' = V_s + V_0'$ with $V_0' = V_0 e^{-2s}$, where s is the squeezing parameter and V_0 is the variance of the thermal noise [61]. Note that as compared to the coherent-state-based CV-QKD protocol, in this protocol, the preparation noise is reduced for the squeezed quadrature. At the receiving
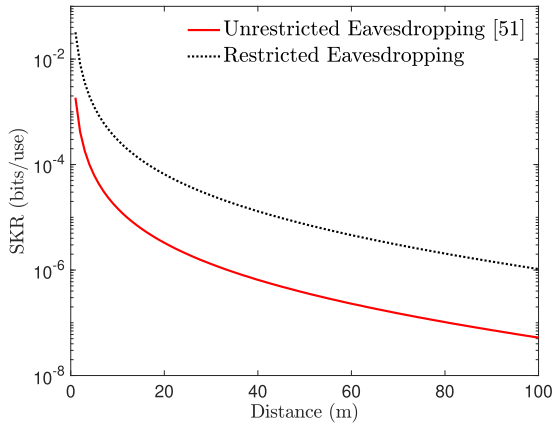
$$R_{c\,\text{MIMO}}^r \approx \left(1 - \frac{T_p}{T_c}\right)\sum_{i=1}^{r}\left[\frac{\beta}{2}\log_2\left(1 + \frac{\hat{T}_i V_s}{\Lambda_i(V_0, W) + \sigma_{\det}^2 + \sigma_{h,i}^2}\right) - \frac{\kappa\hat{T}_i(1 - \hat{T}_i)(V_a - W)^2}{4(\Lambda_i(V_a, W) + \sigma_{\det}^2 + \sigma_{h,i}^2)}\log_2\left(\frac{W' + 1}{W' - 1}\right)\right]^+ \tag{11}$$

$$R_{c\,\text{MIMO}}^d = \left(1 - \frac{T_p}{T_c}\right)\sum_{i=1}^{r}\left[\frac{\beta}{2}\log_2\left(1 + \frac{\hat{T}_i V_s}{\Lambda_i(V_0, W) + \sigma_{\det}^2 + \sigma_{h,i}^2}\right) - h\left(\kappa V_{E_i'} + (1 - \kappa)W'\right)\right.$$
$$\left. + h\left(\sqrt{(\kappa V_{E_i'} + (1 - \kappa)W')(\kappa V_{E_i'|A} + (1 - \kappa)W')}\right)\right]^+ \tag{13}$$

FIGURE 2. Plots show the SKR in RR $R^r_{c\,MIMO}$ (in bits/channel use) as a function of transmission distance for the MIMO CV-QKD scheme with $N_t = N_r = 64$ for two types of eavesdropping models, the unrestricted eavesdropping model from [51] and the restricted eavesdropping model proposed in this article with $\kappa = 0.1$.
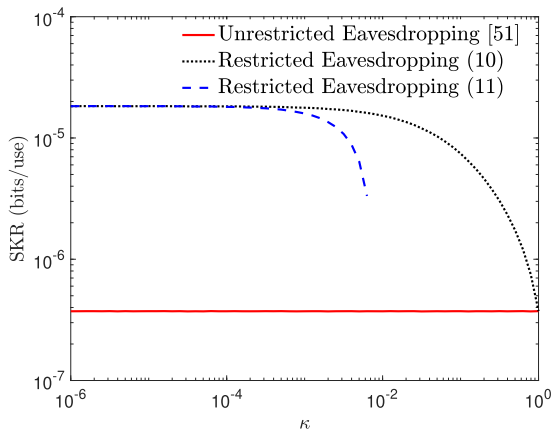

FIGURE 3. Plots show the SKR in RR $R^r_{c\,MIMO}$ as a function of κ for the MIMO CV-QKD scheme with $N_t = N_r = 64$ and a fixed transmission distance of 50 m for both unrestricted eavesdropping of [51] and restricted eavesdropping model.

end, Bob can perform either homodyne or heterodyne detection, which gives two categories of squeezed-state-based CV-QKD protocols.

A. HOMODYNE DETECTION

With homodyne detection, Bob randomly measures one of the quadratures to obtain one real-valued measurement outcome for each received quantum state. During the sifting process, Alice declares over the CAC channel, which of the two quadratures was squeezed for each of the transmitted quantum states. Bob then stores only those measurement outcomes for which the measurement bases matches Alice's squeezing basis. On average, only 50% of the times the measurement basis of Bob and Alice's squeezing basis will match. Therefore, only 50% of the measurement outcomes at Bob can be used for extracting the secret key. Hence, the SKR of the squeezed-state-based CV-QKD protocol with

homodyne detection scheme for RR and DR are given by

$$R^r_{s\,MIMO} = \frac{1}{2}R^r_{c\,MIMO} \qquad (16)$$

$$R^d_{s\,MIMO} = \frac{1}{2}R^d_{c\,MIMO} \qquad (17)$$

where $R^r_{c\,MIMO}$ and $R^d_{c\,MIMO}$ are evaluated from (10) and (13), respectively, by replacing $V_a \rightarrow V'_a$ and $V_0 \rightarrow V'_0$ since the preparation noise variance is reduced due to squeezing.

Remark: There are two competing factors that affect the SKR in the squeezed-state-based CV-QKD protocol with homodyne detection. On the one hand, the reduced noise variance (V'_0) in the squeezed state increases the first term in (11) (i.e., the mutual information between Alice and Bob). For the second term, the numerator is a quadratic function of V_0 (since $V_a = V_s + V_0$), and the denominator is a linear function of V_0: therefore, the second term decreases with decreasing V_0. On the other hand, there is a factor of 0.5 in the SKR expression of the squeezed-state-based CV-QKD protocol, since only 50% of the measurement outcomes could be utilized for extracting the keys. All the measurements cannot be used for extracting the secret key since the noise variance on the orthogonal quadrature will increase due to Heisenberg's uncertainty principle.

B. HETERODYNE DETECTION

With heterodyne detection, Bob measures both quadratures of the received quantum state. As before, during the sifting process, Alice declares which quadrature was squeezed by her. For each quantum state, Bob now has two real-valued measurement outcomes; however, Bob keeps only one of the measurement outcomes which corresponds to the squeezed quadrature of Alice. Thus, in contrast to the homodyne case, the measurement outcomes from all the received quantum states are used for extracting the secret key. However, in this case the detector noise is increased to $\sigma^2_{det} = 1 + 2v_{el}$. Therefore, the SKR for the squeezed-state-based CV-QKD protocol with heterodyne detection for both RR and DR can be obtained from the SKR expressions of the coherent-state-based CV-QKD protocol derived in the previous section [i.e., (10), (13)] by replacing $V_a \rightarrow V'_a$, $V_0 \rightarrow V'_0$, and using $\sigma^2_{det} = 1 + 2v_{el}$ in the SKR expressions.

Remark: There are again two competing factors which affect the SKR. On one hand the preparation noise, V'_0, reduces due to squeezing, however, on the other hand, the variance of the detector noise, σ^2_{det}, increases since a heterodyne detector is used to measure both quadratures simultaneously. The effect of squeezing on the SKR of the MIMO CV-QKD scheme with restricted eavesdropping is numerically investigated in the section that follows.

V. SIMULATION RESULTS
A. COHERENT-STATE-BASED CV-QKD PROTOCOL
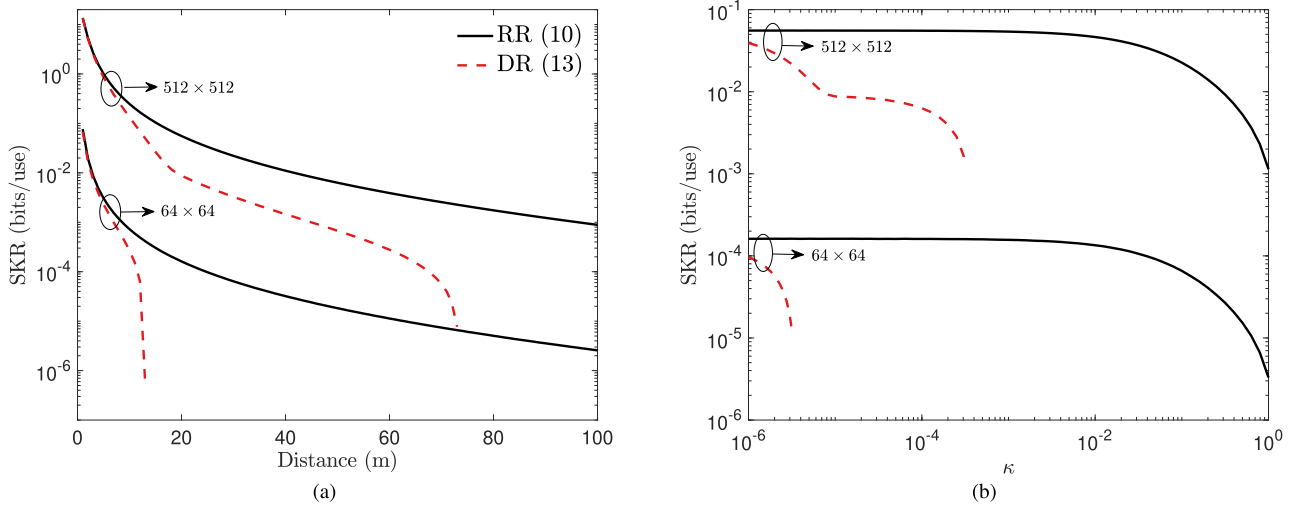We consider a simulation scenario similar to [51] and study the SKR at a frequency of 15 THz. We assume a

FIGURE 4. Plots show the SKR (in bits/channel use) as a function of (a) transmission distance (with fixed $\kappa = 10^{-5}$), and (b) κ (with fixed $d = 20$ m) for two MIMO configurations with restricted eavesdropping for both DR and RR schemes.

propagation scenario with a dominant line of sight (LoS) path such that $L = 1$ [51]. The *general system parameters* (applicable to all the figures) are: $V_s = 10$, $W = 1$, $W' = 1$, $T_e = 296$ K [60], $v_{el} = 0.01$, $\beta = 0.95$, $T_p = N_t + 500$, $T_c = 5 \times 10^5$, $\Gamma = 20$ dB, and the antenna gain is 30 dBi. Fig. 2 shows the plot of SKR of the MIMO CV-QKD system in RR $R^r_{c\,MIMO}$ (in bits/channel use) as a function of transmission distance with $N_t = N_r = 64$ for two types of eavesdropper models, the unrestricted eavesdropping model from [51] and the restricted eavesdropping model proposed in this article with $\kappa = 0.1$. It can be observed that the SKR under restricted eavesdropping is orders of magnitude larger than the pessimistic unrestricted eavesdropping model of [51], where Eve has access to all the photons lost in the environment. This is due to the fact that the Holevo information leaked to Eve is reduced in restricted eavesdropping with $\kappa < 1$, as indicated by the simplified SKR expression in (11).

We also study how the SKR varies as a function of κ. Fig. 3 shows the plot of the SKR $R^r_{c\,MIMO}$ as a function of κ with $N_t = N_r = 64$ and a fixed transmission distance of 50 m for both restricted and unrestricted eavesdropping models. SKR results for the restricted eavesdropping are plotted using the exact expression from (10) and the approximate expression from (11). It can be observed that the approximate SKR expression is accurate for small values of κ. It can also be observed that the SKR of the restricted eavesdropping model is higher than the SKR of the unrestricted eavesdropping, and the SKR with restricted eavesdropping approaches to that of the unrestricted eavesdropping as $\kappa \rightarrow 1$. This observation is in agreement with the analytical SKR approximation in (11).

Next, we evaluate the SKR of the MIMO CV-QKD system obtained from the DR scheme and compare it with that of the RR scheme under the restricted eavesdropping model. Fig. 4(a) shows the plots of the SKR of DR and RR as a function of transmission distance with restricted eavesdropping ($\kappa = 10^{-5}$) for two MIMO configurations. SKR results are
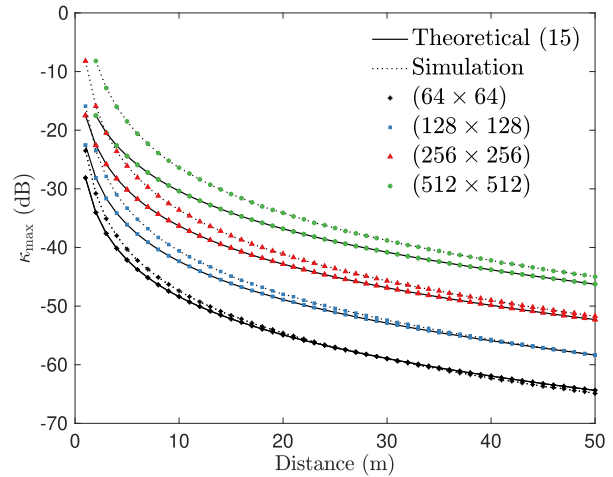

FIGURE 5. Plots show the threshold κ_{max} (above which positive SKR cannot be achieved in DR) as a function of transmission distance for different MIMO configurations.

shown based on the exact expressions from (10), (13) and the approximate expressions from (11), (14). It can be observed that the SKR obtained from the approximate expressions are close to that of the exact SKR expressions for lower transmission distances. It can also be observed that unlike the unrestricted eavesdropping model of [50], positive SKR is achievable in DR for the restricted eavesdropping model at practical transmission distances for which $T_i < 0.5$. This is due to the fact that the Holevo information leaked to Eve is reduced in the restricted eavesdropping model with $\kappa < 1$, as indicated by the simplified SKR expression in (14). Furthermore, it can be observed that at lower transmission distances the SKR obtained from DR and RR are almost the same, whereas at larger transmission distances the SKR obtained from RR is higher. Therefore, in practice, the RR scheme should be used for MIMO CV-QKD. We also evaluate the
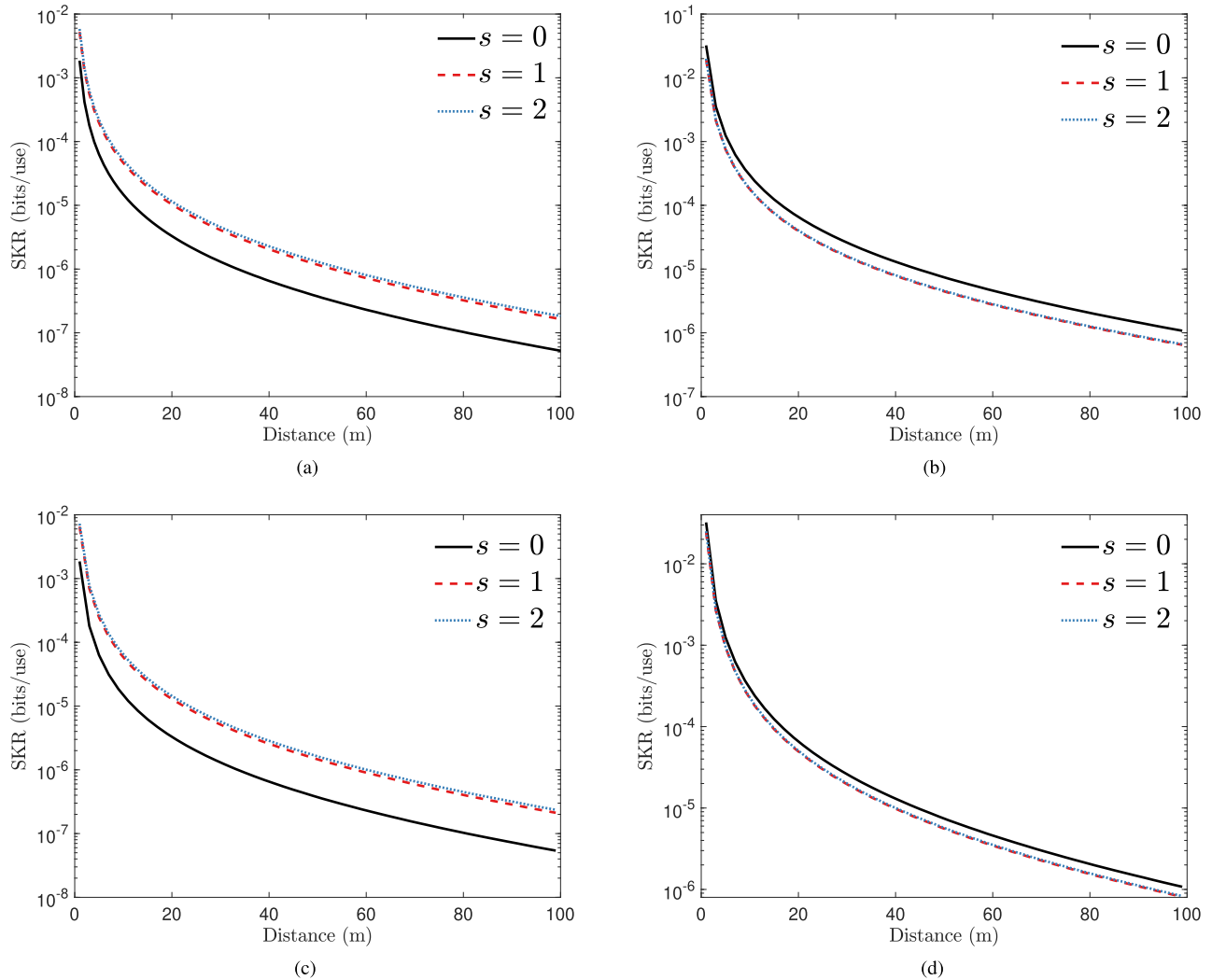
FIGURE 6. Plots show the SKR in RR as a function of transmission distance for the squeezed-state-based CV-QKD protocol for the unrestricted eavesdropping model ($\kappa = 1$) and restricted eavesdropping with $\kappa = 0.1$ at different squeezing levels s. Results are shown for both the homodyne (top row) and heterodyne (bottom row) detection-based protocol for a 64×64 MIMO. (a) Homodyne—Unrestricted Eavesdropping ($\kappa = 1$). (b) Homodyne—Restricted Eavesdropping ($\kappa = 0.1$). (c) Heterodyne—Unrestricted Eavesdropping ($\kappa = 1$). (d) Heterodyne—Restricted Eavesdropping ($\kappa = 0.1$).

SKR obtained from DR and RR as a function of κ. Fig. 4(b) shows the plots of the SKR of DR and RR as a function of κ for two MIMO configurations. It can be observed that the SKR obtained from the approximate expressions are close to those of the exact SKR expressions for small κ ($\kappa \to 0$). It can also be observed that the SKR decreases as κ increases for both DR and RR. However, the DR scheme is more sensitive to κ, since the SKR rapidly decreases and drops to zero as κ increases beyond a threshold value. This is due to the fact that the Holevo information leaked to Eve is higher in DR as compared to RR. The reason for this is that in DR the quantum state transmitted by Alice is accessible to Eve, whereas in RR the quantum state received by Bob is not accessible to Eve.

From Fig. 4(b), it can be observed that in RR positive SKR can be achieved for all values of $0 < \kappa \leq 1$, however, for DR there is a threshold $\kappa_{\max}$ above which positive SKR cannot be achieved. This threshold $\kappa_{\max}$ depends on the channel transmittance $\hat{T}_i$, which depends on the transmission distance and MIMO configuration. Fig. 5 shows the plot of $\kappa_{\max}$ as a function of transmission distance for different MIMO configurations. Results are shown for both the approximate theoretical $\kappa_{\max}$ obtained from (15), and the exact $\kappa_{\max}$ obtained from simulations. It can be observed that the approximate $\kappa_{\max}$ obtained from (15) is close to the exact $\kappa_{\max}$ for lower values of $\kappa_{\max}$ since the approximate SKR expression in (14) is valid for small values of κ ($\kappa \to 0$). In general, it can be observed that both the curves follow the general trend that the threshold $\kappa_{\max}$ decreases as the transmission increases. This is due to the fact that for a fixed MIMO configuration, the channel transmittance ($\hat{T}_i$) of the ith parallel channel decreases with increasing distance due to path-loss and atmospheric-absorption loss, therefore, the threshold $\kappa_{\max}$ should be lower in order to achieve positive
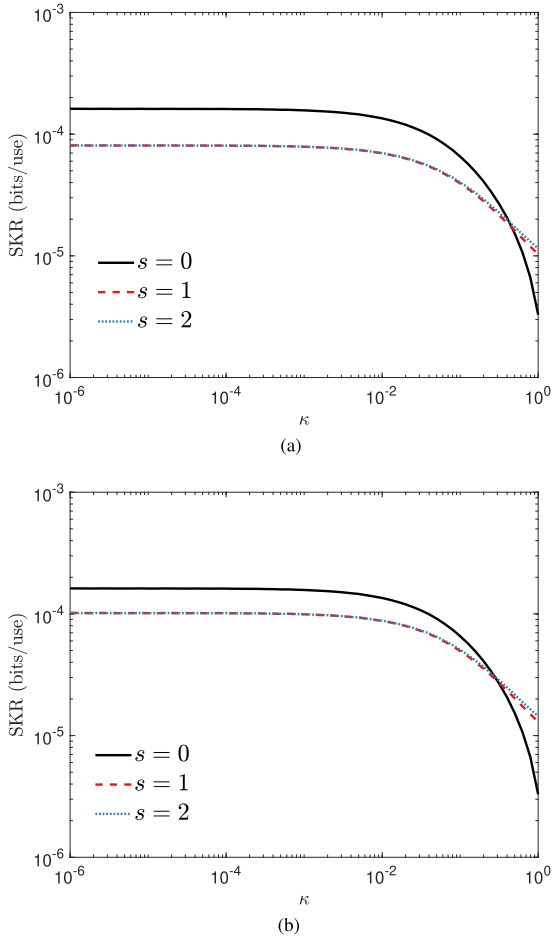
FIGURE 7. Plots show the SKR in RR as a function of κ, with restricted eavesdropping at different squeezing levels *s*. Results are shown for both the (a) homodyne and (b) heterodyne detection-based protocol for a 64 × 64 MIMO configuration at a transmission distance of 20 m.

SKR in DR. However, a higher threshold κ_{max} can be tolerated for larger MIMO configurations since $\hat{T}_i$ increases with increasing N_r, N_t due to the beamforming gain, which can be observed from the vertical shift in the curves for different MIMO configurations.

B. SQUEEZED-STATE-BASED CV-QKD PROTOCOL

Now we compare the SKRs of the squeezed-state-based CV-QKD protocols. Fig. 6 shows the plots of SKR in RR as a function of distance for the squeezed-state-based CV-QKD protocol for unrestricted eavesdropping ($\kappa = 1$) and restricted eavesdropping with $\kappa = 0.1$, at different squeezing levels *s*. Note that $s = 0$ corresponds to the coherent-state-based CV-QKD protocol. Results are shown for the homodyne-detection-based protocol in the top row and for the heterodyne-detection-based protocol in the bottom row for a 64 × 64 MIMO configuration. It can be observed that squeezing leads to an improvement in the SKR for the unrestricted eavesdropping model ($\kappa = 1$) for both homodyne and heterodyne-detection-based protocols. However, in

the case of restricted eavesdropping with $\kappa = 0.1$, squeezing leads to degradation in the SKR.

In the pessimistic scenario of unrestricted eavesdropping, the SKR is limited by the preparation thermal noise, therefore, the SKR improves as the preparation noise decreases with increased squeezing. In this case, the improvement in the SKR due to reduced preparation noise for squeezed state is overweighted by the decrease in SKR due to the factor of 0.5 (in homodyne detection) or the increased detector noise σ_{det}^2 (in heterodyne detection), which leads to an overall improvement in the SKR for the squeezed-state-based CV-QKD protocols. However, for the restricted eavesdropping scenario, the SKR is already higher for the coherent-state-based CV-QKD protocol since Eve can access only a fraction ($\kappa = 0.1$) of the photons lost in the environment. In this case, the reduction in preparation thermal noise does not benefit in increasing the SKR since the factor of 0.5 (in homodyne detection) or the increased detector noise σ_{det}^2 (in heterodyne detection) leads to a more deteriorating effect in the overall SKR. This can be intuitively understood as follows: as compared to the unrestricted eavesdropping model, in restricted eavesdropping the mutual information between Alice and Bob remains the same, whereas the information leaked to Eve (given by the Holevo information) is reduced. Therefore, for the squeezed-state-based CV-QKD protocol with homodyne detection the SKR reduces due to the overall factor of 0.5, whereas for the heterodyne detection the SKR reduces since the mutual information between Alice and Bob reduces due to the higher detector noise. Hence, it is beneficial to use a coherent-state-based CV-QKD protocol (which is also easier to implement) for the restricted eavesdropping scenario.

Next, we evaluate the SKR of the squeezed-state-based CV-QKD protocol as a function of κ in order to understand the range of κ values for which squeezing can improve the SKR of the CV-QKD system for the restricted eavesdropping model. Fig. 7 shows the plots of the SKR in RR as a function of κ with restricted eavesdropping at different squeezing levels *s*. Results are shown for both homodyne and heterodyne detection-based protocols for a (64 × 64) MIMO configuration at a fixed transmission distance of 20 m. It can be observed that there exists a threshold κ_{th} below which squeezing leads to a deteriorating effect on the SKR and above this threshold the SKR improves with squeezing as compared to the coherent-state-based CV-QKD. It can also be observed that for the unrestricted eavesdropping model with $\kappa = 1$, squeezing always leads to an improvement in the SKR for both the homodyne and heterodyne detection-based CV-QKD. The SKR results can be used for practical THz CV-QKD system deployment and to determine if a squeezing-based protocol should be used or not depending on what practical setting the CV-QKD protocol is designed to operate at. Our simulation results suggest that in a practical restricted eavesdropping scenario with κ much less than unity, no real gain in SKR can be achieved by using squeezed states. Moreover, it is much easier to generate coherent states as compared to squeezed states, therefore, in

practice, coherent-state-based CV-QKD protocol should be used.

VI. CONCLUSION

This article analyzes the SKR of a MIMO CV-QKD system under a restricted eavesdropping scenario where Eve can collect only a fraction of photons lost in the environment. In a practical setting, Eve does not have control over the entire environment due to the presence of the lossy wireless link between Alice and Eve. We have presented a system model and derived new SKR expressions for a MIMO CV-QKD system that incorporates the effect of the channel transmittance of the Alice–Eve link. We have investigated the SKR of the system with both coherent-state-based and squeezed-state-based CV-QKD protocols. The SKR expressions reveal that the information leaked to Eve, given by the Holevo information, is reduced for the restricted eavesdropping scenario, which improves the achievable SKR of the system. Our simulation results show that under restricted eavesdropping the SKR improves by orders of magnitude as compared to the pessimistic scenario of unrestricted eavesdropping. Furthermore, our results reveal that squeezing is beneficial for improving the SKR mainly for the unrestricted eavesdropping model. In practical settings with restricted eavesdropping due to the lossy link between Alice and Eve, the SKR degrades as squeezing increases. Therefore, in practice, coherent-state-based CV-QKD protocols should be used, which are also easier to implement. Our results reveal that THz CV-QKD is a promising solution for quantum secure data transmission in future communication networks [62].

There are certain practical challenges that need to be overcome in order to implement the MIMO THz CV-QKD system investigated in this article. A reliable estimate of the MIMO channel is crucial for realizing the SVD-based transmit–receive beamforming. The LS-based channel estimation scheme considered in this article requires a high SNR during the channel estimation phase in order to reliably estimate the channel matrix for large MIMO systems. Therefore, THz sources with high signal power are necessary during the channel estimation phase. This could be realized with the technological advancement of frequency down-conversion of high-power laser sources to THz frequencies [63]. Therefore, significant advances in high-power THz sources and low-noise homodyne/heterodyne detectors are necessary for the implementation of MIMO THz CV-QKD in future communication systems. Alternatively, the transmitted pilot power could potentially be reduced by using compressive sensing-based channel estimation schemes, since the THz MIMO channel has a sparse representation in the angular domain due to the limited number of multipath components at THz frequencies. Therefore, efficient channel estimation schemes for MIMO THz channels and achievable SKR analysis are important research problems that should be investigated in future extensions of this work.

APPENDIX
A. PROOF OF PROPOSITION 1

Using the input–output relation of the quadratures at Alice and Bob from (8), the classical Shannon's mutual information between Alice and Bob is given by

$$I\left(X_{\mathrm{A},i} : X_{\mathrm{B},i}\right) = \frac{1}{2}\log_2\left(1 + \frac{\hat{T}_i V_{\mathrm{s}}}{\Lambda_i\left(V_0, W\right) + \sigma_{\mathrm{det}}^2 + \sigma_{\mathrm{h},i}^2}\right) \tag{18}$$

where $\Lambda_i(x, y) \triangleq \hat{T}_i x + (1 - \hat{T}_i)y$, V_{s} is the variance of the signal quadrature transmitted by Alice, and V_0 and W are the variances of the quadratures of the preparation thermal noise and Eve's injected noise, respectively. Furthermore, note that $\sigma_{\mathrm{det}}^2 = v_{\mathrm{el}}$ for the homodyne detector used in the coherent-state-based CV-QKD protocol.

The Holevo information between Eve and Bob is given by

$$\chi\left(X_{\mathrm{B},i} : e_i E_i''\right) = S(\boldsymbol{\rho}_{e_i E_i''}) - S(\boldsymbol{\rho}_{e_i E_i''|X_{\mathrm{B},i}}) \tag{19}$$

where $S(\boldsymbol{\rho})$ is the von-Neumann entropy of the quantum state with density operator $\boldsymbol{\rho}$ given by $S(\boldsymbol{\rho}) = -\mathrm{Tr}(\boldsymbol{\rho}\log\boldsymbol{\rho})$. In (19), $\boldsymbol{\rho}_{e_i E_i''}$ is the density operator of Eve's state for the ith parallel channel and $\boldsymbol{\rho}_{e_i E_i''|X_{\mathrm{B},i}}$ is the density operator of the conditional quantum state given Bob's measurement outcome $X_{B,i}$. For Gaussian quantum states the von-Neumann entropy depends on the covariance matrix of the quantum states in terms of the symplectic eigenvalues [64]. Using (6), (7), and the covariance matrix of the TMSV state, the covariance matrix of the Gaussian quantum state $\boldsymbol{\rho}_{e_i E_i''}$ admits

$$\boldsymbol{\Sigma}_E^i = \begin{bmatrix} \mathbf{A}_i & \mathbf{C}_i \\ \mathbf{C}_i^T & \mathbf{B}_i \end{bmatrix} \tag{20}$$

where

$$\mathbf{A}_i = a_i \mathbf{I}_2 \quad \mathbf{B}_i = W\mathbf{I}_2 \tag{21}$$

with

$$a_i = \kappa V_{\mathrm{E}_i'} + (1 - \kappa)W' \tag{22}$$

$$V_{\mathrm{E}_i'} = \hat{T}_i W + (1 - \hat{T}_i)V_{\mathrm{a}} \tag{23}$$

and $\mathbf{I}_2$ being the 2×2 identity matrix. Furthermore

$$\mathbf{C}_i = c_i \mathbf{Z} \tag{24}$$

where

$$c_i = \sqrt{\kappa \hat{T}_i(W^2 - 1)} \tag{25}$$

and $\mathbf{Z}$ is the Pauli-z matrix with entries

$$\mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{26}$$

Using the properties of two-mode Gaussian quantum states [33], [65], the symplectic eigenvalues of $\boldsymbol{\Sigma}_E^i$ admit

$$v_{1,2}^i = \sqrt{0.5\left(\Delta_i \pm \sqrt{\Delta_i^2 - 4\det(\boldsymbol{\Sigma}_E^i)}\right)} \tag{27}$$

where $\Delta_i = \det(\mathbf{A}_i) + \det(\mathbf{B}_i) + 2\det(\mathbf{C}_i)$. After some algebra, we obtain

$$v^i_{1,2} = \frac{1}{2}\left(\sqrt{(a_i + W)^2 - 4\hat{T}_i\kappa(W^2 - 1)} \pm (a_i - W)\right). \tag{28}$$

For large signal variance i.e., $V_s \gg W$, $V_s \gg W'$, and $V_s \gg V_0$, the symplectic eigenvalues can be approximated as

$$v^i_1 \approx a_i$$
$$v^i_2 \approx W. \tag{29}$$

The von-Neumann entropy $S(\boldsymbol{\rho}_{e_i E''_i})$ is given by

$$S(\boldsymbol{\rho}_{e_i E''_i}) = h(v^i_1) + h(v^i_2) \tag{30}$$

where the function $h(x)$ is defined as

$$h(x) \triangleq \frac{(x+1)}{2}\log_2\frac{(x+1)}{2} - \frac{(x-1)}{2}\log_2\frac{(x-1)}{2}. \tag{31}$$

Next, we find the covariance matrix of the conditional state $\boldsymbol{\rho}_{e_i E''_i | X_{B,i}}$. This is given by

$$\boldsymbol{\Sigma}^i_{E|B} = \boldsymbol{\Sigma}^i_E - (V_{B,i})^{-1}\mathbf{D}_i\boldsymbol{\Pi}\mathbf{D}_i^T \tag{32}$$

where $\boldsymbol{\Sigma}^i_E$ is given by (20), $V_{B,i}$ is the variance of the output mode measured by Bob given by

$$V_{B,i} = \Lambda_i(V_a, W) + \sigma^2_{det} + \sigma^2_{h,i} \tag{33}$$

and

$$\boldsymbol{\Pi} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \tag{34}$$

is a projection matrix for homodyne measurement. Furthermore, $\mathbf{D}_i$ is the matrix containing the quantum correlations between the modes available to Eve (e_i, E''_i), and Bob's measurement outcome $X_{B,i}$, and is given by

$$\mathbf{D}_i = \begin{bmatrix} \mathbb{E}(E''_i X_{B,i})\mathbf{I}_2 \\ \mathbb{E}(e_i X_{B,i})\mathbf{Z} \end{bmatrix} = \begin{bmatrix} \zeta_i\mathbf{I}_2 \\ \phi_i\mathbf{Z} \end{bmatrix} \tag{35}$$

where

$$\zeta_i = \sqrt{\kappa\hat{T}_i(1 - \hat{T}_i)}(W - V_a) \tag{36}$$

and

$$\phi_i = \sqrt{(1 - \hat{T}_i)(W^2 - 1)}. \tag{37}$$

Substituting (20) and (34)–(37) in (32), we obtain

$$\boldsymbol{\Sigma}^i_{E|B} = \begin{bmatrix} \mathbf{E}_i & \mathbf{F}_i \\ \mathbf{F}_i^T & \mathbf{G}_i \end{bmatrix} \tag{38}$$

where

$$\mathbf{E}_i = \begin{bmatrix} a_i - \frac{\zeta_i^2}{V_{B,i}} & 0 \\ 0 & a_i \end{bmatrix} \quad \mathbf{F}_i = \begin{bmatrix} c_i - \frac{\zeta_i\phi_i}{V_{B,i}} & 0 \\ 0 & -c_i \end{bmatrix}$$

$$\mathbf{G}_i = \begin{bmatrix} W - \frac{\phi_i^2}{V_{B,i}} & 0 \\ 0 & W \end{bmatrix}. \tag{39}$$

The symplectic eigenvalues of $\boldsymbol{\Sigma}^i_{E|B}$ are given by

$$v^i_{3,4} = \sqrt{0.5\left(\Upsilon_i \pm \sqrt{\Upsilon_i^2 - 4\det(\boldsymbol{\Sigma}^i_{E|B})}\right)} \tag{40}$$

where $\Upsilon_i = \det(\mathbf{E}_i) + \det(\mathbf{G}_i) + 2\det(\mathbf{F}_i)$. For large signal variance, the symplectic eigenvalues of the conditional covariance matrix can be approximated as

$$v^i_3 \approx \sqrt{a_i\left(a_i - \frac{\zeta_i^2}{V_{B,i}}\right)}$$

$$v^i_4 \approx W. \tag{41}$$

The von Neumann entropy of Eve's conditional state in terms of the symplectic eigenvalues is given by

$$S(\boldsymbol{\rho}_{e_i E''_i | X_{B,i}}) = h(v^i_3) + h(v^i_4). \tag{42}$$

Thus, the Holevo information in (19) can be evaluated by substituting (30), (42) in (19), and the SKR for the ith parallel channel $R^r_{c,i}$ can be evaluated by substituting (18), (19) in (9). Finally, the total SKR of the MIMO CV-QKD system in RR for the coherent-state-based protocol in (10) is obtained by summing the SKR of all the parallel SISO channels.

B. PROOF OF PROPOSITION 3

In DR, the classical Shannon's mutual information between the measurement outcomes at Alice and Bob $I(X_{A,i} : X_{B,i})$ is same as that of the RR scheme given by (18). The maximum information leaked to Eve given Alice's quadrature measurement $X_{A,i}$ can be upper bounded by the Holevo information. In DR, the Holevo information admits

$$\chi(X_{A,i} : e_i E''_i) = S(\boldsymbol{\rho}_{e_i E''_i}) - S(\boldsymbol{\rho}_{e_i E''_i | X_{A,i}}) \tag{43}$$

where $S(\boldsymbol{\rho}_{e_i E''_i})$ is given by (30), and $S(\boldsymbol{\rho}_{e_i E''_i | X_{A,i}})$ denotes the conditional von Neumann entropy of Eve's state given Alice's measurement outcome $X_{A,i}$. $S(\boldsymbol{\rho}_{e_i E''_i | X_{A,i}})$ depends on the symplectic eigenvalues of the conditional covariance matrix. Using the relationship between the different quadrature modes from (6) to (7) and the covariance matrix of TMSV Gaussian state, the conditional covariance matrix admits

$$\boldsymbol{\Sigma}^i_{E|A} = \begin{bmatrix} \mathbf{J}_i & \mathbf{C}_i \\ \mathbf{C}_i^T & \mathbf{B}_i \end{bmatrix} \tag{44}$$

where

$$\mathbf{J}_i = \begin{bmatrix} b_i & 0 \\ 0 & a_i \end{bmatrix}. \tag{45}$$

In (45), a_i is given by (22), and b_i is given by

$$b_i = \kappa V_{E'_i | A} + (1 - \kappa)W' \tag{46}$$

where $V_{E'_i | A} = (1 - T_i)V_0 + T_iW$. Furthermore, the matrices $\mathbf{B}_i$ and $\mathbf{C}_i$ are given by (21) and (24), respectively. The von

Neumann entropy of the conditional state admits

$$S(\boldsymbol{\rho}_{e_i E_i''|X_{A,i}}) = h(\nu_5^i) + h(\nu_6^i) \tag{47}$$

where ν_5^i, ν_6^i are the symplectic eigenvalues of $\boldsymbol{\Sigma}_{E|A}^i$ given by

$$\nu_{5,6}^i = \sqrt{0.5\left(\Xi_i \pm \sqrt{\Xi_i^2 - 4\det(\boldsymbol{\Sigma}_{E|A}^i)}\right)} \tag{48}$$

where $\Xi_i = \det(\mathbf{J}_i) + \det(\mathbf{B}_i) + 2\det(\mathbf{C}_i)$. For large signal modulation, the symplectic eigenvalues can be simplified as

$$\nu_5^i \approx \sqrt{a_i b_i}$$
$$\nu_6^i \approx W \ . \tag{49}$$

In such a case, R_{ci}^d can be evaluated by substituting (18), (43) in (12). Finally, the total SKR of the MIMO CV-QKD system in DR for the coherent-state-based protocol in (13) is obtained by summing the SKR of all the parallel SISO channels.

REFERENCES

[1] M. Shafi et al., "5G: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1201–1221, Jun. 2017, doi: 10.1109/JSAC.2017.2692307.

[2] A. A. Ateya, A. Muthanna, M. Makolkina, and A. Koucheryavy, "Study of 5G services standardization: Specifications and requirements," in *Proc. 10th Int. Congr. Ultra Modern Telecommun. Control Syst. Workshops*, 2018, pp. 1–6, doi: 10.1109/ICUMT.2018.8631201.

[3] P. Suthar, V. Agarwal, R. S. Shetty, and A. Jangam, "Migration and interworking between 4G and 5G," in *Proc. 3rd 5G World Forum*, 2020, pp. 401–406, doi: 10.1109/5GWF49715.2020.9221021.

[4] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G wireless communications: Vision and potential techniques," *IEEE Netw.*, vol. 33, no. 4, pp. 70–75, Jul./Aug. 2019, doi: 10.1109/MNET.2019.1800418.

[5] I. F. Akyildiz, A. Kak, and S. Nie, "6G and beyond: The future of wireless communications systems," *IEEE Access*, vol. 8, pp. 133995–134030, 2020, doi: 10.1109/ACCESS.2020.3010896.

[6] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 957–975, Jul. 2020, doi: 10.1109/OJCOMS.2020.3010270.

[7] X. You et al., "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *China Inf. Sci.*, vol. 64, no. 1, pp. 1–74, Nov. 2020, doi: 10.1007/s11432-020-2955-6.

[8] M. Alsabah et al., "6G wireless communications networks: A comprehensive survey," *IEEE Access*, vol. 9, pp. 148191–148243, 2021, doi: 10.1109/ACCESS.2021.3124812.

[9] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, "The roadmap to 6G: AI empowered wireless networks," *IEEE Commun. Mag.*, vol. 57, no. 8, pp. 84–90, Aug. 2019, doi: 10.1109/MCOM.2019.1900271.

[10] M. Chiani, A. Conti, and M. Z. Win, "Piggybacking on quantum streams," *Phys. Rev. A*, vol. 102, no. 1, Jul. 2020, Art. no. 012410, doi: 10.1103/PhysRevA.102.012410.

[11] W. Dai, T. Peng, and M. Z. Win, "Quantum queuing delay," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 605–618, Mar. 2020, doi: 10.1109/JSAC.2020.2969000.

[12] D. Maslov, Y. Nam, and J. Kim, "An outlook for quantum computing [Point of View]," *Proc. IEEE*, vol. 107, no. 1, pp. 5–10, Jan. 2019, doi: 10.1109/JPROC.2018.2884353.

[13] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, and L. Gyongyosi, "Wireless myths, realities, and futures: From 3G/4G to optical and quantum wireless," *Proc. IEEE*, vol. 100, no. Special Centennial Issue, pp. 1853–1888, May 2012, doi: 10.1109/JPROC.2012.2189788.

[14] C. Wang and A. Rahman, "Quantum-enabled 6G wireless networks: Opportunities and challenges," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 58–69, Feb. 2022, doi: 10.1109/MWC.006.00340.

[15] P. Botsinis et al., "Quantum search algorithms for wireless communications," *IEEE Commun. Surv. Tut.*, vol. 21, no. 2, pp. 1209–1242, Second Quarter 2018, doi: 10.1109/COMST.2018.2882385.

[16] S. Guerrini, M. Z. Win, M. Chiani, and A. Conti, "Quantum discrimination of noisy photon-added coherent states," *IEEE J. Sel. Areas Inf. Theory*, vol. 1, no. 2, pp. 469–479, Aug. 2020, doi: 10.1109/JSAIT.2020.3012944.

[17] S. Guerrini, M. Chiani, M. Z. Win, and A. Conti, "Quantum pulse position modulation with photon-added coherent states," in *Proc. IEEE Globecom Workshops*, 2019, pp. 1–5, doi: 10.1109/GCWkshps45667.2019.9024469.

[18] S. Guerrini, M. Chiani, M. Z. Win, and A. Conti, "Quantum pulse position modulation with photon-added squeezed states," in *Proc. IEEE Globecom Workshops*, 2020, pp. 1–5, doi: 10.1109/GCWkshps50303.2020.9367479.

[19] W. Dai, T. Peng, and M. Z. Win, "Optimal remote entanglement distribution," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 540–556, Mar. 2020, doi: 10.1109/JSAC.2020.2969005.

[20] A. S. Cacciapuoti, M. Caleffi, R. Van Meter, and L. Hanzo, "When entanglement meets classical communications: Quantum teleportation for the quantum internet," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3808–3833, Jun. 2020, doi: 10.1109/TCOMM.2020.2978071.

[21] M. He, R. Malaney, and J. Green, "Global entanglement distribution with multi-mode non-Gaussian operations," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 528–539, Mar. 2020, doi: 10.1109/JSAC.2020.2968999.

[22] N. Hosseinidehaj and R. Malaney, "Gaussian entanglement distribution via satellite," *Phys. Rev. A*, vol. 91, no. 2, Feb. 2015, Art. no. 022304, doi: 10.1103/PhysRevA.91.022304.

[23] N. Hosseinidehaj and R. Malaney, "Quantum entanglement distribution in next-generation wireless communication systems," in *Proc. 85th Veh. Tech. Conf.*, 2017, pp. 1–7, doi: 10.1109/VTCSpring.2017.8108494.

[24] S. Pirandola et al., "Advances in quantum cryptography," *Adv. Optic Photon.*, vol. 12, no. 4, pp. 1012–1236, Dec. 2020, doi: 10.1364/AOP.361502.

[25] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the Qinternet," *IEEE Commun. Surv. Tut.*, vol. 24, no. 2, pp. 839–894, Second Quarter 2022, doi: 10.1109/COMST.2022.3144219.

[26] Z. Wang, R. Malaney, and J. Green, "Inter-satellite quantum key distribution at terahertz frequencies," in *Proc. IEEE Int. Conf. Commun.*, Shanghai, China, 2019, pp. 1–7, doi: 10.1109/ICC.2019.8761168.

[27] S. P. Kish, E. Villaseñor, R. Malaney, K. A. Mudge, and K. J. Grant, "Feasibility assessment for practical continuous variable quantum key distribution over the satellite-to-earth channel," *Quantum Eng.*, vol. 2, no. 3, Jul. 2020, Art. no. e50, doi: 10.1002/que2.50.

[28] S. Guerrini, M. Chiani, and A. Conti, "Secure key throughput of intermittent trusted-relay QKD protocols," in *Proc. IEEE Globecom Workshops*, 2018, pp. 1–5, doi: 10.1109/GLOCOMW.2018.8644402.

[29] I. B. Djordjevic, *Physical-Layer Security and Quantum Key Distribution*. Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-030-27565-5.

[30] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Commun. Surv. Tut.*, vol. 21, no. 1, pp. 881–919, First Quarter 2019, doi: 10.1109/COMST.2018.2864557.

[31] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, Apr. 1999, doi: 10.1137/S0097539795293172.

[32] A. Manzalini, "Quantum communications in future networks and services," *Quantum Rep.*, vol. 2, no. 1, pp. 221–232, Mar. 2020, doi: 10.3390/quantum2010014.

[33] C. Weedbrook et al., "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, no. 2, pp. 621–669, May 2012, doi: 10.1103/RevModPhys.84.621.

[34] A. Sanenga, G. A. Mapunda, T. M. L. Jacob, L. Marata, B. Basutli, and J. M. Chuma, "An overview of key technologies in physical layer security," *Entropy*, vol. 22, no. 11, Nov. 2020, Art. no. 1261, doi: 10.3390/e22111261.

[35] H. A. Al-Mohammed and E. Yaacoub, "On the use of quantum communications for securing IoT devices in the 6G era," in *Proc. IEEE Int. Conf. Commun. Workshop*, 2021, pp. 1–6, doi: 10.1109/ICCWorkshops50388.2021.9473793.

[36] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 281–291, Aug. 2020, doi: 10.1016/j.dcan.2020.07.003.

[37] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash, and A. K. Mishra, "Quantum key distribution secured optical networks: A survey," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 2049–2083, Aug. 2021, doi: 10.1109/OJ-COMS.2021.3106659.

[38] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, Bangalore, India, 1984, pp. 175–179, doi: 10.1016/j.tcs.2014.05.025.

[39] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," *Nature*, vol. 421, no. 6920, pp. 238–241, Jan. 2003, doi: 10.1038/nature01289. .

[40] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, Jan. 2002, Art. no. 057902, doi: 10.1103/PhysRevLett.88.057902.

[41] L. Hu, M. Al-Amri, Z. Liao, and M. Zubairy, "Continuous-variable quantum key distribution with non-Gaussian operations," *Phys. Rev. A*, vol. 102, no. 1, Jul. 2020, Art. no. 012608, doi: 10.1103/PhysRevA.102.012608.

[42] Y. Guo, W. Ye, H. Zhong, and Q. Liao, "Continuous-variable quantum key distribution with non-Gaussian quantum catalysis," *Phys. Rev. A*, vol. 99, no. 3, Mar. 2019, Art. no. 032327, doi: 10.1103/PhysRevA.99.032327.

[43] H. Elayan, O. Amin, B. Shihada, R. M. Shubair, and M.-S. Alouini, "Terahertz band: The last piece of RF spectrum puzzle for communication systems," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1–32, Nov. 2020, doi: 10.1109/OJCOMS.2019.2953633.

[44] H. Sarieddeen, N. Saeed, T. Y. Al-Naffouri, and M.-S. Alouini, "Next generation terahertz communications: A rendezvous of sensing, imaging, and localization," *IEEE Commun. Mag.*, vol. 58, no. 5, pp. 69–75, May 2020, doi: 10.1109/MCOM.001.1900698.

[45] I. F. Akyildiz, J. M. Jornet, and C. Han, "Terahertz band: Next frontier for wireless communications," *Phy. Commun.*, vol. 12, pp. 16–32, Sep. 2014, doi: 10.1016/j.phycom.2014.01.006.

[46] H. Sarieddeen, M.-S. Alouini, and T. Y. Al-Naffouri, "An overview of signal processing techniques for terahertz communications," *Proc. IEEE*, vol. 109, no. 10, pp. 1628–1665, Oct. 2021, doi: 10.1109/JPROC.2021.3100811.

[47] T. Kürner and S. Priebe, "Towards THz communications-status in research, standardization and regulation," *J. Infrared, Millimeter, THz Waves*, vol. 35, no. 1, pp. 53–62, Jan. 2014, doi: 10.1007/s10762-013-0014-3.

[48] K. M. S. Huq, S. A. Busari, J. Rodriguez, V. Frascolla, W. Bazzi, and D. C. Sicker, "Terahertz-enabled wireless system for beyond-5G ultra-fast networks: A brief survey," *IEEE Netw.*, vol. 33, no. 4, pp. 89–95, Jul./Aug. 2019, doi: 10.1109/MNET.2019.1800430.

[49] S. A. Busari, K. M. S. Huq, S. Mumtaz, and J. Rodriguez, "Terahertz massive MIMO for beyond-5G wireless communication," in *Proc. IEEE Int. Conf. Commun.*, Shanghai, China, 2019, pp. 1–6, doi: 10.1109/ICC.2019.8761371.

[50] N. K. Kundu, S. P. Dash, M. R. McKay, and R. K. Mallik, "MIMO terahertz quantum key distribution," *IEEE Commun. Lett.*, vol. 25, no. 10, pp. 3345–3349, Oct. 2021, doi: 10.1109/LCOMM.2021.3102703.

[51] N. K. Kundu, S. P. Dash, M. R. McKay, and R. K. Mallik, "Channel estimation and secret key rate analysis of MIMO terahertz quantum key distribution," *IEEE Trans. Commun.*, vol. 70, no. 5, pp. 3350–3363, May 2022, doi: 10.1109/TCOMM.2022.3161008.

[52] C. Ottaviani et al., "Terahertz quantum cryptography," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 483–495, Mar. 2020, doi: 10.1109/JSAC.2020.2968973.

[53] X. Liu, C. Zhu, N. Chen, and C. Pei, "Practical aspects of terahertz wireless quantum key distribution in indoor environments," *Quantum Inf. Process.*, vol. 17, no. 11, pp. 1–20, Sep. 2018, doi: 10.1007/s11128-018-2068-6.

[54] Y. He, Y. Mao, D. Huang, Q. Liao, and Y. Guo, "Indoor channel modeling for continuous variable quantum key distribution in the terahertz band," *Opt. Exp.*, vol. 28, no. 22, pp. 32386–32402, Oct. 2020, doi: 10.1364/OE.405020.

[55] C. Liu, C. Zhu, X. Liu, M. Nie, H. Yang, and C. Pei, "Multicarrier multiplexing continuous-variable quantum key distribution at terahertz bands under indoor environment and in inter-satellite links communication," *IEEE Photon. J.*, vol. 13, no. 4, Aug. 2021, Art. no. 7600113, doi: 10.1109/JPHOT.2021.3098717.

[56] T. S. Rappaport et al., "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," *IEEE Access*, vol. 7, pp. 78729–78757, 2019, doi: 10.1109/ACCESS.2019.2921522.

[57] Z. Pan et al., "Secret-key distillation across a quantum wiretap channel under restricted eavesdropping," *Phys. Rev. Appl.*, vol. 14, no. 2, Aug. 2020, Art. no. 024044, doi: 10.1103/PhysRevApplied.14.024044.

[58] N. Hosseinidehaj, N. Walk, and T. C. Ralph, "Optimal realistic attacks in continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 99, no. 5, May 2019, Art. no. 052336, doi: 10.1103/PhysRevA.99.052336.

[59] W. R. Clements, P. C. Humphreys, B. J. Metcalf, W. S. Kolthammer, and I. A. Walmsley, "Optimal design for universal multiport interferometers," *Optica*, vol. 3, no. 12, pp. 1460–1465, Dec. 2016, doi: 10.1364/OPTICA.3.001460.

[60] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, "Quantum cryptography approaching the classical limit," *Phys. Rev. Lett.*, vol. 105, no. 11, Sep. 2010, Art. no. 110501, doi: 10.1103/PhysRevLett.105.110501.

[61] N. K. Kundu, M. R. McKay, and R. K. Mallik, "Machine-learning-based parameter estimation of Gaussian quantum states," *IEEE Trans. Quantum Eng.*, vol. 3, Dec. 2021, Art. no. 3500113, doi: 10.1109/TQE.2021.3137559.

[62] R. Liu, G. G. Rozenman, N. K. Kundu, D. Chandra, and D. De, "Towards the industrialisation of quantum key distribution in communication networks: A short survey," *IET Quantum Commun.*, vol. 3, no. 3, pp. 151–163, 2022 doi: 10.1049/qtc2.12044.

[63] V. A. Trofimov, D. M. Kharitonov, M. V. Fedotov, and Y. Yang, "Frequency down-conversion of optical pulse to the far infrared and THz frequency ranges due to the cascading process in a medium with a quadratic nonlinear response," *Appl. Sci.*, vol. 12, no. 8, 2022, Art. no. 3891, doi: 10.3390/app12083891.

[64] C. Weedbrook, S. Pirandola, and T. C. Ralph, "Continuous-variable quantum key distribution using thermal states," *Phys. Rev. A*, vol. 86, no. 2, Aug. 2012, Art. no. 022318, doi: 10.1103/PhysRevA.86.022318.

[65] A. Serafini, F. Illuminati, and S. D. Siena, "Symplectic invariants, entropic measures and correlations of Gaussian states," *J. Phys. B: Atom., Mol. Opt. Phys.*, vol. 37, no. 2, 2003, Art. no. L21, doi: 10.1088/0953-4075/37/2/L02.

Neel Kanth Kundu (Member, IEEE) received the B.Tech. degree in electrical engineering with a specialization in communication systems and networking from the Indian Institute of Technology Delhi, New Delhi, India, in 2018 and the Ph.D. degree in electronic and computer engineering (ECE) with a concentration in scientific computation from The Hong Kong University of Science and Technology (HKUST), Kowloon, Hong Kong, in 2022.

From September 2022 to January 2023, he was a Postdoctoral Research Associate with the Electronic and Computer Engineering (ECE) Department, HKUST. Since February 2023, he has been a Postdoctoral Research Fellow with the Department of Electrical and Electronic Engineering, The University of Melbourne, Melbourne, VIC, Australia. From May 2016 to July 2016, he was a visiting student intern with the Rice Integrated Systems and Circuits Lab, Rice University, Houston, TX, USA. From May 2017 to July 2017, he was a student trainee with the Samsung Research Institute, Bengaluru, India. From December 2021 to May 2022, he was a visiting Ph.D. student with the Department of Engineering, University of Ferrara, Ferrara, Italy. His research interests include machine-learning and deep-learning-based signal processing for 6G wireless communications, quantum communications, and quantum information processing.

Dr. Kundu is a recipient of the INSPIRE Young Faculty Fellowship awarded by the Department of Science and Technology, Government of India. He was the recipient of the Hong Kong Ph.D. Fellowship and the Overseas Research Award at HKUST.

Matthew R. McKay (Fellow, IEEE) received the Ph.D. degree in electrical engineering from the University of Sydney, Camperdown, NSW, Australia, in 2006.

He is currently a Professor with the Department of Electrical and Electronic Engineering, University of Melbourne, Melbourne, VIC, Australia, and also as a Professorial Fellow (Honorary) with the Department of Microbiology and Immunology. Prior to joining the University of Melbourne, he was a Professor with the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology (HKUST), Hong Kong, and also with the Department of Chemical and Biological Engineering. He is currently an Adjunct Professor with HKUST. He was a Research Scientist with the Institute for Medical Engineering and Science (IMES), Massachusetts Institute of Technology, Cambridge, MA, USA, in 2014, and with the Department of Statistics, Stanford University, Stanford, CA, USA, in 2015.

Dr. McKay and his coauthors were the recipient of best paper awards at multiple conferences (ICASSP, ICC, Globecom, etc.). He has been awarded a Future Fellowship of the Australian Research Council. He was also the recipient of a 2010 Young Author Best Paper Award by the IEEE Signal Processing Society, the 2011 Stephen O. Rice Prize by the IEEE Communication Society, and the Australia-China Alumni Award for Research and Science by the Australia-China Alumni Association, in 2021. He was the Area Editor of Feature Articles for *IEEE Signal Processing Magazine*, and also on the editorial boards of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS *Random Matrices: Theory and Applications*. In 2018, he was selected as a Young Scientist of the World Economic Forum. In 2020 and 2021, he was selected as a Young Scientist of the World Laureates Forum.

Andrea Conti (Fellow, IEEE) is currently a Professor and founding Director of the Wireless Communication and Localization Networks Laboratory, University of Ferrara, Ferrara, Italy. Prior to joining the University of Ferrara, he was with CNIT, and with IEIIT-CNR. In Summer 2001, he was with the Wireless Systems Research Department, AT&T Research Laboratories. Since 2003, he has been a frequent visitor with the Wireless Information and Network Sciences Laboratory, Massachusetts Institute of Technology, Cambridge, MA, USA, where he is currently holds the Research Affiliate appointment. His research interests involve theory and experimentation of wireless communication and localization systems. His current research topics include network localization and navigation, distributed sensing, adaptive diversity communications, and quantum information science.

Dr. Conti was an Editor for IEEE journals and chaired international conferences. He was an elected Chair of the IEEE Communications Society's Radio Communications Technical Committee and is Co-Founder of the IEEE Quantum Communications and Information Technology Emerging Technical Subcommittee. He was the recipient of the HTE Puskás Tivadar Medal, the IEEE Communications Society's Fred W. Ellersick Prize, and the IEEE Communications Society's Stephen O. Rice Prize in the field of Communications Theory. He is an elected Fellow of the IEEE and of the IET, and a member of Sigma Xi. He has been selected as an IEEE Distinguished Lecturer.

Ranjan K. Mallik (Fellow, IEEE) received the B.Tech. degree from the Indian Institute of Technology Kanpur, Kanpur, India, in 1987 and the M.S. and Ph.D. degrees from the University of Southern California, Los Angeles, Los Angeles, CA, USA, in 1988 and 1992, respectively, all in electrical engineering.

From August 1992 to November 1994, he was a Scientist with the Defence Electronics Research Laboratory, Hyderabad, India, working on missile and EW projects. From November 1994 to January 1996, he was a Faculty Member with the Department of Electronics and Electrical Communication Engineering, Indian Institute of Technology Kharagpur, Kharagpur, India. From January 1996 to December 1998, he was with the faculty of the Department of Electronics and Communication Engineering, Indian Institute of Technology Guwahati, Guwahati, India. Since December 1998, he has been with the faculty of the Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi, India, where he is currently an Institute Chair Professor. His research interests are in diversity combining and channel modeling for wireless communications, space-time systems, cooperative communications, multiple-access systems, power line communications, molecular communications, difference equations, and linear algebra.

Dr. Mallik is currently a member of Eta Kappa Nu, the IEEE Communications, Information Theory, and Vehicular Technology Societies, the American Mathematical Society, the International Linear Algebra Society, and the Association for Computing Machinery; a fellow of the Indian National Academy of Engineering, the Indian National Science Academy, The National Academy of Sciences, India, Prayagraj, the Indian Academy of Sciences, Bengaluru, The World Academy of Sciences-for the advancement of science in developing countries (TWAS), The Institution of Engineering and Technology, U.K., The Institution of Electronics and Telecommunication Engineers, India, The Institution of Engineers (India) (IEI), and the Asia-Pacific Artificial Intelligence Association; and a life member of the Indian Society for Technical Education. He is a recipient of the Hari Om Ashram Prerit Dr. Vikram Sarabhai Research Award in the field of electronics, telematics, informatics, and automation, the Shanti Swarup Bhatnagar Prize in engineering sciences, the Khosla National Award, the IEI-IEEE Award for Engineering Excellence, and the J. C. Bose Fellowship. He was an Area Editor and an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS.

Moe Z. Win (Fellow, IEEE) is currently a Professor with the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, and the Founding Director of the Wireless Information and Network Sciences Laboratory. Prior to joining MIT, he was with AT&T Research Laboratories and with NASA Jet Propulsion Laboratory. His research encompasses fundamental theories, algorithm design, and network experimentation for a broad range of real-world problems. His current research topics include ultrawideband systems, network localization and navigation, network interference exploitation, and quantum information science.

Dr. Win has served the IEEE Communications Society as an elected Member-at-Large on the Board of Governors, an elected Chair of the Radio Communications Committee, and an IEEE Distinguished Lecturer. Over the last two decades, he held various editorial positions for IEEE journals and organized numerous international conferences. Recently, he has served on the SIAM Diversity Advisory Committee. He is an elected Fellow of the AAAS, the EURASIP, the IEEE, and the IET. He was honored with two IEEE Technical Field Awards: the IEEE Kiyo Tomiyasu Award (2011) and the IEEE Eric E. Sumner Award (2006, jointly with R. A. Scholtz). His publications, coauthored with students and colleagues, was the recipient of several awards. Other recognitions include the MIT Everett Moore Baker Award (2022), the IEEE Vehicular Technology Society James Evans Avant Garde Award (2022), the IEEE Communications Society Edwin H. Armstrong Achievement Award (2016), the Cristoforo Colombo International Prize for Communications (2013), the Copernicus Fellowship (2011), and the *Laurea Honoris Causa* (2008) from the Università degli Studi di Ferrara, and the U.S. Presidential Early Career Award for Scientists and Engineers (2004). He is an ISI Highly Cited Researcher.